STUDY MATERIAL

PROFESSIONAL PROGRAMME

ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

GROUP 1

ELECTIVE PAPER 4.4

भारतीय कम्पनी सचिव संस्थान
THE INSTITUTE OF
Company Secretaries of India
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

© THE INSTITUTE OF COMPANY SECRETARIES OF INDIA

Timing of Headquarters :

Monday to Friday
Office Timings : 9.00 A.M. to 5.30 P.M.

Public Dealing Timings :

Without financial transactions – 9.30 A.M. to 5.00 P.M.
With financial transactions – 9.30 A.M. to 4.00 P.M.

Phones :

011-45341000 / 0120-4522000

Website :

www.icsi.edu

E-mail :

info@icsi.edu / academics@icsi.edu

For any suggestions/clarifications students may write to *academics@icsi.edu*

Disclaimer

Although due care and diligence have been taken in preparation of this Study Material, the Institute shall not be responsible for any loss or damage, resulting from any action taken on the basis of the contents of this Study Material. Anyone wishing to act on the basis of the material contained herein should do so after cross checking with the original source.

Laser Typesetting by :
AArushi Graphics, Prashant Vihar, New Delhi

PROFESSIONAL PROGRAMME

ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

Artificial Intelligence (AI) to be a kinetic enabler for the growth of our digital economy, investments, and jobs. AI refers to the ability of machines to perform cognitive tasks like thinking, perceiving, learning, problem solving and decision making. Initially conceived as a technology that could mimic human intelligence, AI has evolved in ways that far exceed its original conception. With incredible advances made in data collection, processing and computation power, intelligent systems can now be deployed to take over a variety of tasks, enable connectivity and enhance productivity. As AI's capabilities have dramatically expanded, so have its utility in a growing number of fields.

AI is emerging as a new factor of production, augmenting the traditional factors of production viz. labour, capital and innovation and technological changes captured in total factor productivity. AI has the potential to overcome the physical limitations of capital and labour, and open up new sources of value and growth. From an economic impact perspective, AI has the potential to drive growth through enabling: (a) intelligent automation i.e. ability to automate complex physical world tasks that require adaptability and agility across industries, (b) labour and capital augmentation: enabling humans to focus on parts of their role that add the most value, complementing human capabilities and improving capital efficiency, and (c) innovation diffusion i.e. propelling innovations as it diffuses through the economy. AI innovations in one sector will have positive consequences in another, as industry sectors are interdependent based on value chain. Economic value is expected to be created from the new goods, services and innovations that AI will enable.

On the other hand data is one of the primary drivers of AI solutions, and thus appropriate handling of data, ensuring privacy and security is of prime importance. Challenges include data usage without consent, risk of identification of individuals through data, data selection bias and the resulting discrimination of AI models, and asymmetry in data aggregation.

To ensure that Internet in India is Open, Safe, Trusted and Accountable, the Central Government, in exercise of powers conferred by the Information Technology Act, 2000 ("IT Act"), has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021"). The rules cast specific obligation on intermediaries vis-à-vis what kind of information is to be hosted, displayed, uploaded, published, transmitted, stored or shared. Intermediaries are also required to remove any content violative of any law for the time being in force as and when brought to their knowledge either through a court order or through a notice by appropriate government or its authorised agency.

In the light of above developments, this study material has been prepared to provide an understanding of AI, Data Protection and cyber security legislations which have direct bearing on the functioning of companies. The study material has been divided into three parts consisting of twenty study lessons. Part-I dealing with Legal & Compliance Perspective consists of Study Lessons 1 to 6, whereas Part-II dealing with Technological perspective consists of Study Lessons 7 to 15.

This study material has been published to aid the students in preparing for the Artificial Intelligence, Data Analytics and Cyber Security – Laws & Practice Elective paper of the CS Professional Programme. It has been prepared to provide basic understanding of some of the Artificial Intelligence, Data Analytics and Cyber Security legislations thereunder, which have a bearing on the conduct of corporate affairs. It is part of the educational kit and takes the students step by step through each phase of preparation stressing key concepts, principle, pointers and procedures.

The legislative changes made upto May 31, 2026 have been incorporated in the study material. In addition to Study Material students are advised to refer to the updations at the Regulator's website, supplements relevant for the subject issued by ICSI and ICSI Journal Chartered Secretary and other publications. Specifically, **students are advised to read "Student Company Secretary" e-Journal which covers regulatory and other relevant developments relating to the subject,** which is available at academic portal *https://www.icsi.edu/student-n/academic-portal/*. In the event of any doubt, students may contact the Directorate of Academics at academics@icsi.edu.

The amendments to law made upto 31st May of the Calendar Year for December Examinations and upto 30th November of the previous Calendar Year for June Examinations shall be applicable.

Although due care has been taken in publishing this study material, the possibility of errors, missions and /or discrepancies cannot be rules out. This publication is released with an understanding that the Institute shall not be responsible for any errors, omissions and/or discrepancies or any action taken in that behalf.

PROFESSIONAL PROGRAMME

Group 1

Elective Paper 4.4

ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

(Max Marks 100)

SYLLABUS

OBJECTIVE

To provide skills of high order regarding digital technological developments in emerging economic environment.

Level of Knowledge : Expert Knowledge

Part I : Legal & Compliance Perspective

1. **Artificial Intelligence ("AI") : Introduction and Basics :** Introduction : Meaning and Definition ● Emergence of AI in modern IT world ● ChatBots and Virtual Assistance: Boon or Bane ● Need and Significance for AI in cyberspace ● Challenges and Opportunities of AI ● AI and Cyber Security ● AI vs. Ethics and Morality ● AI vs. Law and Compliance ● Case Studies
2. **Cyber Security :** Cyber Security ● Cyber Security Techniques ● Challenges and Restrictions ● Cyber Security Policies – National and International ● International Convention on Cyberspace ● Cyber Security: Legal and Compliance Assessment
3. **Cyber Threats and Cyber Laws** : Introduction ● Cyber Threats - Cyber Warfare - Cyber Crime - Cyber Terrorism ● Types of Cyber Threats/ Attacks ● Cyber Threat Hunting and Digital Forensics ● Digital Intellectual Property ● Liability of online platforms ● Laws applicable to AI and Cyber Laws - Information Technology Act, 2000 ● Overview of IT Act, 2000, The important provisions of IT Act, 2000, Positive and negative aspects of IT Act, 2000, Information Technology Rules (IT Rules), Companies Act, 2013, Indian Penal Code, 1860, Cyber security Framework (NCFS), Data Protection and AI: Laws and Regulations
4. **Cyber Crimes and Investigation Procedures** : Computer Forensics and Digital Evidence ● Security Audit
5. **Regulatory Framework on AI, Cyber Security and Cyberspace :** E-Governance in India ● RBI Regulations governing AI, Cyber Security and Cyberspace ● SEBI Regulations governing AI, Cyber Security and Cyberspace ● International Principles governing AI, Cyber Security and Cyberspace ● Other Applicable Regulatory Framework
6. **Data Analytics and Law :** Introduction to Data Analytics ● Introduction to Legal Analytics ● Introduction to Machine Learning for Lawyers ● Quantitative Legal Prediction vis-à-vis Business of Law ● Bias/

Variance, Precision/Recall & Dimensionality ● Overfitting, Underfitting, & Cross-Validation ● Logistic Regression and Maximum Likelihood ● Triple C Theory and Data Assessment ● Network Analysis and Law

Part II : Technological Perspective

7. **Computer Hardware and Software :** An Introduction – Computer System Concept, Types, Categories and Emerging Technologies ● Components of a Computer System ● Primary and Secondary Storage ● Computer Storage Capacities ● Computer Peripherals – Inputs, Output and Storage Devices ● Computer Software: An Introduction ● Software Trends ● Multi-Programming, Multi-Processing, Time Sharing, Batch Processing ● On-Line and Real Time Processing ● Application Software

8. **Network Basics and Security :** Intranets ● Extranets ● Internet ● Networking concepts OSI models TCP/IP model ● Ports ● Secure protocols ● Common Network Attacks ● Network Devices Hubs ● Bridges Switch ● Security Devices ● Firewall

9. **Softwares and Software Security**

10. **Database Management :** Data Base Concepts ● Data Structure ● Data Base Management System ● Data Base Files ● Data Mining and Warehousing

11. **Data Analytics :** Data Recovery Tools ● Data Recovery Procedures and Ethics ● Gathering Evidence Precautions, Preserving and safely handling original media for its admissibility ● Document a Chain of Custody and its importance ● Complete time line analysis of computer files based on file creation, file modification and file access ● Recover Internet Usage Data ● Data Protection and Privacy ● Recover Swap Files/Temporary Files/Cache Files ● Introduction to Encase Forensic Edition, Forensic Toolkit ● Use computer forensics software tools to cross validate findings in computer evidence-related cases

12. **Information Systems :** Systems : An Overview ● Features and Qualities of Information ● Types of Information ● Process of Generating Information ● Value and Cost of Information ● Information Needs a Various Levels of Management ● Factors Influencing Information Needs ● Information System Activities ● Types of Information Systems ● Information Systems in Business Management ● Recent Trends in Information System

13. **Management Information Systems**: **An Overview** : Concept, Evolution and Elements ● Structure ● Computerized MIS ● Approaches of MIS ● Development ● Pre-requisites of an Effective MIS ● MIS and Decision Support Systems ● MIS and Information Resource Management ● Artificial Intelligence and Expert System

14. **Enterprise Resource Management :** ● Understanding Enterprise Resource Planning ● ERP Related Technologies ● Planning Evaluation and Selection of ERP Systems ● Recent Trends in ERP

15. **Internet and Other Technologies** : Applications of Internet ● Internet Protocols ● E-Commerce ● Nature, Types (B2B, B2C, C2C) ● Supply Chain Management ● CRM, Electronic Data Interchange (EDI) ● Electronic Fund Transfers (EFT) ● Digital Currency ● Block Chain Technology ● Payment Portal ● E-Commerce Security – Mobile Commerce ● Bluetooth and Wi-Fi

ARRANGEMENT OF STUDY LESSONS

ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

GROUP 1 • ELECTIVE PAPER 4.4

Part I : Legal & Compliance Perspective

Sl. No.	Lesson Title
1.	Artificial Intelligence ("AI") – Introduction and Basics
2.	Cyber Security
3.	Cyber Threats and Cyber Laws
4.	Cyber Crimes and Investigation Procedures
5.	Regulatory Framework on AI, Cyber Security and Cyberspace
6.	Data Analytics and Law

Part II : Technological Perspective

7.	Computer Hardware and Software
8.	Network Basics and Security
9.	Softwares and Software Security
10.	Database Management
11.	Data Analytics
12.	Information Systems
13.	Management Information Systems – An Overview
14.	Enterprise Resource Management
15.	Internet and Other Technologies

LESSON WISE SUMMARY

ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

PART I : LEGAL & COMPLIANCE PERSPECTIVE

Lesson 1 – Artificial Intelligence ("AI") – Introduction and Basics

This lesson gives a thorough overview of the emergence of the concept of Artificial Intelligence (AI) as a branch of computer science, which is capable of performing operations that normally call for human intellect. It involves discussions on various types of AI, its usage in various sectors, introduction to Chatbots, Virtual Assistance along with challenges and opportunities for AI. It also elaborates upon the use of AI in Cyber security, the effects of AI on ethics and morality and the need for a legal and compliance framework to regulate the AI sector.

Lesson 2 – Cyber Security

This lesson focuses on Cyber Security, its significance and cyber-security techniques that can be used to protect against threats in the cyberspace. This lesson will also discuss the various challenges and restrictions of cybercrime and the various national and international cyber security policies formulated by nations over the world, including the International Convention on Cyberspace. Thereafter, an attempt will be made to look into the legal and regulatory framework concerning cybersecurity and the recent government initiatives in India in the area of cyber security.

Lesson 3 – Cyber Threats and Cyber Laws

This lesson focuses on cyber threats and the various types of cyber threats/ attacks that expose users to vulnerabilities in the cyber space, including web based and system-based attacks. Through the course of this chapter, an attempt will also be made to understand cyber threat hunting investigations and role of digital forensics in preserving digital evidence. Furthermore, this lesson will also trace the methods of protecting digital intellectual property and legal framework on liability of Intermediaries/Online Platforms in India. Important laws applicable to cyberspace and relevant case laws and case studies along with Indian legal perspective on data protection will also be looked into in this Lesson.

Lesson 4 – Cyber Crimes and Investigation Procedures

This lesson discusses cyber-crimes in the Indian scenario, including the various initiatives adopted by the government and investigative authorities to regulate and control cyber-crime in India. An attempt will be made to provide an easy understanding of the process regarding how to report a cyber-crime in India and step-by-step guide as to how the investigation of cyber-crimes takes place in India. This lesson will also elaborate upon concepts of computer forensics and digital evidence and its role in cyber security, chain of custody procedures, security audit, case studies and discussion on the Indian law on Cyber Terrorism.

Lesson 5 – Regulatory Framework on AI, Cyber Security and Cyberspace

This lesson will discuss the concept of e-governance in India along with an overview of the central government projects, state government projects and integrated initiatives on e-governance and digital India. An attempt

will also be made to trace the framework of the RBI as well as SEBI for governing Artificial Intelligence, Cyber Security and Cyber Space along with a look at its implications. This lesson will also give an overview of the international principles governing AI, Cyber Security and Cyber Space.

Lesson 6 – Data Analytics and Law

This lesson is based on data analytics, need and significance of data analytics, its types, processes and the different methods and techniques used by data analysts to effectively analyze the data. Students will also be introduced to the area of legal analytics and how it is implemented to legal practice. Discussion will also be made on machine learning for lawyers and its various uses, benefits, concept of quantitative legal prediction and its use in predicting case outcomes. The lesson will end with a discussion on bias and variance in machine learning and network analysis and law to understand the emerging AI trends in legal sector.

PART II : TECHNOLOGICAL PERSPECTIVE

Lesson 7 – Computer Hardware and Software

In this lesson, an attempt will be made to understand the computer system, its types along with all its constituent elements like hardware, software and liveware. After reading this lesson, students will be able to understand concepts like primary and secondary storage, computer peripherals and multiprogramming. This lesson will also include detailed discussion on software systems, its types, and the recent and emerging software trends.

Lesson 8 – Network Basics and Security

This lesson is aimed at fostering an understanding of network and computer security, with emphasis on understanding the different types of network and its operation. This lesson will further elaborate upon the need and implications of ensuring network security. After reading this lesson, students will get familiar with common threats to network security and measures that can be taken to avoid the same.

Lesson 9 – Softwares and Software Security

This lesson will outline the concept of software, its various types and functioning of software security mechanisms. The Indian legal and regulatory framework on software security will be explored in depth along with analysis of various case laws and case studies in the Indian scenario. The lesson will conclude with a discussion on recent trends in software security, what to avoid in software security and best practices of software security.

Lesson 10 – Database Management

This lesson will explore the concept of database with the basics of data structure, followed by discussion on database abstraction, implementation and creation. An attempt will be made to familiarize the students with database management system, its components, advantages and its applications. Concepts of data mining, warehousing and data base files will also be discussed in detail.

Lesson 11 – Data Analytics

In this lesson, students will learn about data recovery, its tools, procedures, types and data recovery ethics, in the light of data analytics. This will be followed by discussion on gathering evidence for its admissibility in court of law, duplication and preservation of digital evidence, legal aspects of collecting and preserving computer, digital IDs and authentication and importance of chain of custody. Students will be able to understand the different nuances of identification, preservation and analysis of evidence related to data analytics.

Lesson 12 – Information Systems

This lesson will look into the meaning and concept of information system, its application in different spheres of business and the various types of information system along with key features, advantages, disadvantages and function of such information system. This will be followed by a discussion on information systems and security and application of information systems in daily life situations.

Lesson 13 – Management Information Systems – An Overview

This lesson will foster an understanding of the management information system, its components and utilization of management information system in Indian business world. Thereafter, the student will be introduced to the inter-relationship between management information system with other information systems and applications of management information system. The lesson will conclude with a discussion on management information system and security.

Lesson 14 – Enterprise Resource Management

This lesson will delve into the concept and meaning of Enterprise Resource Planning (ERP), its advantages, disadvantages and functioning of ERP systems. This will be followed by discussion on ERP related technologies, ERP system modules, planning, evaluation and selection of ERP systems. The lesson will end with a discussion on recent trends in ERP in 2023.

Lesson 15 – Internet and Other Technologies

This lesson will comprehensively discuss the concept of internet, internet technologies and internet protocols, followed by discussion on e-commerce and its benefits, limitations and development. This lesson will also discuss important concepts of Supply Chain Management, Customer Relationship Management, Electronic Data Interchange, Electronic Fund Transfers. Furthermore, this lesson will contain an elaborate discussion on Digital Currency and its types, block chain technology and payment portals. The lesson will conclude with a discussion on mobile commerce, its types, working, future trends and its comparison with traditional e-commerce.

CONTENTS

PART I : LEGAL & COMPLIANCE PERSPECTIVE

LESSON 1

ARTIFICIAL INTELLIGENCE ("AI") – INTRODUCTION AND BASICS

Introduction	4
Artificial Intelligence: Characteristics	4
Evolution of Artificial Intelligence	5
Examples of Artificial Intelligence	6
Types of Artificial Intelligence	6
The Emergence of Artificial Intelligence in a Modern it World	6
The History of AI	7
Advent of Contemporary AI	7
AI's influence on Modern Society	7
Growth of AI vis-à-vis Indian Vision: Glimpse of Future of India	7
Chatbots and Virtual Assistance: Boon or Bane	10
Latest Trends	12
Need and Significance of AI in Cyberspace	13
AI's requirement in Cyberspace	14
Reduced Revenue	14
In the loop	14
Challenges and Opportunities of AI	16
Increased AI Interest In India	17
Major Challenges	18
Policy Changes Needed	19
AI and Cyber Security	20
Benefits of AI in Cyber Security	21
Disadvantages of AI in Cyber Security	22
AI Versus Ethics & Morality	23
AI Versus Law And Compliance	24
Conclusion	25
AI and Intellectual Property Rights	25

Requirement of Amendment in Laws 27
Transforming India with AI 29
Lesson Round-Up 35
Test Yourself 36
List of Further Readings 36
List of Other References 37

LESSON 2

CYBER SECURITY

Cyber Security 36
Significance of Cyber Security 40
Cyber Security Fundamentals 41
Cyber Security Techniques 42
Challenges and Restrictions 45
Cybercrime as one of the major challenges 45
Snap-Shot of Common Kinds of Cyber-attacks 46
Solution – Confrontation Strategy to Challenges and Limitations 47
Additional Challenges and Limitations: Recent Trends 48
Rise of AI Threats and Cybersecurity: Predictions For 2024 52
Rise of Specialized Language Models 52
Threat Actors will use AI to get ahead 52
Spike in Third-Party Data Breaches 52
Cyber expertise is coming to the Boardroom 53
Managing Third-Party risk to stay resilient 53
Cyber Security Policies - National and International 53
Cyberspace: Boon as well as Bane 53
Requirement of Cyber Security Policies 54
National Cyber Security Policy -2013: A Brief 54
National Cyber Security Strategy: Recent Trends 60
Draft National Cyber Security Strategy 61
National Cyber Security Strategy 2023: Latest Updates 61
Bharat National Cyber Security Exercise 2023: Elevating India's Cybersecurity Preparedness to New Heights 62

Cyber Security Policy: International Standards 62
International Convention on Cyberspace 64
International Convention on Cyberspace: A Brief Timeline 64
Cyber Security: Legal And Compliance Assessment 65
Cyber Security: Legal Assessment 66
Digital Personal Data Protection Act, 2023: New Paradigm of Data Privacy and Compliance 69
Cyber Security: Major Regulating Bodies and Compliance Requirements 73
Cyber Security: Recent Government Initiatives in India 76
Concluding Remarks: Need of the Hour 76
Lesson Round-Up 78
Test Yourself 80
List of Further Readings 80
List of Other References 81

LESSON 3

CYBER THREATS AND CYBER LAWS

Regulatory Framework 84
Introduction 84
Cyber Threats 86
Cyber Warfare 86
Cyber Crime 87
Cyber Terrorism 87
Cyber Terrorism vis-à-vis Cyber Crime 88
Basic elements of Cyber Terrorism 88
Legal Provisions dealing with Cyber terrorism 88
Types of Cyber Threats/ Attacks 89
Web-Based Attacks 90
System-Based Attacks 93
Recent Cybers Threats - 2022 94
Covid-Themed Phishing Attacks 94
Ransomware Attacks 94
Insider Threats 95
Supply Chain Attacks 95
Polyglot Files 95

Distributed Denial of Service (DdoS) Attacks	95
Social Engineering	96
Phishing	96
Malvertising	96
Zero-Day Exploits	96
Cyber Threat Hunting and Digital Forensics	97
Cyber Threat Hunting	97
Threat Hunting Investigations	97
Threat Hunting Techniques	98
Hunting Steps	98
Digital Forensics	99
Digital Intellectual Property	99
Liability of Online Platforms	101
26 Leading E-Commerce Platforms Declare Compliance with Self-Audit to Eliminate Dark Patterns	101
Legal/Regulatory regime of “Intermediary/Online Platform Liability” in India	103
Laws Applicable to AI and Cyber Laws	108
Information Technology Act, 2000 (IT Act, 2000)	108
Information Technology Rules (IT Rules)	110
Proposed Digital India Act: An Act in Progress to replace Information Technology Act, 2000	111
Nine Pillars of Digital India	111
Necessity for Digital India Act (DIA)	111
Need for Digital India Act	111
Salient Features of Proposed Digital India Act	112
Government notifies amendments to Rule 3(1)(d) of the IT Rules, 2021 to enhance transparency, accountability and safeguards	113
Requirement of Industry Alignment towards Goals and Proposed Structure of DIA:	114
Challenges Ahead in the Implementation of DIA, 2023	114
Way Forward for Effective Implementation of DIA, 2023	115
Way Forward	115
Companies Act, 2013	116
Indian Penal Code, 1860	116
Criminal Law is proposed to be replaced from New Legislations	117
Cyber Security Framework (NCFS)	118
Data Protection and AI: Laws And Regulations	118
Artificial Intelligence: Brief Description	119

Evolution 119
AI Methods 120
India and AI 120
Benefits 121
Steps taken by the Government 121
Data Protection: Indian Legal Perspective 122
The Information Technology (Amendment) Act, 2008 126
Personal Data Protection Bill, 2019 - Key Highlights 128
India's Digital Personal Data Protection Act, 2023: Key Provisions 129
Exemptions under the DPDP Act 131
Steps for companies prepare for compliance under the Digital Personal Data Protection Act 131
Global Data Protection Models 132
European Union (Proposed) AI Act, 2024 133
Summary of European Union proposed AI Act 133
Four (4) Point Summary of European Union Proposed AI 134
Governance 135
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 135
Salient Features 137
Other Statutes on Data Protection 140
Lesson Round-Up 142
Test Yourself 144
List of Further Readings 144

LESSON 4

CYBER CRIMES AND INVESTIGATION PROCEDURES

Introduction 146
Overview of Cyber Crimes 146
Cyber crime vis-à-vis Indian scenario 147
India is the 80th most targeted country worldwide in cybercrime: Report 147
Tools and Techniques used to Commit Cyber Crimes 148
Initiatives to Regulate and Control Cyber Crimes: Governmental and Law Enforcement Agencies 149
Central Government Initiative on Strengthening Mechanism to Lever Cyber Crimes 150
Citizen Financial Cyber Fraud Reporting and Management System 151
Reporting of Cyber Crime 151

Process of Reporting A Cyber Crime	152
Work Flow for Reporting a Cyber Crime	153
State Nodal Officer and Grievance Officer	155
Investigation of Cyber Crimes Under Indian Laws	155
Who can investigate?	155
Process of search & arrest	155
Documentation	157
Preservation	157
Examination	158
Presentation	160
Some of the common cyber-crimes of 2023-2024	160
Computer Forensics and Digital Evidence	161
What are Computer Forensics?	161
Use of Computer Forensics	162
Types of Computer Forensics	162
Role of Computer Forensics	163
Computer Forensics vis-a-vis Cyber Security	163
Investigations vide Computer Forensics	163
Digital Forensics - Chain of Custody	167
Significance of maintaining Chain of Custody	167
Security Audit	169
Meaning of Audit	169
Significance of Security Audit	170
Advantages of Security Audit	170
Types of Security Audit	170
Cyber Security Audit: A Snapshot	174
Cyber Attacks in Middle East	176
India and Pakistan Conflict	176
Retribution by China	176
Cyber attack by Tamil Tigers	176
Yugoslavia Conflict	176
Cyber Attack on Estonia	177
Sony PlayStation Network, Microsoft's Xbox Live network case	177
Indian Law & Cyber Terrorism	177
Hacking	180

Here is a short list of great hackers of the world. 180
Lesson Round-Up 183
List of Further Readings 186
List of Other References 186

LESSON 5

REGULATORY FRAMEWORK ON AI, CYBER SECURITY AND CYBERSPACE

E-Governance in India 188
Meaning of e-Governance 188
Evolution of E-Governance 188
Objectives 189
Pillars of e-Governance 189
Types of Interaction in e-Governance 189
Types of interactions in e-Governance 190
Government to Government (G2G) 190
Government to Citizen (G2C) 190
Government to Businesses (G2B) 190
Government to Employees (G2E) 190
National E-governance Plan 190
Central government initiatives as mission mode projects (MMP) 191
State Mission Mode Projects 192
Integrated Mission Mode Projects 193
Recent Initiatives 193
E-Governance/Digital India: Snap Shot of Recent Government Initiatives 197
RBI Regulations governing AI, Cyber Security and Cyberspace 198
Implications of RBI Requirements 203
Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 205
RBI's Updated Master Direction: Navigating the Digital Landscape Safely 206
Thematic Objectives of the New RBI Master Directions: 207
Sebi Regulations Governing AI, Cyber Security and Cyberspace 207
SEBI Cyber Security Guidelines, 2023 – Cyber Security and Cyber Resilience framework for Portfolio Managers 209
Governance 210
Identify 211

Protection 211
Monitoring and Detection 214
Response and Recovery 214
Sharing of information 214
Training 215
Periodic Audit 215
Vendors or Service Providers 215
MeitY Unveils India AI Governance Guidelines under IndiaAI Mission to Ensure Safe, Inclusive, and Responsible Adoption of Artificial Intelligence across Sectors 215
International Principles Governing AI, Cyber Security and Cyberspace: An Overview 216
OECD AI Principles: Overview 216
Other Applicable Regulatory Framework 217
Lesson Round-Up 220
Test Yourself 222
List of Further Readings 222
List of Other References 222

LESSON 6

DATA ANALYTICS AND LAW

Introduction 224
Data Analytics 224
Kinds of Data collected by Company 225
The Evolution of Data Analytics 225
Data Analysis Steps 226
Types of Data Analytics 226
Data Analytics Techniques 227
Data Analytics Tools 227
Introduction to Legal Analytics 228
Legal Data Analytics: Meaning 228
Advantage of Legal Data Analytics: 228
Implementing Data Analytics to Legal Practice: 229
Business of Law Analytics vis-à-vis Practice Law Analytics 229
Practice of Law Analytics 230
Contract Analytics 230
Case Analytics 230

Introduction to Machine Learning for Lawyers	230
Use of Artificial Intelligence and Machine Learning in Law	230
Review Documents and Legal Research	230
Help perform Due Diligence	231
Contract Review and Management	231
Predict Legal Outcomes	231
Legal Research	232
Data Incorporated into Legal Analytics	232
Ways to use Legal Analytics	232
Quantitative Legal Prediction vis-à-vis Business Of Law	234
Overview of Quantitative Legal Prediction (QLP)	234
Applications of Quantitative Legal Prediction	235
Limitations of Quantitative Legal Prediction	237
Using QLP to Predict Court Case Outcomes	238
Using QLP for Profiling Judges and its Rule of Law Implications	239
Bias/ Variance, Precision/Recall & Dimensionality	239
Bias and Variance in Machine Learning	239
Errors in Machine Learning	240
What is Bias?	241
Ways to reduce High Bias:	241
What is a Variance Error?	241
Ways to Reduce High Variance:	242
Different Combinations of Bias-Variance	242
How to identify High variance or High Bias?	243
Trade Offs and Bias	243
Bias-Variance Trade-Off	244
Overfitting, Underfitting, & Cross-Validation	244
Overfitting	245
How to avoid the Overfitting in Model	246
Underfitting	246
Logistic Regression and Maximum Likelihood	247
Logistic Regression in Machine Learning	247
Maximum Likelihood Estimation (MLE)	247
What is the likelihood?	248
Working of Maximum Likelihood Estimation	248

Triple C Theory and Data Assessment 248
Direct Assessment 249
Indirect Assessment 249
Triple C Theory and Data Analysis 249
Network Analysis and Law 250
Examples of Network Analysis and Law 250
Research Case of Network Analysis in Law 251
Future of network analysis in legal history 254
Lesson Round-Up 255
Test Yourself 255
List of Further Readings 256
List of Other References 256

LESSON 7

COMPUTER HARDWARE AND SOFTWARE

An Introduction 262
Computer System: Concept 262
Characteristics of a Computer 263
Categories: Types of Computer System 264
Emerging Technologies 268
Components of Computer System 272
Primary and Secondary Storage 273
Computer Storage Capacities 274
Computer Peripherals – Inputs, Output, and Storage Devices 275
Computer Software : An Introduction 276
Software Trends 278
Multi-Programming 280
Multi-Processing 280
Time Sharing 280
Batch Processing 280
On-Line and Real Time Processing 281
Application Software 282
Lesson Round-Up 283
Test Yourself 285
List of Further Readings 285

List of Other References 285

LESSON 8

NETWORK BASICS AND SECURITY

Introduction 288
Network Security 288
Objectives of Network Security 289
Intranets 289
Extranets 289
Internet 289
Networking Concepts 290
OSI model 290
TCP/IP model (the Internet Protocol Suite) 291
The Internet Protocol Suite 291
Ports 293
Secure Protocols 294
Common Network Attacks 295
Network Devices Hubs 296
Bridges 297
Switch 297
Security Devices 298
Firewall 299
Lesson Round-Up 300
Glossary 301
Test Yourself 302
List of further readings 302

LESSON 9

SOFTWARES AND SOFTWARE SECURITY

Introduction 304
Software-Overview 304
Characteristics Of Good Software 305
Software Classification 305
Application Software 308

Utility Software	308
Other Types of Software on the Basis of Availability and Shareability	308
Software Security	309
Software Security: Overview and Significance	309
Software Security: A Proactive Security	310
Software Security Goals	311
Software Security: Best Practices	311
What to avoid in Software Security?	312
Case Study and Case Laws of Indian Law on Software Security .	313
SAAS; PAAS, IAAS and On-Premise Software: Overview 1Recent Trends	318
IAAS Services	318
IAAS Platform and Architecture	318
Pricing	319
Advantages	319
Typical use Cases	319
IAAS: Storage	320
PAAS	320
Advantages of PAAS	321
Disadvantages of PAAS	321
Use Cases for PAAS	321
Purpose-Built PAAS Types	322
SAAS SERVICES	323
Characteristics of SAAS	323
Advantages of SAAS	324
Future of SAAS	324
On Premise Software	325
Pros and Cons of On-Premise Software	325
Legal and Compliance Requirements of Software Security	325
Lesson Round-Up	328
Glossary	328
Test Yourself	329
List of further readings	329

LESSON 10

DATABASE MANAGEMENT

Database Concepts 332
Purpose of Database 332
Database Abstraction 332
Advantages of Database 334
Disadvantages of Database 334
Data Structure 334
Types of Data Structures 335
Primitive Data Structures 335
Non-Primitive Data Structures 335
Key Features of Data Structures 336
Implementation of Data Structures 336
Database Management System 337
DBMS Architecture 337
DBMS Components 337
Advantages of DBMS 338
Disadvantages of DBMS 339
Database Files 339
Types of Database Files 339
Access and Manipulation of Database Files 340
Data Mining And Warehousing 340
Data Mining 340
Some key characteristics of data mining include 341
Data Warehousing 341
Differences between Data Mining and Data Warehousing 342
Uses of Data Mining and Data Warehousing: 342
Lesson Round-Up 342
Test Yourself 343

LESSON 11

DATA ANALYTICS

Introduction to Data Analytics 346
Process of Data Analytics 346
Data Analytics Types 346
Benefits of Data Analytics 347

Data Recovery Tools	347
Data Recovery Procedures and Ethics	350
Digital Ethics	350
Role of Digital Ethics in Data Storage	351
Data Recovery Ethics	351
Types of Data Recovery	351
Business continuity/disaster recovery (BCDR)	352
Gathering Evidence- Precautions, Preserving and Safely Handling Original Media for its Admissibility	352
Collection Options	353
Obstacles	353
Volatile Evidence	354
Methods of Collection	354
Reconstructing the Attack	355
Searching and Seizing	355
Methodology Development	356
Evidence Search and Seizure	356
Duplication and Preservation of Digital Evidence	357
Preserving the Digital Crime Scene	357
SafeBack	357
SnapBack	357
Computer Evidence Processing Steps	357
Legal Aspects of Collecting and Preserving Computer	359
Forensic Evidence	359
Legal Requirements	359
Evidence Collection Procedure	360
The Incident Coordinator	360
The Incident Coordinator	360
The Evidence Notebook	360
Evidence Collection	361
Computer Image Verification and Authentication	362
Special Needs of Evidential Authentication	362
Digital IDS and Authentication Technology	362
Authenticode	362

Public Key Cryptography	363
Certificate Authorities (CA)	363
Digital ID	363
How Authenticode works with VeriSign Digital IDs?	364
Document a Chain of Custody and its Importance	364
Evidence Collection	364
Evidence Marking and Packaging	365
Chain of Custody	366
Transfer of Evidence to Property Room	367
Some commonly used file systems	368
EXT File Systems	369
What is a file format?	370
Steps in the file system forensics process	370
Acquisition	370
Validation and discrimination	370
Extraction	370
Reconstruction	371
Reporting	371
Recovery of Internet Usage Data	371
Requirements of remote recovery	372
Why is data privacy important?	373
What are some of the challenges users face when protecting their online privacy?	373
What are some of the challenges businesses face when protecting user privacy?	374
Recover Swap Files/Temporary Files/Cache Files	374
Ways to Recover Deleted Temp Files	375
Retrieving deleted files	375
Retrieving cached files	375
Retrieving files in unallocated space	375
Usage of computer forensics software tools to cross-validate findings in computer evidence-related cases	376
Why is computer forensics important?	377
Types of computer forensics	377
How does computer forensics work?	377
Lesson Round-Up	379
Glossary	379

Test Yourself 380
List of Further Readings 380

LESSON 12

INFORMATION SYSTEMS

What is Information System 382
Components of Information System 382
Elements of complete Information System implementation 383
Implementation Plans of Information System 383
How Information System is Useful for Business 384
Transformation of Business through Information System 385
Types of Information System 386
Benefits of an Office Automation System 395
Key features of an Office Automation System 395
Application of Information Systems in Business 396
Information Systems and Security 398
Lesson Round-Up 399
Glossary 399
Test Yourself 400

Lesson 13

Management Information Systems – An Overview

Introduction 402
Evolution of the Concept of Management Information System 403
Objectives of Management Information System 403
Characteristics of Management Information System 404
Advantages of Management Information System 405
Disadvantages of Management Information System 405
Components of Management Information System 406
MIS and Its Functional Subsystems 407
Utilization of Management Information System in Indian Business Scenario 407
Role of Management Information System in Decision Making 408
Management Information System and Other Information Systems 409
Applications of Management Information System 410

Applications of Management Information System in Service Sectors 411
Management Information System and Other Academic Disciplines 412
Management Information System and Security 413
Lesson Round-Up 413
Glossary 414
Test Yourself 415

LESSON 14

ENTERPRISE RESOURCE MANAGEMENT

Enterprise Resource Management: Introduction 418
Understanding Enterprise Resource Planning (ERP) 419
Significance of ERP 419
How ERP Works 419
Before ERP and After ERP 419
Benefits of Enterprise Resource Planning 421
Limitations of Enterprise Resource Planning 423
ERP Related Technologies 424
Type of ERP System Modules 424
Planning Evaluation and Selection of ERP Systems 426
Stage 1 - Plan Requirement 428
Stage 2 - Request For Proposals (RFP) 428
Stage 3 - Solution Evaluation 428
Stage 4 - Contract Negotiation 428
Stage 5 - Selection and Agreement 428
Recent Trends In ERP: 2023 428
Lesson Round-Up 431
Test Yourself 432
List of Further Readings 432
List of Other References 432

LESSON 15

INTERNET AND OTHER TECHNOLOGIES

Applications of Internet 434

Application of Internet: Major Types	434
Example of Application of Internet	435
Internet Protocols	436
Working of Internet Protocol	436
Need of Protocols	436
What is IP Address?	436
Types of Internet Protocol	436
E-Commerce	440
Development of E-commerce	440
Benefits and Limitations of E-Commerce	442
Types of E-Commerce (B2B, B2C, C2C AND C2B)	445
Supply Chain Management	446
Customer Relationship Management (CRM)	448
Electronic Data Interchange (EDI)	449
Electronic Funds Transfer (EFT)	450
Electronic Funds Transfer (EFT): How it works	450
Major Features of Electronic Funds Transfer (EFT)	451
Digital Currency	451
Types of Digital Currencies	451
Advantages and Disadvantages	452
Block Chain Technology	453
Transaction Process	453
Payment Portal	454
Examples of Payment Gateways	455
E-Commerce Security – Mobile Commerce (M-Commerce)	455
Types of M-commerce	456
Working of Mobile Commerce	456
M-commerce vs. E-commerce	456
Future of Mobile Commerce	457
Bluetooth and WI-FI	458
List of Further Readings	461
List of Other References	461
TEST PAPERS	**464**

PART I

LEGAL & COMPLIANCE PERSPECTIVE

Artificial Intelligence ("AI") – Introduction and Basics

Lesson 1

KEY CONCEPTS

■ Artificial Intelligence ■ ChatBots and Virtual Assistants ■ Use of Artificial Intelligence in Cyberspace ■ Challenges in Implementing AI Technologies ■ Legal Trends in India related to Artificial Intelligence

Learning Objectives

To understand:

- The concept of Artificial Intelligence
- And get an idea about basic uses of Artificial Intelligence
- The AI technology with its pros and cons
- The Challenges faced in implementing AI
- And get an idea about recent Legal trends in AI
- The ethical questions related to AI

Lesson Outline

- Introduction
- The Emergence of Artificial Intelligence in a Modern IT World
- ChatBots and Virtual Assistance: Boon or Bane
- Need and Significance of AI in Cyberspace
- Challenges and Opportunities of AI
- AI and Cyber Security
- *AI* v. *Ethics & Morality*
- *AI* v. *Law and Compliance*
- AI and Intellectual Property Laws
- Efforts of Government of India on Artificial Intelligence
- Case Studies
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

INTRODUCTION

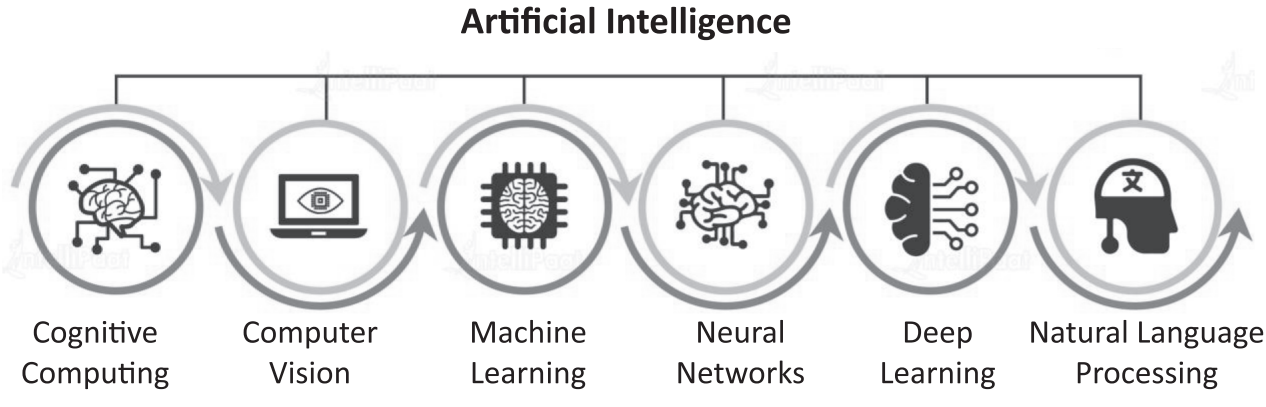
Artificial Intelligence ("AI") is a branch of computer science and engineering that focuses on developing devices and programmes that are capable of carrying out operations that ordinarily call for human intellect, such as comprehending natural language, identifying objects, and forming judgements. As per the Investopedia, Artificial Intelligence (AI) is defined as the simulation of human intelligence by software-coded heuristics. Nowadays this code is prevalent in everything from cloud-based, enterprise applications to consumer apps and even embedded firmware.

Interesting Fact[1]

The year 2022 brought AI into the mainstream through widespread familiarity with applications of Generative Pre-Training Transformer. The most popular application is Open AI's ChatGPT. The widespread fascination with ChatGPT made it synonymous with AI in the minds of most consumers. However, it represents only a small portion of the ways that AI technology is being used today.

Depending on the situation, several interpretations of AI's significance can be made. The capacity of computers to display intelligent behaviour, such as learning, thinking, and problem-solving, is at the heart of Artificial Intelligence (AI). Yet, the technology or environment in which AI is utilised can also have an impact on what it means.

Artificial Intelligence, for instance, pertains to a machine's capacity to comprehend and produce human language in the context of natural language processing. Artificial Intelligence (AI) can also refer to a machine's capacity to comprehend and engage with the physical environment.



Source: https://intellipaat.com

Under this background, this lesson aims to introduce the concept of AI, explore its meaning and definition.

Artificial Intelligence: Characteristics

The goal of Artificial Intelligence (AI), which an interdisciplinary study, is to develop intelligent computers that can carry out activities that ordinarily require human intelligence. AI aims to create robots that can reason, learn, and understand like humans, and that are able to solve challenging issues and adapt to evolving circumstances.

The ideal characteristic of artificial intelligence is its ability to rationalize and take actions that have the best chance of achieving a specific goal. A subset of artificial intelligence is Machine Learning (ML), which refers to the concept that computer programs can automatically learn from and adapt to new data without being

1. Source: https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp

assisted by humans. Deep learning techniques enable this automatic learning through the absorption of huge amounts of unstructured data such as text, images, or video.

Several sectors, including healthcare, banking, transportation, and entertainment, can benefit from the use of AI. For instance, AI-powered autonomous cars can increase transportation safety and efficiency while AI-powered medical imaging technologies can assist doctors in providing more precise diagnoses.

Key Takeaways

- Artificial Intelligence (AI) refers to the simulation or approximation of human intelligence in machines.
- The goals of artificial intelligence include computer-enhanced learning, reasoning, and perception.
- AI is being used today across different industries from finance to healthcare.
- Weak AI tends to be simple and single-task oriented, while strong AI carries on tasks that are more complex and human-like.
- Some critics fear that the extensive use of advanced AI can have a negative effect on society.

In conclusion, artificial intelligence is a fast-expanding topic that entails the creation of computer devices capable of carrying out operations that normally call for human intellect. AI is a fast-developing field that aims to alter how humans live, work and interact with the world around us. AI is intended to be independent and intelligent.

EVOLUTION OF ARTIFICIAL INTELLIGENCE

John McCarthy, the founder of artificial intelligence, provided the original definition of the word in 1955, essentially stating: “The goal of AI is to develop machines that behave as though they were intelligent”.

The science of Artificial Intelligence (AI), which is expanding quickly, is transforming the manner we operate, live, and interact with the environment. The creation of computer systems with Artificial Intelligence (AI) is what allows them to do things like understand language, acquire, organize, solve problems, and make decisions—tasks that would ordinarily need human intellect.

Although the idea of artificial intelligence has been known since the 1950s, it has only recently gained widespread recognition. AI is currently employed in a wide range of industries, from voice assistants like ‘Siri’ and ‘Alexa’ to self-driving automobiles and medical diagnosis, owing to developments in machine learning and deep learning.

The study of Artificial Intelligence (AI) spans a wide range of technologies and methodologies. Building systems that can acquire information and adjust to changing conditions is at the heart of artificial intelligence. A mix of algorithms, data processing methods, and numerical simulations are used to do this.

The fact that AI is built to be independent is one of its fundamental qualities. This implies that AI can make decisions independently of human input. However, the autonomy that gives AI its strength also comes with several grave difficulties. It may be difficult to comprehend why such an AI system committed an error and how to fix it, for instance, if the system makes one.

The fact that AI is clever by design itself is another important feature. This intelligence may manifest itself in a variety of ways, from the capacity to spot data trends to the capacity for deliberation and judgement. Although it is the eventual objective of AI, there is still a long way for development of machines that can replicate human intellect.

A rapid emerging field among technology is AI that is rapidly evolving with each passing day. The potential of AI systems is always growing as new methods and algorithms are created. So, a large increase in the number of AI technologies is to be anticipated in the upcoming years.

Examples of Artificial Intelligence[2]

AI is used in different types of technologies. For example,

- Machine Learning – It helps computers act without the need for programming. There are three types of machine learning.
- Supervised learning – Patterns can be recognized using labeled data sets and then used to label new data sets.
- Unsupervised learning – Data sets can be sorted according to how similar or different they are.
- Reinforcement learning – The AI system is given feedback after actions are performed.
- Automation – Tasks can be enhanced when automation tools are coupled together with AI. Big enterprise jobs can be automated while the intelligence from AI is passed on to process changes.
- Machine Vision – Machine Vision uses a camera, digital signal processing, and analog-to-analog conversion, to capture and then analyze visual information. It is used in signature analysis to medical analysis.
- Self-driving Cars – Automatic vehicles use deep learning, image recognition, and machine vision to make sure the vehicle stays in the proper lane as well as dodges pedestrians.
- Robotics – Robotics is an engineering field that focuses on the designing and manufacturing of robots. Nowadays, Machine Learning is being used to build robots so that they can interact with society.

Types of Artificial Intelligence[3]

There are four types of AI:

Reactive Machines	*Limited Memory*	*Theory of Mind*	*Self-Awareness*
• Simple classification and pattern recognition tasks	• Complex classification tasks	• Understands human reasoning and motives	• Human-level intelligence that can by-pass human intelligence too
• Great when all parameters are known	• Uses historical data to make predictions	• Needs fewer examples to learn because it understands motives	• Sense of self-consciousness
• Can't deal with imperfect information	• Current state of AI	• Next milestone for the evolution of AI	• Does not exist yet

THE EMERGENCE OF ARTIFICIAL INTELLIGENCE IN A MODERN IT WORLD

Although artificial intelligence has been available for a long time now, it has only recently become a significant technical breakthrough in the current IT industry. AI has improved substantially in recent years thanks to

2. Reproduced from https://intellipaat.com/blog/what-is-artificial-intelligence/#no2

3. Reproduced from https://intellipaat.com/blog/what-is-artificial-intelligence/#no2

developments in computing power, storage systems, and algorithmic methods. With the advent of AI in the contemporary IT world, its effects on humanity have handed numerous benefits.

The History of AI

The first attempts to create technologies that could replicate human intellect were made in the 1950s, which is when Artificial Intelligence (AI) was first explored. Rule-based technologies, which were designed with a set of guidelines to carry out particular tasks, were the foundation for initial AI systems. These systems had constrained capacities and were able to carry out the tasks that were specified in their programming.

During 1980s, AI systems started to advance more toward advanced structures like neural networks, which mimic the functioning of the human brain. As a result, innovations in speech processing, language processing, and picture identification occurred, laying the groundwork for current artificial intelligence.

Advent of Contemporary AI

AI has just become a significant technological development in the current IT industry. With the development of datasets, cloud technology, and cutting-edge techniques, AI systems can now analyse vast quantities of data, learn from that, and base recommendations or conclusions on it.

The two primary kinds of AI systems are specific AI and general AI. Narrow AI is created to carry out particular functions, such language translation or picture identification. Contrarily, general AI is intended to be intelligent like humans and to be able to reason and learn in a variety of contexts.

AI's influence on Modern Society

AI's advent has had a big effect on modern society, both for the better and worse. Positively, artificial intelligence has the ability to completely transform a variety of sectors, including healthcare, transportation, and finance. For instance, AI-powered autonomous cars can increase transportation safety and efficiency while AI-powered diagnostic imaging technologies can assist doctors in providing more accurate diagnoses. Concerns exist, nevertheless, on how AI will affect society.

The possibility that AI may displace human labour in many areas, resulting in mass layoffs and economic instability, is one of the main worries. Concerns exist over AI's use in monitoring and command, as well as its potential for unethical uses such militarization or cyberattacks.

Growth of AI vis-à-vis Indian Vision: Glimpse of Future of India

The News article of Ujjal De in ABP Live (March 16, 2023)[4] highlighted the fact that AI is still an integral part of the Union Budget 2023 as it shows the Government's continuous commitment to driving the mission. As India stands has already left China behind to be the most populous country in the world[5], it now holds immense responsibility to decide the future of education, employment, and skill development of nearly one-fifth of the global population. With 65 percent of the population under 35 in contrast to a mostly ageing population of developed countries, India's human capital impact is no longer regional. In the roadmap to becoming the next economic powerhouse and spearheading Industry 4.0 initiatives, the government is taking significant initiatives to rank India at the top of several technological capabilities, including Artificial Intelligence (AI).

AI Announcements in Union Budget 2023

- In 2018, the Government's apex public policy think-tank NITI Aayog proposed the creation of Centers of Excellence (CoEs) for AI learning and development.

4. Reproduced from De Ujjal (March, 2023) Make AI Work For India: What The Future Holds For Artificial Intelligence, ABP Live India.

5. See, https://thewire.in/society/india-china-highest-populated

- The fact that AI is still an integral part of the Union Budget 2023 shows the government’s continuous commitment to driving the mission; the vision is clear: ‘Make AI in India and Make AI work for India,’ as outlined by Finance Minister Nirmala Sitharaman during her Union Budget address.
- Some of the announcements provided a glimpse into the plans for India’s AI implementation:
  - Set up three CoEs in top educational institutions for advanced AI research and development. It can develop next-generation AI solutions and also address the growing talent demand.
  - Increase AI usage and partner with industries for the R&D of scalable solutions in agriculture, health, and sustainable cities. Projects like Digital India BHASHINI and Digi Yatra can be the stepping-stone for large-scale AI implementation across all major sectors.
  - The Government will launch a National Data Governance Policy to enable widespread access to anonymized data and boost innovation for startups and academia.
  - Pradhan Mantri Kaushal Vikas Yojana (PMKVY 4.0) will be upskilling lakhs of youths and aligning courses with industry needs, such as AI, IoT, etc., in the next three years.

Earlier in 2023, Minister of State for Electronics and Information Technology mentioned at the first India Stack Developers Conference that India Stack 1.0 version would evolve and become more sophisticated and nuanced with the integration of the AI layer into the stack.

Increase in AI Usage in Various Sectors

- A comprehensive approach to building cloud infrastructure, 5G connectivity, data centres, and access to quality talent can increase the AI adoption rate.
- Already a leading IT services and offshoring destination, India is making products for global markets and steadily implementing AI solutions to harness the massive volume of domestic data.
- The coronavirus-induced pandemic catapulted the digitalization pace as the larger population embraced digital technologies like UPI (digital payment platform), CoWIN (Covid-19 vaccination portal), and DigiLocker (digital document repository).
- India’s manufacturing sector aims to be a trillion-dollar sector and contribute 25 percent of the national GDP by 2025.
- With a continuous increase in technology spend, AI adoption is gaining momentum in shopfloor automation, predictive maintenance, and reduced wastage.
- The Banking, Financial Services, and Insurance (BFSI) sector is witnessing a rapid digital transformation with the increased demand from the tech-savvy working population.
- With a total banking asset of $2.67 trillion in 2022, India’s key focus is improving the tech infrastructure to enhance customer experience. With an initial implementation in payments and wallets, AI solutions are making their mark in digital lending, insurance, and investment processes.
- The retail sector in India contributes to 10 percent of the country’s GDP and 8 percent of employment. Improved digital connectivity has aided e-commerce to trigger a surge in consumption in cities and rural areas. The FMCG sector is growing at a CAGR of 14.9 percent to reach $220 billion by 2025, and more and more brands are focusing on digital advertising to increase their consumer base.
- AI solutions are at the forefront of data-driven analysis and decision-making like demand forecasting and marketing spend optimization.
- The healthcare market has grown three-fold at a CAGR of 22 percent between 2016–22 and is one of the largest employers in India. Rising income levels and the post-pandemic shift toward preventive healthcare have increased investment in high-end health tech products and facilities.

- Organizations are exploring viable use cases through PoCs in cutting-edge healthcare technologies ranging from remote diagnostics, robotic surgeries and preventive analytics.
- Tech giants like Google and Microsoft heavily invest in AI research and development in India.
- Google Research India Lab is working on the ethical implementation of AI to transform healthcare, agriculture, wildlife conservation, and education. It also implements machine learning (ML) solutions to understand multilingual and multicultural nuances and improve Google’s apps and services like search, assistant, and payment.
- Besides the data-intensive core sectors, AI is gaining a prominent foothold in digital-first sectors like telecom, tourism, education, digital media, and entertainment.
- Microsoft India Development Center (MSIDC) is also working on various projects ranging from theory to advances in large-scale AI models. Project Jigsaw deals with large pre-trained language models such as GPT-3, and Project LITMUS discovering strategies to evaluate massive multilingual models are some projects initiated in the last few years.

Future of AI in India

An IDC report projected India’s AI market to reach $7.8 billion by 2025, growing at a CAGR of 20.2 percent. Organizations will invest in AI solutions across functions like customer service, HR, IT automation, security, etc.

India has already built an edge in AI talent. The latest NASSCOM report ranks India first in terms of AI skill penetration and also in AI talent concentration globally. The rich and massive digital talent pool is rapidly upskilling for AI and catering to the talent demand in India and overseas.

Despite the government’s ongoing skilling initiatives and development of the infrastructural framework, the NASSCOM AI Adoption Index 2022 positions India in the middle of the maturity scale, revealing the need for enterprises to scale up their AI initiatives significantly.

Organizations should embed their AI strategy with the broader corporate strategy and invest more in developing data standards and building dedicated AI teams.

The emergence of platform-agnostic AI solutions delivered on-demand over the cloud is helping organizations reduce deployment and maintenance costs, scale AI projects, and witness sustaining business outcomes. Implementing regulatory policies that ensure data protection, continuous government support, and a high concentration of qualified talent puts India in a unique position to expand its AI ecosystem and become the global leader.

Concluding Remarks

AI’s future holds both promise and uncertainty. AI has the ability to change a variety of societal spheres, including healthcare, academics, and entertainment. Yet there are additional obstacles to be addressed, such moral dilemmas, security issues, and legal problems.

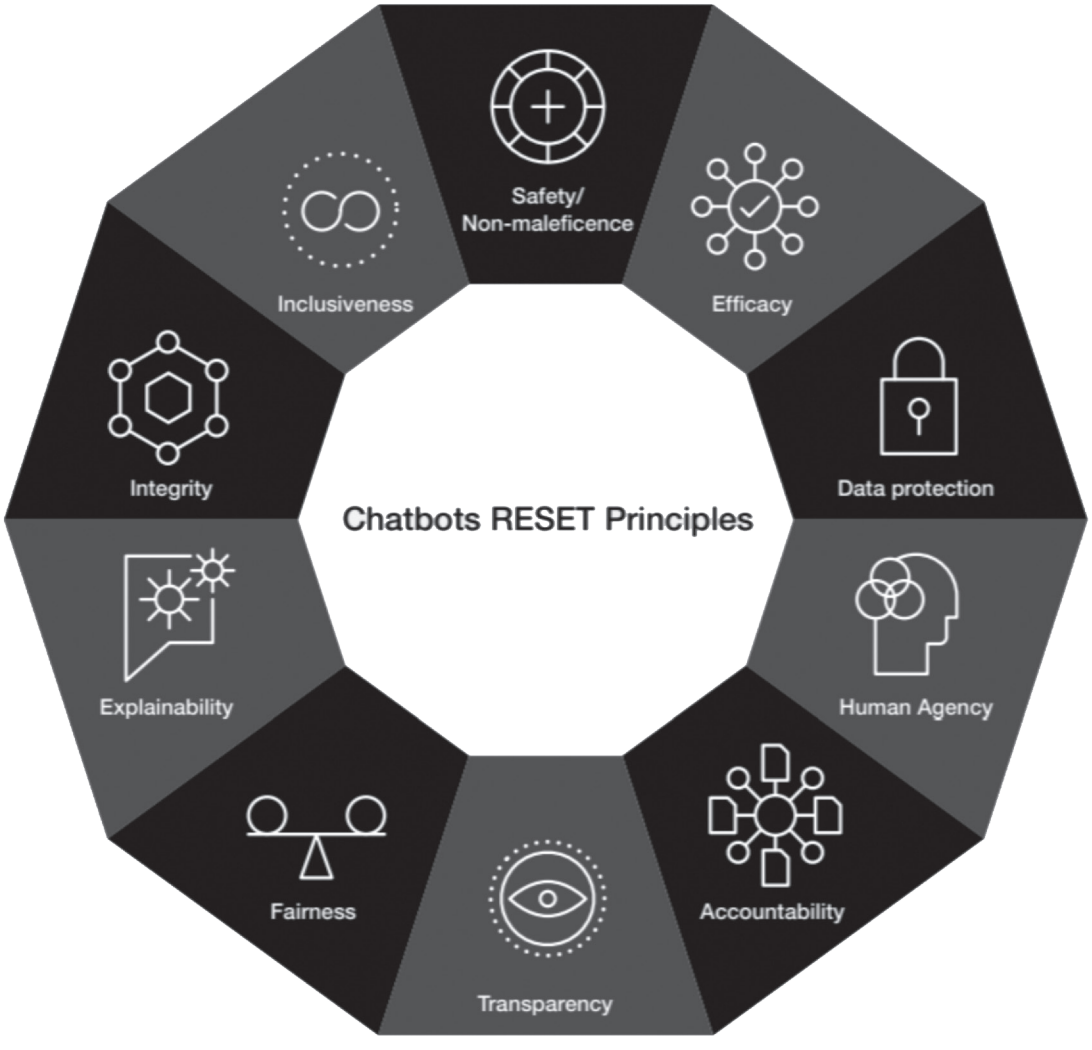
The creation of general AI, which has the potential to outperform human intellect and resolve challenging issues across several disciplines, is one of the major fields of AI study. Yet there are also worries about the dangers of developing highly intelligent AI, which, if not adequately controlled, may endanger human survival.

However, the growth of AI in today’s IT industry is a big one that has the potential to change a lot of facets of mankind. The hazards must be properly managed, though, in order to guarantee that AI is created in a competent, moral, and responsible way.

CHATBOTS AND VIRTUAL ASSISTANCE: BOON OR BANE[6]

Virtual Assistant, referred to as an AI assistant, is one that can recognize natural language audio instructions and carry out the user's requests to fulfill and accomplish tasks. Previously, a personal assistant or secretary would handle activities including taking dictation, reading aloud email or text messages, searching up phone numbers, organizing, making phone calls, and alerting the user of scheduled appointments. Nowadays, Google Assistant, Apple's Siri, Amazon Alexa, and Microsoft's Cortana are some of the most well-known virtual assistants.

On the other hand, a chatbot is a software package that mimics human conversation using text or voice inputs. It can provide customer support, carry out activities automatically, or even sell goods. Despite the fact that chatbots have been around for a while, current developments in Artificial Intelligence (AI) have made them more realistic and valuable than before. During the last few years, there has been a significant surge in the adoption of chatbots online and many businesses are using them every day.



Source: World Economic Forum

6. Source: Sinha Smita (2018) Is Chatbot a Boon or Bane? Here's why Companies Are Using Them Despite Tech Gliches. Analyticsindiamag.com

Chatbots as well as Virtual Assistants which were previously considered as cutting-edge innovation/ technology - are now commonplace for businesses. Over fifty thousand known chatbots are available in the marketplace and the majority of them focus on consumers, while just a tiny subset of these serves business purposes. According to recent patterns, the perception of chatbots and virtual assistants being backed by artificial intelligence as viable professional solutions might improve engagements at the company level and help the businesses to expand.

Advantages of Using ChatBots and Virtual Assistance:

- **Minimizing Operational Expenses:** Responding to consumer inquiries is a substantial expense for e-commerce companies because they need to employ, train as well as pay customer service personnel. According to a data analysis, chatbots and virtual assistance could lower a company’s operating costs by up to thirty per cent.
- **Time Saving:** Customers’ questions can be answered by such technologies by using datasets. They are capable of handling data more accurately thanks to their clever algorithms and programmes. Time that would otherwise be wasted is greatly reduced and productivity increases. Like for example, when selecting an applicant from a huge pool of applications, bots may be used to screen the prospects by posing pertinent questions.
- **Minimizing Error:** Chatbots and Virtual Assistants do not have the same tendency to overlook information as people do. Hence, the chance of someone committing a mistake is eliminated. Also, the quick response time and accurate responses increase client satisfaction to a greater extent. As a result, businesses may use such technologies to perform various human activities and accordingly, the personnel who might typically be hired for duties involving customer support might be assigned other crucial jobs.
- **24X7 Availability:** Chatbots and Virtual Assistants may be utilized anytime to offer customer support online and they do not take time off unlike humans. Users won’t have to wait for assistance when they browse on the internet or visit a particular website. Visitors can ask the virtual assistant/ bots for assistance to find the solutions on their own respective devices or online. Thus, one of the finest client engagement methods is to have a chatbot deployed on your website. According to statistics, sixty-four per cent of web users concur that a Chabot’s’ 24X7 availability is their greatest advantage.
- **Higher Conversion Rate:** According to estimates, nearly thirty-seven per cent of web users consult a user support bot to receive answers to urgent questions. Chatbots can help any website convert more visitors by promptly and effectively responding to their questions.
- **Increases Customer Satisfaction:** Customers frequently find information systems to be extensive and complicated to effectively answer their questions. Chatbots can be used to resolve this. They can handle heavy traffic while still offering reliable service. Moreover, they guarantee a positive customer interaction and contentment. So, this considerably increases customer satisfaction and minimizes discontent. According to studies, businesses that maintain their consumers’ interest in them might increase overall revenues. Incorporating chatbots on the website and incorporating them into well-known networking sites may communicate with the visitors and increase conversion rates.
- **Finding Promising Clients:** Chatbots can help any business achieve its primary objective of creating plenty of prospects and converting them into clients. One may get the chatbots to deliver the qualified leads by using smart qualifying criteria. This might subsequently speed up the sales process of any business.

Latest Trends

The overwhelming majority of internet users wish to connect with brands/businesses. It is due to the fact that a quick and simpler solution is available this way. Utilizing chatbots allows businesses to reach a wider range of consumers while also staying up to date with current developments.

- **Enhanced Client Support**

  There are several ways by which virtual assistants and chatbots may enhance customer service. The best method to provide the consumers the assistance they need while purchasing something is to act as a live marketing advisor. Nearly eighty-three per cent of potential online shoppers want answers to their questions regarding money, shipping, etc. answered as they browse through the website. Moreover, the virtual assistants also help the customer/user in finding the desired result without the hassle of going through a large database of information.

- Also, as previously indicated, providing round-the-clock services without making any customers wait in line is the basic objective. They also improve customer service by engaging with consumers whenever they want to regarding any problem. This enhances a consumer's perception of any business or brand.
- The benefits of such technology outweigh any technological flaws, making such tech the prevailing trends that are also anticipated to last a long time. As a result, companies are using them more and more for diverse reasons.
- Nowadays, extremely interactive and context-aware AI tools may be created by utilizing massive datasets and substantial training. These technologies can even recollect consumer behavior and associated information from prior discussions and apply those observations to appropriately handle client inquiries.
- The knowledge may also be improved and organized to make it more bot-friendly. It will allow the AI to analyze the information effectively and find the best answers according to the client's demand. Also, such technologies can be trained to speak to the clients effectively. One may even think about instructing it to exhibit emotions if needed during a conversation.

Demerits of Using ChatBots and Virtual Assistance:

The technological resources currently available are insufficient to create a Chatbot that can manage complicated questions. There has never been a chatbot that has achieved complete recognition. Following are some drawbacks of chatbots:

- **Information is Less Secure**

  Chatbot security isn't very good. They can allow hackers entry to any company's network, user information, datasets, and apps through their interface. Hence, businesses utilising chatbots must think about issues including the lifetime of the data and how it is preserved, utilized, and who has access to it. For industries like banking and finance that handle highly confidential customer data, it is indeed crucial that some precaution must be taken.

- **Restricted Pre-Programmed Responses**

  Chatbots can only respond to clients with replies from a small array of databases. However, not all clients will find their questions resolved by using these. Also, considering they don't always grasp what is being requested, interactions could get tedious for consumers if they go round in loops. The initial investment would be significant if someone chooses a smart bot with a sizable dataset.

- **Apparent Incapability to Determine**

  Chatbots are unable to make judgements the same way that people do. Your chatbot might not be

able to handle the issue raised by the consumer if your knowledge base doesn’t have the solutions to their questions. In order to make your content chatbot-friendly, one must organize and expand it. It will make it possible for the bot to scan the information efficiently and find the best answers to each customer’s requirements. Also, one must prepare it so that it can interact well with the customers.

- **AI/ChatBots/Virtual Assistance Lack Emotions**

  To communicate effectively, emotions are necessary. Bots may be exceedingly impersonal and devoid of sentiments, in contrast to humans. These can manage client queries according to predetermined discussions only if the interaction flow follows the path provided. Yet, if a subject suddenly changes, they could become perplexed & find it difficult to respond. Also, because they lack sentiments and impulses, they sometimes find it difficult to interact positively with people.

Concluding Remarks

Notwithstanding their flaws, chatbots are being used by organizations and institutions all over the world on an increasing basis. The reason for this is because their benefits exceed their drawbacks. Indeed, bots and AI assistants are a future trend. They are still in their development stage and have not yet reached their entire capabilities, but due to their increasing use by organizations, they belong in this technological age. In the upcoming years, improvements in machine learning and artificial intelligence will contribute to furthering the innovation and technology. Businesses will use it more frequently as a result to keep their focus on the client.

For business owners to effectively manage their customer service and marketing practices, bots may be a huge help. These technologies must be taken with caution because just like any other technology, these also have certain drawbacks. Before selecting if a chatbot is right for the business, owners must investigate all of the alternates available. Effective chatbot deployments can offer significant insights into what functions and what does not while using chatbots. Chatbots may be a potent tool for entrepreneurs to keep one step ahead of the other competitors while deploying the correct strategy. Organizations may save resource and money by automating particular operations while providing clients with the ease of round-the-clock access.

There are a few significant downsides to adopting chatbots, like user privacy issues or the possibility for AI algorithms to malfunction, it is crucial to balance the benefits and drawbacks when thinking about such technologies. Chatbots may be highly advantageous to any organisation across a wide range of sectors when used with caution and in accordance with highest ability for ethical database processing. Making sure that chatbots and virtual assistants are utilised in a responsible and ethical way requires taking a careful strategy to their creation and execution.

NEED AND SIGNIFICANCE OF AI IN CYBERSPACE[7]

Artificial Intelligence (AI) is a branch of computer science where a machine is made capable of possessing human decision-making ability, based on certain unique algorithms and related mathematical calculations. On the other side, Cyber Security consists of security measures to protect the virtual world from cyber-attacks and threats. Artificial Intelligence is capable of securing and cleaning up the cyberspace by taking security measures related to accurate algorithms and mathematical calculations. With an increase in the role of AI in modern world threat to cybersecurity has become a serious issue.

AI is vital for the management of cyberspace, which includes all digital networks, devices, and information systems. AI in this world has emerged as a crucial component. The amount of information stored in the online world is exploding, making it impossible to manage and secure cyberspace using conventional methods. AI is a useful tool for managing the intricacy of cyberspace and the risks that are continuously changing because of its capacity to understand and adjust in real-time. The importance and necessity of AI in cyberspace are covered in this chapter.

7. Source: https://www.geeksforgeeks.org/significance-of-artificial-intelligence-in-cyber-security/

AI's requirement in Cyberspace

Although the web has become an essential component of modern life, the number of digital risks has also skyrocketed along with its use. Threats on people, companies and governments are conducted by cybercriminals using highly technical tools and methods. In order to defend against all of these attacks, standard security methods like firewalls, antivirus software, and systems for detecting intrusions are no longer effective. AI can help in this situation. Massive volumes of data may be analysed in real-time by AI systems to swiftly identify and address dangers.

Recent Example of Cyber Attacks

PT Jyothi Datta (March 27, 2023)[8] has reported a recent incidents of security breaches in many companies. It is reported – "*over three weeks after being hit by an information technology (IT) security breach, drugmaker Sun Pharmaceutical Industries said its business operations have been impacted following the incident and efforts to contain and redress the situation. It also said that revenues would be reduced in some businesses as a result.*

A ransomware group has claimed responsibility for the incident, Sun Pharma disclosed to the stock exchanges, without divulging the name of the group or outlining the quantum of impact. This is the third high-profile cyber-security linked incident on a large Indian drugmaker in about three years. In late 2020, Dr. Reddy's Laboratories and Lupin reported cyber-security breaches. Last year, the All-India Institute of Medical Sciences was also hit by a ransomware attack.

While no information has been shared on the region from where the online attack was possibly launched or the precise data that may have been breached, Sun Pharma[9] said the incident's effect includes a breach of certain file systems and the theft of certain company data and personal data."

Reduced Revenue

As part of containment measures, Sun said, it had "proactively" isolated its network and initiated the recovery process. "As a result of these measures, Company's business operations have been impacted.

Consequently, revenues are expected to be reduced in some of our businesses," it added.

"The Company would incur expenses in connection with the incident and the remediation. The Company is currently unable to determine other potential adverse impacts of the incident, including but not limited to additional information security incidents, increased costs to maintain insurance coverage, the diversion of management and employee time or the possibility of litigation," Sun Pharma said.

In the loop

A media channel named ransomware group ALPHV as the alleged actor behind the attack, and threatening more damage. This has not been confirmed from any other quarter. Ransomware groups hold an organization's data for ransom, seeking a payment, for instance, to withdraw its threat and give the organization access to its own data.

Former Maharashtra Director General of Police (DGP) and former Commissioner of Police (Mumbai) told businessline, that local law enforcement authorities need to be in the loop at the earliest. Companies have to step up their defense to prevent data from being contaminated or frozen for ransom, he said, because "once a company becomes a victim, it becomes difficult for (the) cops to identify the international criminal and later

8. Reproduced from PT Jyothi Datta (2023), Security Breach Ransomware Attack: Sun Pharma says business operations impacted, The Hindu Business lines. Available at: https://www.thehindubusinessline.com/companies/ransomware-attack-sun-pharma-says-business-operations-impacted/article66667349.ece

9. Sun Pharma eyes revenue hit due to ransomware attack (March 27, 2023), The Economic Times. Available at https://economictimes.indiatimes.com/industry/healthcare/biotech/pharmaceuticals/sun-pharma-eyes-revenue-hit-due-to-ransomware-attack/articleshow/99023464.cms

follow it up with MLAT process (Mutual Legal Assistance Treaty),” which would involve the Ministry of External Affairs having to get in touch with authorities in the country from where the attack had been launched.

According to IBM Security’s annual X-Force Threat Intelligence Index report (2023), ransomware attacks persisted, despite better detection. Besides, it added, Asia saw more cyberattacks than any other region, accounting for nearly one-third of all attacks that X-Force responded to in 2022. “Manufacturing accounted for nearly half of all cases observed in Asia last year,” the report said.

Organizations operating online can benefit from AI in the following ways:

- **Detection of Threats**

  In order to find abnormalities and possible risks, AI can scan huge amounts of data, including network activity, records, and system events. AI-powered platforms are very good at spotting and stopping assaults because they can continually adapt to new risks and learn from prior ones.

- **Automation in Cybersecurity**

  Several cybersecurity jobs, including incident management, threat hunting and security screening, may be automated by AI. Businesses may use this automation to speed up reaction times, increase precision, and remove unnecessary security staff to focus on more difficult duties.

- **Statistical Analysis**

  To identify possible cyber dangers, AI may evaluate data from a variety of domains, particularly social networking sites. This makes it possible for companies to take preventive steps to stop assaults before they happen.

- **Detecting fraud**

  By examining huge databases to find abnormal behaviour patterns and abnormalities, AI may assist businesses in identifying and preventing fraud.

- **Usefulness of AI in the Current Digital World**

  It is impossible to exaggerate the importance of AI in the digital world. AI-powered technologies are becoming into crucial tools for businesses to secure their online resources as the quantity and complexity of cyber threats rise.

Some important advantages of AI in cyberspace include:

- **Better and Quick Reaction Times**

  Real-time data analysis and fast response to threats are capabilities of AI systems. As a result, organizations have more time to control the assault and limit additional harm since the reaction period is shorter.

- **Enhanced Accuracy**

  Systems using artificial intelligence (AI) can evaluate enormous volumes of data and spot possible hazards that conventional analysts would miss. This lessens the possibility of both false positives and false negatives and enhances the security monitoring precision.

- **Scalability**

  Artificial Intelligence technologies can tackle complicated tasks and expand quickly to evaluate enormous datasets. They are therefore perfect for handling the massive volumes of data generated by the internet.

- **Ongoing Development**

  Artificial Intelligence systems have the capacity to memorise from the past and constantly acclimatize to new dangers. They can thus effectively handle the continuously changing risks in cyberspace.

Concluding Remarks

AI is an effective tool for controlling cyberspace, which is ever more complicated and challenging to control. AI is capable of promptly identifying dangers and taking appropriate action because of its capacity to evaluate massive volumes of datasets in real-time and gain insight from previous experiences. AI-powered systems will become crucial tools for enterprises as cyber threats develop further.

CHALLENGES AND OPPORTUNITIES OF AI

One of the most significant technical developments of the twenty-first century has been Artificial Intelligence (AI), which has transformed the way people live, work, and connect. AI has shown that it has the ability to automate repetitive jobs, solve complicated issues, and enhance decision-making in a variety of circumstances. To ensure AI’s safe and ethical development and deployment, there are a number of issues that must be resolved, just like with any other technical advance.

Bias and Discrimination: The possibility for prejudice and discrimination is one of the biggest problems with artificial intelligence. Because AI algorithms can only be as objective as the data they are trained on, biased data will result in biased algorithms. This may result in prejudice towards people on the basis of things like colour, gender, religion, and age, among other things. If left uncontrolled, this might result in widespread prejudice and strengthen already-existing societal injustices.

Transparency: Lack of openness and ability to explain is yet another difficulty with artificial intelligence. The majority of AI algorithms are complicated, making it difficult to comprehend how they make judgments. This lack of openness may breed mistrust and uncertainty, especially when the decision made by the algorithm has major ramifications. Transparency and comprehensibility in AI systems are crucial for ensuring the ethical and safe research and application of AI.

Concerns regarding Security and Safety: Artificial Intelligence systems have the potential to have severe negative effects, especially if they break down or are compromised. This can involve causing bodily harm to people, as in the instance of manufacturing robots or driverless automobiles, or causing harm to systems, as in the case of cyberattacks. Thus, it is crucial to ensure the safety and security such technologies, especially as these systems grow increasingly embedded into our everyday lives.

Displacement of Jobs: When AI develops, it will be able to perform numerous activities in lieu of humans, which would cause redundancy and societal unrest. This can have a significantly negative impact on employees in some sectors, such the industrial sector, and worsen already existing socioeconomic imbalances.

Privacy: With AI, data collection, gathering a lot of personal information if ends up being in the possession of some unwanted person/hacker, it might be misused. Hence, protecting the security and privacy of sensitive data is essential for the ethical creation and utilization of AI.

The field of Artificial Intelligence (AI), which is quickly expanding, is changing a wide range of sectors and facets of our life. AI offers a wide range of options, and those prospects are only growing as technology develops. We will examine some of the most significant prospects that AI offer in this chapter.

Automation of Work: Automation of chores is one of AI’s most important potential benefits. Large database processing and other activities that would take humans a very long time to accomplish can be handled by AI systems. This can allow people to concentrate on harder activities that demand more innovation and judgment.

AI may streamline the examination of medical information, for instance, in the healthcare sector, freeing up professionals to devote more time with patients. Artificial Intelligence (AI) may be utilised in the industrial sector to streamline operations like quality checks, lowering the likelihood of a human inaccuracy and boosting productivity.

Personalization: The potential to customise products and offerings is yet another advantage AI offers. In order to offer personalised suggestions and insights, AI systems may examine data on consumer behaviour and preferences.

For instance, AI may be utilised in the e-commerce sector to offer clients individualised product suggestions depending on their browsing and purchasing activity. AI may be utilised in the healthcare sector to create individualised treatment regimens for individuals based on their unique traits and medical histories.

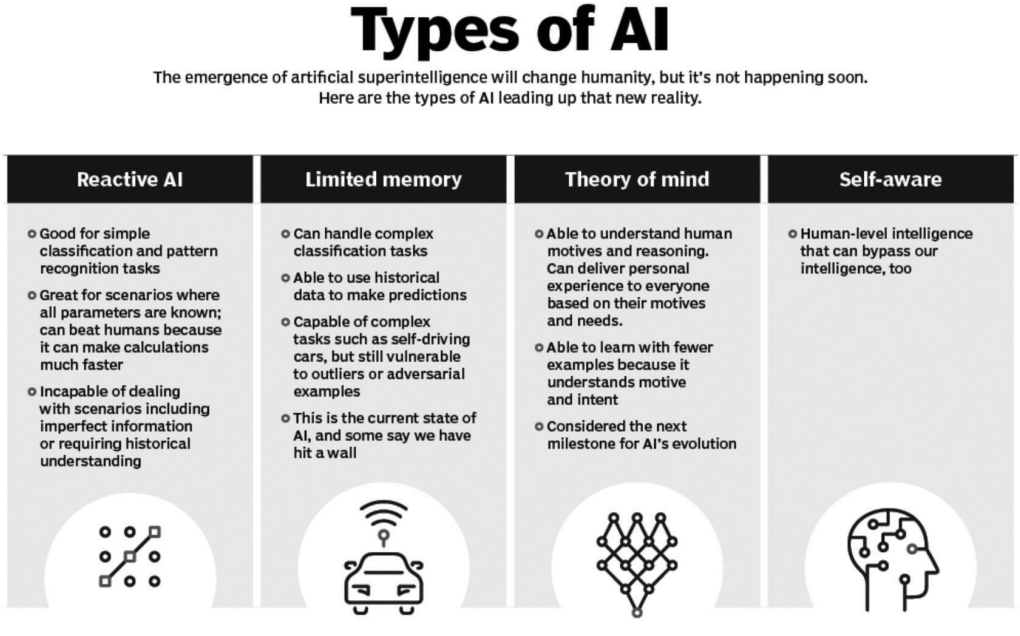
Making better decisions: AI may be applied to numerous businesses to enhance decision-making. In order to find patterns and forecast outcomes, AI systems can analyse vast volumes of data, allowing businesses and organisations to make better decisions.

AI may be utilised, for instance, in the commercial sector to assess market patterns and offer investment suggestions. AI may be used to the shipping sector to improve logistics and route optimization.

INCREASED AI INTEREST IN INDIA[10]

In India today, "Artificial Intelligence" has become the new wave, and everyone wants in. Every engineer claims some type of machine learning project on resume. The ubiquitous library management system, a software development project has now been replaced by a project to automatically recognizing handwriting.

A cottage industry of training courses in AI, machine learning, and data science has blossomed throughout the country. Most businesses have a top-down mandate to incorporate AI in their processes and product.



Source: Davit Peterson and Techtarget

10. Reproduced from Opportunities and Challenges for Artificial Intelligence in India, IT Articles, IASTOPPERS. Available at https://www.iastoppers.com/articles/opportunities-and-challenges-for-artificial-intelligence-in-india-mains-article

Although AI attention is considerably slighter in India than in China or the USA, the increased AI interest has manifested itself in the following three ways:

- Industries have started working to skill their manpower to enable themselves to compete with other global players.
- Educational institutions have started working on their curricula to include courses on machine learning and other relevant areas.
- Individuals and professionals have started acquiring these skills and are comfortable investing in upgrading their own skills.

Major Challenges

- Fundamental challenges: India has a relatively small body of researchers and research output in the field of machine learning.
- The contribution of Indian researchers to top AI conferences constitutes one-fifteenth of the U.S. contribution and one-tenth of that of China.
- India has little local expertise in the new knowledge that is being created every day by others. India do not have people who can train a new cohort of machine-learning engineers and scientists to develop and commercialize technology.
- Despite the opportunities for the present and future, Indian companies have been slow to adopt AI.
- India does not possess enough trained manpower to apply machine learning to our own problems and data, in spite of the number of standard packages available.
- Despite the initial enthusiasm for AI, there were unfulfilled potential and that the country could be doing far more to adopt and integrate AI technologies.
- The cost of failure is much higher in India than the West. This has historically meant a lack of room for innovative experimentation.
- Lack of Collaboration between Industry and Academia: The boom in the Indian IT services sector in the early 90s was partially born out of necessity – India just did not have a good “products ecosystem”.
- India has historically not done well with products, there also seems to be a dearth of good talent specifically for design and user-interface functions.
- Talent will be the biggest strength for India with respect to AI. But AI is still new, so current talent in the market is very limited.
- Some challenges that the progress of AI in India faces is limited availability of manpower and of good quality and clean data, as there is no institutional mechanism to maintain high quality data.
- The country’s diversity and complexity present a rich set of challenging problems for artificial intelligence.
- Current AI techniques are limited in their ability to handle complexity, and they’ll have to mature to deal with the diversity of life in India.

Challenges are concentrated across common themes of:

- Lack of enabling data ecosystems.
- Low intensity of AI research (i) Core research in fundamental technologies; (ii) Transforming core research into market applications.

- Inadequate availability of AI expertise, manpower and skilling opportunities.
- High resource cost and low awareness for adopting AI in business processes.
- Unclear privacy, security and ethical regulations.
- Unattractive Intellectual Property regime to incentivize research and adoption of AI.

Opportunities

- India forms the IT backbone of the world. The country’s companies and talent are the natural contenders to add ‘intelligence’ to all the digitization.
- Investment in India can help move the whole field ahead.

Indian Services Sector

- India’s services sector (call centers, BPOs, etc. – roughly 18% of the Indian GDP) have a significant potential opportunity to cater to the coming demand for data cleaning and human-augmented AI training (data labelling, search engine training, content moderation, etc.).

Space and Defense Research

- India’s Department of Science and Technology could hire program managers to frame hypotheses around problems that could be solved using AI, and then fund research programs for these problems through grants.
- Researchers could bid for these grants in open competition by devising a variety of approaches and solutions to the research problem.
- This would help create large useful labelled data sets and the technology needed for India. Students who work on these projects will naturally go on to create startups around them.
- Government should do impact evaluation for the technologies created and select worth ones for implementation.
- India’s space and defense research organizations could enact similar programs involving the AI research community to develop solutions for them.

Policy Changes Needed

Need for legal definition of AI

- Given the importance of intention in India’s criminal law jurisprudence, it is essential to establish the legal personality of AI (which means AI will have a bundle of rights and obligations).
- To answer the question on liability, a strict liability scheme that holds the producer or manufacturer of the product liable for harm, regardless of the fault, might be an approach to consider.
- Since privacy is a fundamental right, certain rules to regulate the usage of data possessed by an AI entity should be framed as part of the Personal Data Protection laws in India.

Data Protection Law

- A data protection law is needed which aims to give more security to consumers of technology.
- Law provides for the processing of personal data, including digital media, by either a natural person or a public or private legal entity, for the purpose of protecting a person’s fundamental rights of freedom, privacy, and free development of personality.

Trade Negotiations

- Trade and Development agreement to work together to harness the power of cutting-edge technologies such as AI and blockchain to enhance and improve trade.
- With the growing complexity of international trade agreements, the purpose of the use of AI is to reduce such complexity and help representatives of less favored nations achieve better results.

Fraud Detection

- The idea is to develop a system to help customs officers identify suspicious customs operations, and to develop a product and foreign exporter information system to help importers in the registration and classification of their products and corresponding exporters.

Criminal Investigation

- The investment is geared towards data science and AI to collect, store, and analyze large volumes of information.
- The system allows information from different sources and bodies to be collected and also allows a series of real-time data to be collected from suspected criminals.

Way Forward

- As with any major advancement in technology, it brings with it a spectrum of opportunities as well as challenges. On one hand, several applications have been developed or under development with potential to improve the quality of life significantly.
- Artificial Intelligence (AI) is likely to transform the way we live and work. Due to its high potential, its adoption is being treated as the fourth industrial revolution.

Concluding Remarks

Currently, most of the traction in India is in the form of AI pilot projects from the government in agriculture and healthcare, and the emergence of AI startups in cities like Bangalore and Hyderabad. Though these are indications of grassroots level AI adoption, the pace of innovation isn't comparable to the USA or China today.

AI AND CYBER SECURITY[11]

In this age, cyber security has grown to be a big challenge. Database breach, identity theft, captcha cracking and various issues frequently harm countless individuals as well as corporations. Devising the proper rules and methodologies and putting them into practice with exacting accuracy to combat cyberattacks and cybercrimes remains an on-going challenge. Recent advances in artificial intelligence have significantly increased the danger of such attacks along with other activities. It has been used in practically all branches of science and research. AI has sparked a transformation in fields ranging from robotics to healthcare.

By incorporating AI into cyberspace, the potentially evolving cyber security threat that faces multinational corporations could be minimized. As processing power, storage capacities and database collecting expand, machine learning and artificial intelligence are integrated more broadly across sectors than at any other time recently. Humans can't process this much information in a sequential manner. Using machine learning and AI, this data surge might be reduced in a short amount of time, assisting the organization in recognizing and addressing the security concern.

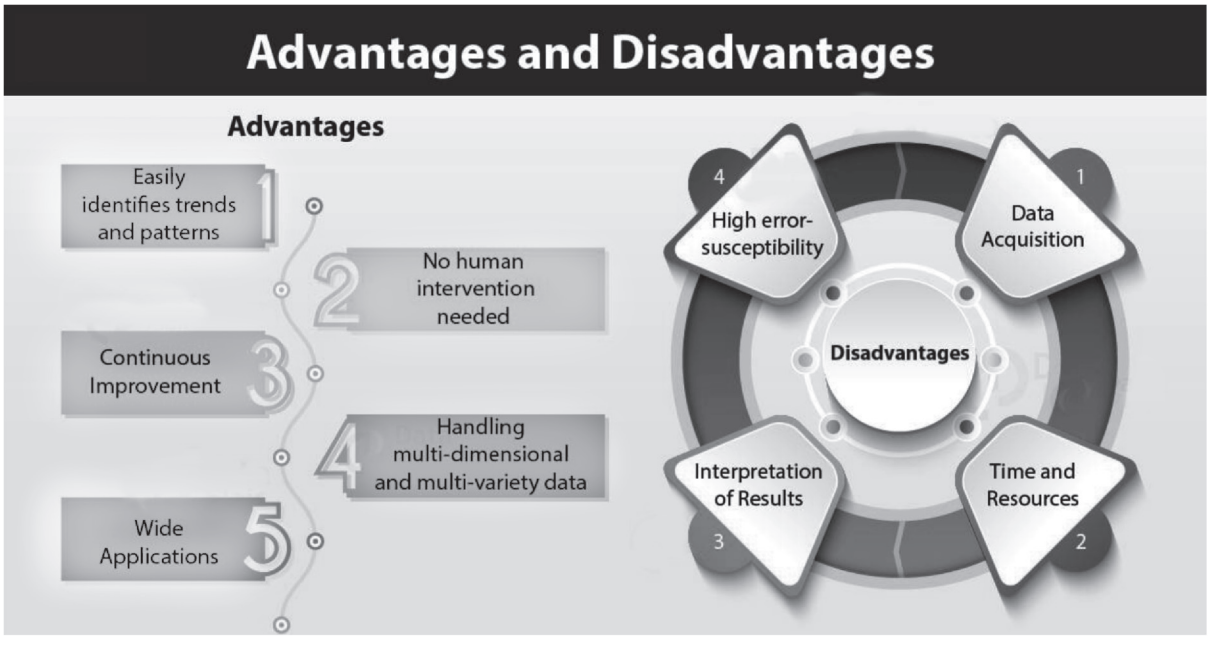
11. See, Fay Robert and Trenholm Wallace, The Cyber Security Battlefield, CIGI Online. Available at https://www.cigionline.org/articles/cyber-security-battlefield/?utm_source=google_ads&utm_medium=grant&gclid=EAIaIQobChMIwb2dyoXU_gIVUGErCh1UrgJFEAAYAyAAEgKmmfD_BwE

Emergence of AI in Cyber Security:

Owing to its recognizing capabilities, data collection, and other capabilities, machine learning and Artificial Intelligence are being integrated more deeply than ever before across organisations and apps. This vast collection of data is valuable food for AI, which can analyze every gathered information to identify unique patterns and intricate characteristics. This means that in terms of cyber security, new initiatives and flaws may be quickly identified and studied to help avoid more attacks. It may lessen some of the burden placed on human cybersecurity partners. When a task is necessary, they are notified, but they also have the option of devoting their time to more creative and fruitful tasks.

Use of AI in Cyber Security:

Artificial Intelligence is already being adopted in numerous fields of cyber safety or is currently being considered in these areas. For example, Gmail uses artificial intelligence to detect unwanted spam and malicious mails and blocks them by using AI tools. Whenever any user clicks any email message or marks it to be safe, they are basically helping to educate the AI to distinguish spam and safe mails in the future. Due to these advancements, AI is now capable of detecting even the subtlest spams that try to pass as normal regular mails.



Source: https://data-flair.com

Benefits of AI in Cyber Security

- **Threat Assessment:** Threats are identified using conventional security techniques like signatures. This method may work well for risks that have already been encountered, but it is ineffective for hazards that haven't yet been discovered. Around ninety per cent of attacks may be distinguished using signature technique. AI can boost recognition percentages up to ninety-five, but one will experience a huge data of "false-positives" if someone replaces traditional techniques with it. The optimal method integrates traditional methods with AI. It could increase the location rate up to hundred per cent and reduce false positives. By combining some behaviour assessment techniques, institutions can additionally employ AI to enhance the risk-chasing approach.

- **Improvements in Threat Detection:** Significantly better detection systems rates could well be obtained by combining conventional security mechanisms (i.e. utilising the database of all recorded security concerns till date) and employing automation to identify new risks.
- **Detecting Frauds:** Fraudulent purchases and actions may be recognised and stopped in a timely manner by seeing patterns and identifying breaches from the expected baseline behaviour. "Anomaly detection" is one of the most well-known uses of machine learning since it is a commonly used technique.
- **Detecting Malwares:** In most cases, hackers deliberately design malwares, which once made, automates the creation of successive version that evade detection. Machine learning techniques are used to improve traditional signature-based malware identification algorithms in order to identify and stop the transmission of certain possible malware copies and variations.
- **Protection of Passwords:** Passwords have long been one of the privacy concerns of organizations. In fact, passwords are usually the primary connection involving our identities and the conduct of online fraudsters. Although biometric authentication has been considered a viable answer, it's not currently the easiest practical answer to apply in this case. With the use of AI, it might change over a period of time. Developers are implementing AI to strengthen authentication process and get rid of any flaws. A good illustration of this is Apple's face identification software. This technique, called 'Face ID', uses infrared sensors that detect a user's facial characteristics. The Apple AI algorithm then develops a complex representation of the user's face to aid in the identification of significant resemblance.
- **Secure Network Automation:** The creation of security policies and organizational network structure are two fundamental elements of cybersecurity. Admittedly, these demand a great deal of effort and attention from people to attain and manage.

Thankfully, AI can partially simplify these processes. By monitoring network activity trends, AI may produce and advice rules and processes that are tailored to one's specific environment.

Disadvantages of AI in Cyber Security

- **Cost Efficiency:** Usually, the expense of deploying AI services is too high, making it impossible for everybody to benefit from them.
- **Online Threats:** Nowadays, hackers have too much access to our data and safety. If precautions are still not followed, they may simply monitor our whereabouts and hack our individual data anytime.
- **Humans are being controlled by machines:** Humans are being controlled by machines and this was the first concerns of using AI. This issue has previously been discussed in several novels and movies. It is necessary to take action to stop this from happening.
- **Cybercriminals are aware of the public access to AI knowledge:** Cybercriminals may easily obtain cybersecurity products developed by AI and utilise these to attack users through malware. Hackers have the ability to develop harmful, AI-resistant programs that more effectively penetrate sites and businesses.
- **Job Losses:** AI is regarded as a danger since some estimates indicate that a significant portion of the workforce in any organisation over a period of time will be replaced by AI apps and machines. Many people do not want to learn or understand new technologies, which in turn leads to the decrease in workforce.
- **Evolving Cyberthreats:** Even by incorporating AI into the business doesn't guarantee that one will instantly become immune to all threats. Even AI systems need ongoing redesign, improvement and maintenance since viruses and malware are always evolving.

Concluding Remark

It is impossible to overlook the need for advanced cyber security measures in a situation where malicious cyber threats are growing exponentially. The significance of AI in cyber security, as well as the many problems that occur from it and how to mitigate them has its own pros and cons. Despite the limitations, AI still plays a big part in cyber security. Artificial intelligence over time will help to develop data protection by helping to overcome the shortcomings.

AI VERSUS ETHICS & MORALITY

The significance of Artificial Intelligence (AI) has increased significantly during the past few decades. Self-driving vehicles, chatbots, speech assistants and many other technologies have revolutionised the way we live our lives as a result of AI technology. The importance of moral foundations and ethical issues has increased as AI becomes more pervasive. The growth of artificial intelligence poses moral questions about matters like bias, responsibility, justice, and openness. More advanced and effective AI systems have been developed due to the developments in machine learning and other fields and so the importance of artificial intelligence (AI) has grown in this century. Besides this, as the AI has developed, significant moral and ethical issues are also being raised. The effects of Artificial intelligence on ethics and morality are covered here.

Confidentiality

Concerns regarding confidentiality/privacy are quite substantial in regard to AI. Massive quantities of private information, including surfing histories and shopping patterns, are collected about people by AI systems. Predictive models and tailored marketing campaigns may be created using this data. Moreover, it may be used to determine a person’s eligibility for jobs, insurance, and loan prospects. A serious breach of privacy may result from the improper application of this dataset.

AI’s Prejudice

The data that AI is fed determines how objective it really is. As statistical information is the basis for training AI models, biased statistical information will result in biased AI models. Policies may be taken as a consequence that is unfair and arbitrary. For instance, if the learning data comprises primarily of white people, an AI system utilised in recruiting may be prejudiced towards people of colour. Consequently, if the testing dataset comprises disproportionate detention and acquittals of members of minority populations, an AI system utilised in criminology may be prejudiced against them.

Responsibility and Transparency

It might be challenging to comprehend how AI technologies make judgments since they are frequently “black boxes.” Due to the difficulty of holding an Artificial Intelligence’s algorithm accountable for its actions, the absence of openness may also result in lack of responsibility. It could be difficult to comprehend the rationale behind a suggestion given by an AI system utilized in healthcare, for instance. Due to the absence of openness, it may be impossible to contest the choice or consider the program responsible for any unfavourable results.

Discrimination and Bias

AI systems are susceptible to prejudice and bias, which might have detrimental effects on specific human beings or communities. For instance, a recruiting prejudice may occur if an AI system used to filter job candidates favours women or minorities. According to this, a criminal justice AI system might be unfavourable to minorities, resulting in unfair prosecutions.

Regardless of whether AI’s algorithms can be trained to be ethical or moral is among the fundamental questions

regarding Artificial Intelligence and ethics. Some studies contend that it is feasible to build AI systems to act morally and ethically, whereas others counter that it is not possible to build fully moral or ethical Artificial intelligence technology.

It may prove challenging to encode moral and ethical ideas into algorithms or principles that AI technologies can adhere to since they might be complicated and context-dependent. For instance, the ethical precept of “do no damage” is vital in many disciplines, yet defining meaning of damage means in a specific situation might be complex.

Another difficulty is that ethical and moral concepts sometimes include irrational judgments that are hard to define or assess. Considering everyone equally may well be required under the idea of justice, however fairness can be a subjective concept that varies based on the situation.

Notwithstanding these obstacles, attempts are being made to create ethical and moral guidelines for Artificial Intelligence. For instance, a set of standards for the moral development and design of Artificial intelligence systems has been created by the “IEEE Global Initiative for Ethical Issues” in AI and Autonomous Systems. Similar to this, a group of business, academics, and philanthropic group has created a set of ethical guidelines for Artificial Intelligence.

The ethical and moral ramifications of AI continue to raise problems, despite the existence of these models. One worry is the possibility that prejudices and inequities might be reinforced or even made worse by AI technologies.

AI VERSUS LAW AND COMPLIANCE

In India, numerous industries have seen significant advancements in artificial intelligence (AI). Despite the prospective advantages it may provide, AI deployment in the legal sector has been somewhat gradual. In this chapter, we’ll look at some of the applications of AI in the Indian legal sector and the difficulties that come with them, notably in terms of complying with legal requirements.

AI’s in the Legal Industry

In the domain of law and compliance, AI has the capacity to revolutionize the legal sector. AI can help lawyers and legal departments deal with the volume of data produced as well as the increasing complication of rules and guidelines. Artificial intelligence (AI) may, for example, simplify the contract monitoring, compliance, and assessment processes.

By combing through voluminous data to find pertinent cases as well as precedents, AI may also help attorneys with their research work. This may save professionals a great deal of time and free them up to work on other legal compliances.

AI-powered solutions may also classify and analyse data to find possible regulatory or legal concerns, assisting organizations in adhering to rules and averting expensive legal fights.

Although, AI can simplify repetitive operations and improve the productivity and efficiency of attorneys, some legal duties still demand human involvement. For example, complicated legal disputes or discussions call for human knowledge, wisdom and competence.

Challenges in AI adoption in Law and Compliance

Notwithstanding the potential advantages of AI in law and compliance, India faces a number of barriers to its implementation. Lack of knowledge and trustworthiness is one of the major problems. Many law companies and attorneys are still unaware of the potential benefits of AI for the legal industry.

The expense of deployment is another issue because it necessitates using specialist technologies and high-quality datasets. Smaller legal companies may find it difficult to employ AI solutions due to the high expense.

Another important problem is privacy issues. Information protection and privacy are issues that are raised with the introduction of AI systems that utilise personal information. When utilising AI systems that gather and handle personal data, lawyers and legal departments must exercise caution.

The regulatory framework presents another obstacle to AI use in law and compliance in India. There isn't a specific legislative mechanism that covers the implementation of AI in the legal sector, and India's data security regulations are still in the process of development. Due to this, it is challenging for legal firms to embrace and use AI technology.

Conclusion

In India, the legal sector is poised to undergo a transformation, especially in the areas of compliance and legislation. Yet, there are considerable obstacles to its acceptance, including a lack of knowledge and confidence, high adoption costs, security issues as well as the regulatory compliance. Thus, it is crucial that Indian law companies and legal departments spend the time learning about the competence of AI and the prospective advantages it brings to the legal field. Law businesses and legal teams may save time, cut expenses, and do better work by investing in AI solutions.

AI AND INTELLECTUAL PROPERTY RIGHTS

Introduction of Artificial Intelligence and its use has considerably changed the arrangement of how people work. Similarly, its use in intellectual property has become increasingly prevalent. One of the most important applications of AI in IP is the creation of new work as it can generate original work. AI focuses on performing tasks with the help of intelligence methods such as Reasoning, Machine Learning, Problem Solving, Perception, and Linguistic Intelligence. With the help of AI-powered algorithms, comprehensive searches of existing IP databases can be performed more efficiently and accurately. Along with this, it also helps in analyzing technical information and documents to determine existing relevant work to prevent copyright infringement. As AI technology becomes more advanced, it will likely be used more in areas related to intellectual property. This could lead to new legal issues and problems.[12]

> "As artificial intelligence (AI) continues to emerge as a general-purpose technology with widespread applications throughout the economy and society, this poses fundamental questions that sit at the heart of the existing IP systems. Some major questions involve – (i) Does AI innovation and creation need IP incentives? (ii) How should the value of human invention and creation be balanced against AI innovation and creation? (iii) Does the advent of AI require any changes to the existing IP frameworks?" - **World Intellectual Property Organization**

Some of the IPR issues related to AI generated output are as follows:

1. **Ownership and Authorship**

   One of the most important legal challenges posed by Artificial Intelligence on IP is the issue of ownership and authorship of AI-generated works. As discussed earlier, one can generate original work with a high level of creativity with the help of AI but the question arises 'Who owns that work?' one who gives directions to the AI system to create the work (User), the developer of the AI system, or the AI system itself. According to the traditional intellectual property law, the creator or author of the work is considered the sole owner of the work but this is not the case with the AI-generated art.

2. **Copyright Challenges**

   The ability of Artificial Intelligence to generate huge content quickly raises copyright issues as it can easily duplicate and reproduce copyrighted content such as images, texts, videos, music, etc. AI-

12. Reproduced from Impact of AI on Intellectual Property Practices (January 31, 2024), Free Law.

powered systems can copy any work or art or content without permission of the owner, making it difficult to identify the original and duplicate or unauthorized work. Now, the question arises whether the content generated through AI can be copyrighted. In most jurisdictions including Spain and Germany, it has been determined that only works created by a human being can be protected by copyright.

A key question regarding AI copyright in India is whether computer-authored works meet the originality criterion under Section 13 of the Copyright Act[13]. Courts have interpreted originality as intellectual effort furnished by humans. But training neural networks involves significant human endeavour in curating datasets, designing architectures, etc. Developers argue this effort imbues originality into works like AI-generated music.[14] Similarly, in the M/S Kibow case, the Delhi High Court ruled that AI systems cannot be officially registered as the proprietor of a trademark. It also highlighted that the Trade Marks Act, of 1999 illustrates that only a human being can apply for and be officially registered as the proprietor of a trademark.

Amending the law to designate AI developers as owners could incentivize building socially useful AI assistants and content generators. However, some caution this may create monopolies over data used to train models.[15] Nuanced provisions may be needed to balance interests, like compulsory licensing of protected AI works. Infusing human intent into generative processes can also strengthen copyright claims. India's jurisprudence around AI copyright will likely evolve case-by-case.

However, others contend processing data alone may not satisfy originality – focus should be on the creative process itself.[16] Especially with advanced AI like Generative Adversarial Networks, outputs manifest autonomously with little human input during generation. Even if AI works get copyright, determining the rightsholder is difficult – the programmer, user, or AI system itself? Overall, more clarity is required on copyright's applicability to AI works in India.

3. Patent Law

India's patent regime faces similar quandaries around AI. Under Section 2(1) of the Patents Act[17], AI developed inventions like new chemicals or devices may meet patentability criteria of novelty, utility and industrial applicability. However, such works may not demonstrate sufficient inventive step since the AI system rather than a human brain conceived the invention16. This could preclude patentability.

Again, developers try asserting their efforts training the model should count[17]. But others argue the critical inventive aspect under law is conceiving the final patented product or process, which AI does autonomously.[18] Section 6's terminology of identifying a human "true and first inventor" also suggests difficulty accommodating AI inventors.[19] Like copyright, approaches are debated like designating the programmer or user as deemed inventor for AI creations.

Clearer guidelines are required on evaluating and assigning patents for AI outputs. Suitably defining inventiveness for AI systems, while upholding patent law's intent of protecting true human inventors, will be key. India could emulate US and UK patent office moves to allow naming AI systems alongside humans as joint applicants on patents they contributed to overall, India's patent law will require modernizing to appropriately incentivize AI innovation.

13. The Copyright Act, 1957, §13, No. 14, Acts of Parliament, 1957 (India)

14. Ramakrishna B & Anil Kumar H.S., Fundamentals of Intellectual Property Rights: For Students, Industrialist and Patent Lawyers (2017)

15. Ibid

16. Guadamuz, A. (2021). Do androids dream of electric copyright? Comparative analysis of originality in artificial intelligence generated works. Intellectual Property Quarterly, (2), 169-186

17. The Patents Act, 1970, §2(1), No. 39, Acts of Parliament, 1970 (India)

18. Yanisky-Ravid, S., & Liu, X. (2018). When artificial intelligence systems produce inventions: An alternative model for patent law at the 3A era. Mich. St. L. Rev., 2018, 839

19. The Patents Act, 1970, §6, No. 39, Acts of Parliament, 1970 (India)

4. Other IPR Issues

Automated content generation, data privacy and security, deep fakes, and manipulated content are some other issues posed by AI in safeguarding intellectual rights. Moreover, the use of AI increases various ethical concerns; therefore, there is a need to balance the benefits of AI with the protection of intellectual property rights by introducing appropriate frameworks.

Requirement of Amendment in Laws

Due to the emergence of AI, below are some of the sections that may require changes in the IPR related laws[20] :

- **Copyright:** AI-generated works may raise questions about authorship and ownership. Section 17 of the Copyright Act may need to be amended to address the issue of ownership of AI-generated works.
- **Patents:** AI technology can generate novel inventions that may require patent protection. Section 3(k) of the Patents Act may need to be reviewed to address the patentability of AI-generated inventions.
- **Trademarks:** AI systems can generate trademarks, which raises questions about the ownership and distinctiveness of such marks. Sections 9 and 11 of the Trademarks Act may require amendments to address these issues.
- **Trade secrets:** AI technology can facilitate the disclosure and misappropriation of trade secrets. Section 2(1)(a) of the Trade Secrets Act may need to be amended to clarify what constitutes a trade secret in the context of AI.
- **Enforcement:** The use of AI can make it difficult to detect and enforce IPR violations. Section 53 of the IPR Act may need to be amended to address these challenges and to ensure that appropriate enforcement mechanisms are in place.

Existing IPR regime well-equipped to protect AI generated works, no need to create separate category of rights[21]: Recent Statement of Union Minister of State for Commerce and Industry, Government of India in a written reply in the Rajya Sabha on 9th February, 2024.

Intellectual Property Rights including Copyright and Related rights provide exclusive rights to the right owner who are legal persons for a set duration. These rights allow for the work or creation or innovation to be protected and enables collection of royalties through licensing. For a right to be granted, the owner is required to meet the criteria specified under the law. India being a member of all major international conventions and agreements for the protection of Intellectual Property Rights grants adequate protection of rights for works created by legal persons through Copyright Law and protects inventions through the Patent system. Therefore, there is no requirement to create a separate category of rights for AI and related innovations in the Indian IPR Regime. Therefore, while Artificial Intelligence (AI) and related innovations is an evolving stream of technology the current legal framework under the Patent and Copyright Act is well-equipped to protect Artificial Intelligence generated works and related innovations. Presently, there is no proposal to create any separate right so ram end the law in the context of AI-generated content.

The exclusive economic rights of a copyright owner such as the right of reproduction, translation, adaptation etc. granted by the Copyright Act, 1957 obligates the user of Generative AI to obtain permission to use their works for commercial purposes if such use is not covered under the fair dealing exceptions provided under Section 52 of the Copyright Act. Since Intellectual property rights are private rights, these are enforced by the individual rights holders. Adequate and effective civil measures and criminal remedies are prescribed under the Copyright Law against any act of infringement or unauthorized use of works, including digital circumvention.

20. Reproduced from Vishaka Aditya, Navigating the Legal Challenges posed by AI on Intellectual Property, Legal Service India

21. This information has been provided by the Union Minister of State for Commerce and Industry, Shri. Som Parkash in a written reply in the Rajya Sabha on 9th February, 2024. Reproduced from Press information Bureau. Available at https://pib.gov.in/PressReleasePage.aspx?PRID=2004715

CASE LAWS

Recent Indian case laws related to ai and intellectual property:

AI technology has had an impact on landmark judgments passed by the courts in India.

These case laws demonstrate the need for clarity and amendments in Indian intellectual property laws to address the emerging challenges posed by AI technology. The Indian judiciary has taken a pragmatic approach in these cases by balancing the need for innovation with the protection of intellectual property rights.

These case laws demonstrate the evolving nature of the relationship between AI and intellectual property in the Indian legal system and highlight the need for clear legal frameworks to address the legal challenges posed by AI on intellectual property.

In 2021, the Delhi High Court ruled in the case of M/S Kibow Biotech v. M/S The Registrar of Trade Marks that an AI system cannot be considered a proprietor of a trademark. The court held that under the Trade Marks Act, of 1999, only a person can apply for and be registered as the proprietor of a trademark, and an AI system cannot be considered a person for the purposes of the Act.

In another case, Ferid Allani v. Union of India, the Delhi High Court examined the issue of whether an AI-generated work can be copyrighted in India. The court held that copyright protection can be granted to AI-generated works if they meet the criteria for originality and authorship under the Copyright Act, of 1957. The court also held that the authorship of an AI-generated work should be attributed to the person who decided to create the work, such as the programmer or user of the AI system.

In the case of South Asia FM Limited v. Union of India, the Delhi High Court examined the issue of whether a song created by an AI system could be considered a work of original authorship under the Copyright Act, of 1957. The court held that the song was not eligible for copyright protection as it lacked the human element of creativity and was the result of an algorithmic process. The court held that for a work to be eligible for copyright protection, it must result from human creativity and originality.

In the case of Gaurav Bhatia v. Union of India, the Delhi High Court held that AI-generated inventions could be patented if they met the requirements of novelty, non-obviousness, and industrial applicability under the Patents Act.

In the case of Nippon Steel Corporation v. Union of India, the Bombay High Court held that computer programs that generate inventions or discoveries could not be patented because they are not capable of being invented by a person.

In the case of In Re: Sugen Life Sciences Pvt. Ltd, the Indian Patent Office rejected a patent application for a drug discovery algorithm, stating that it was not a patentable invention under Section 3(k) of the Patents Act because it was a computer program per se.

In the case of Dr. Alaka Sharma v. Union of India, the Delhi High Court held that an AI-generated portrait could not be registered as a trademark under the Trademarks Act because it did not satisfy the distinctiveness requirement.

In the case of MySpace Inc. v. Super Cassettes Industries Ltd., the Delhi High Court held that an AI-based algorithm used to identify and remove infringing content on a social media platform did not violate the Copyright Act because it was not reproducing the copyrighted content.

Transforming India with AI

1. India’s AI Ecosystem

India ranks third globally in AI competitiveness according to the Stanford University 2025 Global AI Vibrancy Tool. The technology sector is projected to generate $280 billion in revenue in 2025, employing six million people across the AI and technology ecosystem. Approximately two lakh startups are registered as of January 2026, of which roughly ninety percent are AI-powered in some form, and India is the second-largest contributor to AI projects on GitHub worldwide. AI is projected to add $1.7 trillion to the Indian economy by 2035. These indicators reflect a broad-based technology culture that extends well beyond a handful of metropolitan hubs, providing fertile ground for the government’s institutional investments.

The IndiaAI Mission, approved in March 2024 with an outlay of Rs 10,371.92 crore over five years, constitutes the foundational architecture of this strategy. Its design reflects a systems-level understanding of AI development: raw compute, curated datasets, foundation models, skilled talent, entrepreneurial financing, and regulatory safety are treated as interdependent requirements rather than sequential priorities. The Mission’s original target of 10,000 GPUs has already been surpassed, with more than 38,000 high-end GPUs onboarded at Rs 65 per hour — approximately one-third of the global average cost — alongside 1,050 Tensor Processing Units, making advanced AI compute accessible to startups and research institutions that would otherwise be priced out.

2. IndiaAI Mission — Seven Pillars

Pillar 1 – Compute

38,000 high-end GPUs have been onboarded under the Mission and are available to researchers, developers, and institutions at Rs 65 per hour – a price that is approximately one-third of the prevailing global average, making advanced AI compute economically viable for a vastly wider range of actors than would otherwise be possible. In addition, 1,050 Tensor Processing Units have been onboarded to support large-scale AI model training workloads, which are computationally intensive and require specialised hardware beyond standard GPU clusters. The scale of this achievement is particularly notable given that the Mission’s original target was 10,000 GPUs; the actual deployment of more than 38,000 represents a near-fourfold overperformance relative to the initial plan, reflecting both strong institutional execution and a rapidly growing demand for AI compute across India’s research and innovation ecosystem

Pillar 2 – Application Development

By July 2025, thirty AI applications had been formally approved under this pillar, spanning a deliberately diverse range of sectors: healthcare, agriculture, governance, climate science, and assistive technology for persons with disabilities. Each application represents a structured collaboration between the IndiaAI Mission and the relevant sectoral ministry or agency, ensuring that AI deployment is driven by genuine public need rather than technology-push alone. The pillar has also pioneered the use of focused hackathons as a mechanism for rapid application ideation.

Pillar 3 – AIKosh (Dataset Platform)

As of February 2026, AIKosh hosts 7,541 datasets and 273 AI models spanning twenty sectors, drawing on contributions from both government departments and non-government sources. The platform serves as a one-stop resource enabling developers to access ready-to-use training data and model weights, dramatically reducing the time and cost required to build new AI applications. The scale of engagement with the platform is a meaningful indicator of its utility: by December 2025, AIKosh had recorded 3.85 lakh visits, 11,000 registered users, and 26,000 dataset and model downloads. These numbers suggest that the platform has moved well beyond a symbolic data repository and is functioning as a genuinely active infrastructure resource within India’s AI development ecosystem.

Pillar 4 – Foundation Models

The Foundation Models pillar has received more than 500 proposals from organisations across India, demonstrating the depth of domestic ambition and technical capacity in this space. From these proposals, twelve startups have been selected across two competitive phases to build sovereign, multilingual foundation models: Sarvam AI, Soket AI, Gnani AI, Gan AI, Avaatar AI, BharatGen led by IIT Bombay, Zenteiq, Gen Loop, Intellihealth, Shodh AI, Fractal Analytics, and Tech Mahindra Maker's Lab. BharatGen, the first government-funded multimodal large language model, launched in June 2025, covers 22 Indian languages and is capable of processing and generating text, speech, and image content – a significant milestone in India's development of AI systems that are truly built for and by India. Sarvam AI, approved in April 2025, is developing a Sovereign LLM Ecosystem and has entered into a partnership with the Unique Identification Authority of India for AI-powered Aadhaar-linked services.

Pillar 5 – Future Skills

The Mission provides 13,500 fellowships in total: 8,000 at the undergraduate level, 5,000 at the postgraduate level, and 500 doctoral fellowships. The doctoral programme currently has 73 institutes onboarding PhD students, building a pipeline of deep research expertise that will sustain India's AI frontier capabilities over the long term. To extend AI education into the vocational and technical training system, 31 AI Data Labs have been launched across India in partnership with the National Institute of Electronics and Information Technology (NIELIT), giving students and practitioners in tier-two and tier-three cities access to hands-on AI training infrastructure. Additionally, 174 Industrial Training Institutes and polytechnics have been nominated to integrate AI-related courses into their curricula, bringing AI literacy into the Craftsmen Training Scheme and ensuring that AI skills are not confined to elite institutions.

Pillar 6 – Startup Financing

The IndiaAI Startups Global initiative, launched in March 2025, represents the first structured effort under this pillar to do so. Ten carefully selected Indian AI startups received targeted assistance to enter the European market, with access provided through Station F in Paris – Europe's largest startup campus – and HEC Paris, one of Europe's leading business schools. This programme offers participating startups mentorship, network access, and market entry support of a kind that is typically available only to startups based in established technology hubs such as Silicon Valley or London. By deliberately opening these pathways for Indian AI companies, the Mission is signalling that India's AI ambitions extend beyond serving its own 1.4 billion citizens and encompass the aspiration to build globally competitive AI enterprises capable of shaping technology development on an international scale.

Pillar 7 – Safe & Trusted AI

Thirteen research projects are currently underway under this pillar, covering four critical dimensions of AI safety. Work on bias mitigation investigates how AI systems trained on historical data can perpetuate or amplify existing social inequalities, and how these tendencies can be detected and corrected. Research on model explainability addresses the challenge of making AI decision-making processes transparent and interpretable to users, regulators, and affected communities – a particular concern in high-stakes domains such as medical diagnosis or credit assessment. Machine unlearning explores the technical problem of removing specific information from a trained model without retraining it entirely, which is essential for compliance with data protection legislation including India's own Digital Personal Data Protection Act 2023.

3. Infrastructure: Compute, Connectivity, and Energy

India's AI ambitions rest on a rapidly expanding physical infrastructure. The National Supercomputing Mission has deployed over 40 petaflops of high-performance computing capacity across IITs and IISERs. The India Semiconductor Mission, backed by Rs 76,000 crore, has approved ten projects with cumulative investments

of Rs 1.60 lakh crore across six states, targeting a domestic chip market of $100 to $110 billion by 2030. India Semiconductor Mission 2.0, announced in Budget 2026-27 with Rs 1,000 crore for the first year, deepens the commitment to technological self-reliance in AI hardware.

On connectivity, 5G services now reach 99.9 percent of districts, covering 85 percent of the population across 5.08 lakh base stations. Broadband connections have grown 1,532 percent since 2014 to reach 99.56 crore, with mobile data costs of $0.10 per gigabyte among the lowest globally. The BharatNet programme has connected 2,14,843 Gram Panchayats via optical fibre. India has also become only the fifth country worldwide to deploy an indigenous 4G technology stack – integrating Tejas Networks, C-DOT, and TCS – at approximately 98,000 BSNL towers, while the Bharat 6G Mission targets global leadership by 2030. Cloud data centre capacity stands at 1,280 MW and is expected to grow four to five times by 2030, anchored by major foreign investments including Google’s $15 billion AI hub in Visakhapatnam and Amazon Web Services’ $8.3 billion commitment in Maharashtra. The energy foundation is equally significant. India reached 50 percent non-fossil fuel electricity capacity in June 2025, five years ahead of its Paris Agreement target, with renewable capacity at 253.96 GW. The SHANTI Act 2025 projects nuclear capacity growth from 8.78 GW to 22.38 GW by 2031-32. A clean, abundant, and affordable energy supply is a structural prerequisite for the data centre expansion and AI workload growth that India’s digital strategy requires.

4. Regulatory & Policy Framework

- MeghRaj (GI Cloud): 2,170 Ministries & Departments hosting applications; pay-per-use model reduces AI adoption costs.
- Digital Personal Data Protection Act 2023: Compliance requirements for all entities handling personal data.
- Government Open Data License India: Enables reuse of non-sensitive public data for AI development via data.gov.in.

5. AI in Everyday Life

(a) Healthcare and Agriculture

AI is deployed for early disease detection, medical image analysis, and telemedicine platforms that connect rural patients with urban specialists. ICMR-IndiaAI collaborations with the United Kingdom and Singapore are developing diagnostic tools calibrated to Indian epidemiological contexts. In agriculture, Kisan e-Mitra provides farmers with AI-assisted guidance on government schemes and agronomic decisions, while the National Pest Surveillance System and Crop Health Monitoring integrate satellite, soil, and weather data into real-time field advisory services for smallholder farmers.

(b) Education and Governance

The CBSE has introduced an AI curriculum from Class VI under the National Education Policy 2020. The YUVAi programme engages students from Classes 8 to 12 across eight applied domains including health, environment, and law. FutureSkills PRIME has registered 18.56 lakh participants, with NASSCOM projecting India’s AI talent pool to reach 12.5 lakh professionals by 2027. In governance, e-Courts Phase III uses AI for case translation, automated filing, and intelligent scheduling, while High Court AI Translation Committees are systematically translating Supreme Court and High Court judgments into vernacular languages – extending access to justice to non-English-speaking citizens through the e-HCR and e-ILR portals.

(c) Media and Broadcasting

In March 2026, the Ministry of Information and Broadcasting partnered with Google and YouTube through the Indian Institute of Creative Technologies to launch a National AI Skilling Initiative providing

free training to 15,000 creators, media professionals, and students. Phase I covers foundational AI literacy; Phase II, running July to December 2026, delivers advanced project-based training using tools including Gemini 3, Veo, and Vertex AI. MyWAVES, a citizen creator platform on the WAVES OTT service, enables content creation and sharing in multiple Indian languages and integrates with the Create in India Challenge, strengthening India's creative economy.

(d) Financial Inclusion and the Digital Economy

India's financial inclusion ecosystem is anchored in the JAM Trinity of Jan Dhan accounts, Aadhaar, and mobile connectivity. As of April 2026, 58.16 crore Jan Dhan accounts hold cumulative deposits of Rs 3.02 lakh crore, while 144 crore Aadhaar numbers provide a universal digital identity layer. UPI processed Rs 29.53 lakh crore worth of 2,264 crore transactions in March 2026 alone, accounting for 81 percent of retail payment volume across 691 live banks. The Direct Benefit Transfer system has transferred Rs 49.09 lakh crore cumulatively to citizens, eliminating Rs 4.31 lakh crore in leakages – one of the most consequential applications of digital infrastructure to public finance in recorded administrative history. AI is extending the reach of formal credit to previously excluded borrowers. The Unified Lending Interface has onboarded 64 lenders offering 136 data services across twelve loan journeys, with expansion underway to rural cooperative banks. The Account Aggregator framework has enabled 2.6 billion accounts for consent-based data sharing. AI credit models that analyse UPI histories, GST filings, and utility payments are estimated to unlock a $130 to $170 billion credit gap, substantially reducing MSMEs' dependence on informal lenders. Banking BHASHINI, developed through a February 2026 MoU between the Digital India BHASHINI Division and the Reserve Bank of India, will provide multilingual AI access to banking services across all 22 scheduled Indian languages. MuleHunter.AI, launched by the RBI Innovation Hub, detects cybercrime-linked mule accounts through real-time transaction pattern analysis, strengthening the security of India's digital financial system.

6. Inclusive Development: The Informal Sector

NITI Aayog's October 2025 report on AI for Inclusive Societal Development identifies India's 490 million informal workers – carpenters, gig workers, smallholder farmers, domestic care workers – as the primary beneficiaries that AI policy must reach if democratisation is to be more than a rhetorical commitment. Mission Digital ShramSetu, proposed in the same month, is a phased national initiative that deploys AI, blockchain, IoT, and immersive learning to dismantle the structural constraints of financial insecurity, limited market access, and the absence of formal skill credentials. The four-phase roadmap runs from mission design and stakeholder engagement in 2025-26, through governance structure-building and infrastructure preparation in 2026-27, to sector-specific pilots from 2027-29 and nationwide scale-up from 2029 onward. By 2035, the mission envisions voice-first AI interfaces, smart payment contracts, and portable micro-credentials that allow informal workers to integrate into the mainstream economy with full economic dignity.

7. Key Programmes & Platforms

- **Bhashini:** AI translation platform; 36+ Indian languages; 1.2 million downloads; 350+ AI models; 450+ customers. MoU with CRIS (Railways, Jun 2025) and RBI (Feb 2026) for Banking BHASHINI.
- **BharatGen AI:** First government-funded multimodal LLM (launched Jun 2025); 22 Indian languages; text + speech + image understanding.
- **Sarvam AI:** Sovereign LLM Ecosystem (approved Apr 2025); partnership with UIDAI for AI-powered Aadhaar services.
- **AI Competency Framework:** Structured AI training for government officials aligned with global benchmarks.

- **India–AI Impact Summit 2026:** Held Feb 2026 at Bharat Mandapam; 15–20 Heads of Government, 50+ ministers, 100+ global CXOs; Democratizing AI Resources Working Group co-chaired by India, Egypt & Kenya.

India’s AI strategy as documented through mid-2026 is notable for three qualities that distinguish it from analogous national strategies in high-income countries. First, it is systemic: the IndiaAI Mission addresses compute, data, models, talent, financing, and safety simultaneously rather than in sequence. Second, it is sovereign: the deliberate development of indigenous semiconductor capacity, domestic 4G and 6G stacks, and multilingual foundation models reflects a determination to build genuine technological self-reliance. Third, and most distinctively, it is explicitly inclusive: the democratisation of AI – extending its benefits to informal workers, non-English speakers, rural populations, and the previously unbanked is not a secondary social objective but the primary design criterion of the entire policy architecture. Whether India fully realises these ambitions will depend on implementation quality and regulatory adaptability, but the institutional foundations laid in this period are substantial and serious.

CASE STUDIES

The society we are living in today is being drastically changed by artificial intelligence (AI). It has transformed a number of sectors, including production, medical, academics, and finance, to mention some. Several businesses have actively adopted AI-powered techniques to enhance their processes, and plenty more are thinking about doing the same.

In the drive to deploy AI and take leverage of its benefits, India is catching up quickly. Companies all over India are examining AI-enabled technologies to drive growth, simplify processes, and enhance client satisfaction. To guarantee that AI is utilised ethically and appropriately, laws and regulations must be implemented as new technology brings new challenges post its adoption.

India has encountered several cases that address the legal ramifications over this decade itself. Several of these judgments have established significant precedents that can direct corporations and lawmakers in how they view and perceive AI.

The Supreme Court of India achieved a huge technical advancement during March 2023 by using AI to live-transcribe its proceedings/hearings. Despite this, courts throughout the nation have not used text-generating bots or algorithms to make rulings or support conclusions up to this point.

The High Court of Punjab and Haryana in the last week of March 2023 has made legal history by integrating human and artificial intelligence in its ruling in a case concerning assault and murder. HMJ Anoop Chitkara used the ChatGPT AI tech’s response in the ruling while he was addressing the issue of jurisprudence of bail in a case where assault and cruelty are the main ingredients. This in itself will set a good precedent for the courts in the future.

Right to Privacy (Aadhaar Case)

One of the notable instances involving AI in our country was the Aadhaar case. In this case, the Apex Court had to establish whether the Aadhaar database infringed on Indian residents right to privacy.

The biometric authentication Aadhaar employs artificial intelligence to collect the confidential information of Indian people. Since its inception, the program has generated controversy, and various data protection activists have attacked it for gathering excessive amounts of personal data.

The Aadhaar system was found to be lawful by the Constitutional Bench in the year 2018, however some limitations were placed on its application. The judgment said that people should have the option of opting out of the programme and that Aadhaar cannot be made compulsory for operations like banking and cellphone communications.

Organisations who employ AI to gather and preserve customer information should take note of the Aadhar issue. The case emphasises the need of protecting personal data and preventing the misuse of AI systems to violate people's right to privacy.

Shamnad Basheer* vs. *Union of India

In the case of Shamnad Basheer vs. Union of India, the Delhi High Court had issued an order in 2020 requiring the authorities to be fairly transparent regarding the implementation of AI in decision making procedures. The court determined that the application of Artificial Intelligence must be open and responsible in the matters involving the National Law School of India University's (NLSIU) usage of Artificial Intelligence to evaluate candidates for admission.

The Gig Economy Case

During the last few decades, India's gig economy has expanded substantially, with industry leaders like Uber and Ola leading the market. In 2018, a lawsuit was brought against all these businesses before the Supreme Court, requiring it to determine whether gig workers should be classified as autonomous contractors or workers.

The court determined that gig workers, who already have authority over their jobs and the freedom to select the time and place they operate, must be regarded as independent contractors rather than workers.

For companies that employ AI-powered systems to hire autonomous workers, the gig economy argument is important. The situation emphasises how crucial it is to comprehend the legal ramifications of the gig economy and make sure that employees have the freedoms and safeguards they need.

The Facial Recognition Case

2019 saw a facial-recognition software case heard by the Delhi High Court. A person filed the lawsuit, claiming that the Delhi police had breached his right to privacy by using facial-recognition software.

The court decided that the implementation of face recognition software by the Delhi police was not an invasion of confidentiality, as long as it was carried out with sufficient precautions. The Delhi police was instructed by the HC to take steps to guarantee that the software is only used for positive purpose and that any information gathered is not exploited.

For companies that employ technology to recognize faces driven by AI, this particular case is important. The case underlines the necessity of verifying that such technologies are utilised responsibly and professionally, with sufficient protections in place to protect personal data.

Other Developments

One significant breakthrough was the establishment of the "Committee on Artificial Intelligence (AI) for Economic Transformation" by the Government of India in August, 2017. Then in June, 2018, the group, which was entrusted with creating a framework for the usages of Artificial Intelligence in India, published its findings.

The National Plan for Artificial Intelligence, which was unveiled by the Indian Government in 2018, also provides an extensive roadmap for the advancement of AI in our country, including investments in R&D, educational and manpower development and regulatory guidelines.

Given the possible hazards involved with Artificial Intelligence systems that manage personal datasets, there have also been conversations in India about the requirement for Intelligence specific laws and regulations to safeguard information. Unfortunately, no explicit law has been approved on this subject as of now.

Nevertheless, there have been a number of significant advancements and conversations regarding the management of AI and its possible implications for society, despite the fact that there haven't been enough particular AI-related precedents in our country.

Conclusion

The aforementioned Indian AI precedents demonstrate the necessity for corporations and governments to comprehend the legal repercussions of AI. Organizations utilizing AI-powered services must make sure the independent workers/contractors are provided the freedoms and safeguards they deserve, whereas organizations that use AI to gather and keep individual information must ensure that they preserve personal individual privacy. Also, businesses must make sure that face recognition software as well as other AI-powered technologies are utilised morally, sensibly and with appropriate privacy protections.

LESSON ROUND-UP

- Artificial Intelligence (AI) describes the creation of smart computers that can carry out activities that traditionally call for human intelligence.
- Artificial Intelligence (AI) programmes that interact with people and carry out tasks include chatbots and virtual assistants.
- Customer service, healthcare, and education are just a few applications for chatbots and virtual assistants. Chatbots and virtual assistants enabled by AI can have advantages including higher productivity, increased customer happiness, and lower expenses.
- AI has important ramifications for cybersecurity and cyberspace. Data breaches and other cyberattacks are less likely when AI is used to quickly identify and respond to cyberthreats.
- Automation of basic cybersecurity chores with AI can free up human specialists to concentrate on more difficult problems.
- Cybercriminals may also utilise AI to develop more complex and focused assaults, so it’s critical for businesses to have robust cybersecurity safeguards in place.
- AI offers society both advantages and disadvantages. Possibilities include boosted productivity, better judgment, and fresh inventions.
- Difficulties include the loss of jobs, ethical issues, and prejudice in AI systems. When addressing these issues, it’s crucial to take use of AI’s potential.
- AI development and application must take ethics into account. Algorithm bias, a lack of transparency, and the potential for AI to be misused negatively are a few examples of ethical problems.
- During the AI development process, including data collecting, algorithm creation, and deployment, organizations should give ethical issues top priority.
- Although the legal environment surrounding AI is still developing, rules and regulations that affect AI development and deployment are currently in existence. Examples include legislation governing data privacy, consumer protection, and employment.
- One of the most important applications of AI in IP is the creation of new work as it can generate original work.
- AI focuses on performing tasks with the help of intelligence methods such as Reasoning, Machine Learning, Problem Solving, Perception, and Linguistic Intelligence.
- As AI technology becomes more advanced, it will likely be used more in areas related to intellectual property. This could lead to new legal issues and problems.

- Some of the IPR issues related to AI generated output are as follows:
  - Ownership and Authorship
  - Copyright Challenges
  - Patent Law
  - Other IPR Issues like data privacy, deep fakes, security of contents and alike
- AI technology has had an impact on landmark judgments passed by the courts in India. Hence many judgements by the court of law demonstrate the demonstrate the need for clarity and amendments in Indian intellectual property laws to address the emerging challenges posed by AI technology.
- However, Union Minister of State for Commerce and Industry, in a written reply in the Rajya Sabha on 9th February, 2024 stated Presently, there is no proposal to create any separate right so ram end the law in the context of AI-generated content.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. What is artificial intelligence, and how does it differ from other types of computer systems?
2. What are the different uses of AI, and what are their applications?
3. What are some of the ethical concerns surrounding AI, and how are they being addressed?
4. What are some of the most significant recent advancements in AI technology?
5. What are the limitations of AI, and what are some of the challenges facing the field?
6. How can individuals and organizations prepare for the impact of AI on the job market?
7. What is the future of AI, and what are some of the potential implications for society?
8. How can we ensure that AI is developed and deployed in an ethical and responsible manner?
9. Write a brief note on explaining IPR related challenges in AI generated material. Also describe whether there is requirement of amending the current regime of IPR laws to address the challenges generated out of the used of AI.

LIST OF FURTHER READINGS

- Wolfgang Ertel, "Introduction to Artificial Intelligence", Second Edition, Springer Publishing
- Philip C. Jackson, Jr., "Introduction to Artificial Intelligence", Third Edition, Dover Publications, Inc.
- Bart Custers, Eduard Fosch-Villronga, "Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice", TMC Asser Publishing, Springer
- P Mohan Chandran (August 2021) Artificial Intelligence (AI) & Intellectual Property Rights (IPR) Role, Impact, Contribution, Challenges, and Legal Implications of AI on IPR, Paperback – 17
- National Strategy for Artificial Intelligence, Niti Aayog, Government of India, June 2018. Available https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

LIST OF OTHER REFERENCES

- Adixon Robert (2019) Artificial Intelligence Opportunities and Challenges in Businesses, Towards Data Science. Available at https://towardsdatascience.com/artificial-intelligence-opportunities-challenges-in-businesses-ede2e96ae935
- Artificial Intelligence - Chatbots and other virtual assistants are here to stay – here’s what that means (2021), World Economic Forum.
- AI Compliance: What it is and Why You Should Care, EXIN. Available at https://www.exin.com/article/ai-compliance-what-it-is-and-why-you-should-care/
- Artificial Intelligence and Equality Initiative, Carnegie Council for Ethics in International Affairs.
- Artificial Intelligence: Example of Ethical Dilemmas (2022), UNESCO.
- Brian J. Bouchard (2023) Using AI for legal compliance, Seacoastline.
- Hacker Philipp et al (2022) AI Compliance – Challenges of Bridging Data Science and Law, Journal of Data and Information Quality Volume 14 Issue 3 Article No.: 21 pp 1–4
- Martin Dale Bolima (2023) The Chatbot Conundrum: Are Digital Assistants a Boom or a Bane, Disruptivetechasia. https://disruptivetechasia.com/
- Mohaghegh Shahab (2021) The Ethics of AI evolves with the Technology, The Way Ahead. See https://jpt.spe.org/
- S. Shanthi (April, 2023), Deeptech Experts on ChatGPT and the Future of AI in India, Entrepreneur India. Available on https://www.entrepreneur.com/en-in/technology/deeptech-experts-on-chatgpt-and-the-future-of-ai-in-india/449697
- Sterling Miller, Artificial intelligence and its impact on legal technology: to boldly go where no legal department has gone before, Thomson Reuters.
- Vedapalli Pavan (2022) Top 7 Challenges in Artificial Intelligence in 2023, Upgrad.com
- What are the Applications of AI in Legal Compliance Practices, Lawyers Monthly.
- Xhristoph Bartneck and et al. (2020) An Introduction to Ethics in Robotics and AI, Springer Briefs in Ethics, Springer International Publishing

Cyber Security

Lesson 2

KEY CONCEPTS

■ Cyber Crime ■ Cyber Security ■ Cyberspace ■ Information and Communication Technology (ICT) ■ Information Infrastructure ■ Legal Policy ■ Regulation ■ Strategy ■ Techniques

Learning Objectives

To understand:

- Role of Information and Communication Technology in the growth of business and society
- Concept of Cyber Security
- Significance of Cyber Security
- Challenges and Restriction in Cyber Security
- Solution towards enhanced level of Cyber Security
- Contemporary Techniques for ensuring effective Cyber Security
- Cyber Security Policies – National and International
- National and International Perspectives of Cyber Security
- Legal Assessment of Cyber Security
- Regulatory/Compliance Assessment of Cyber Security

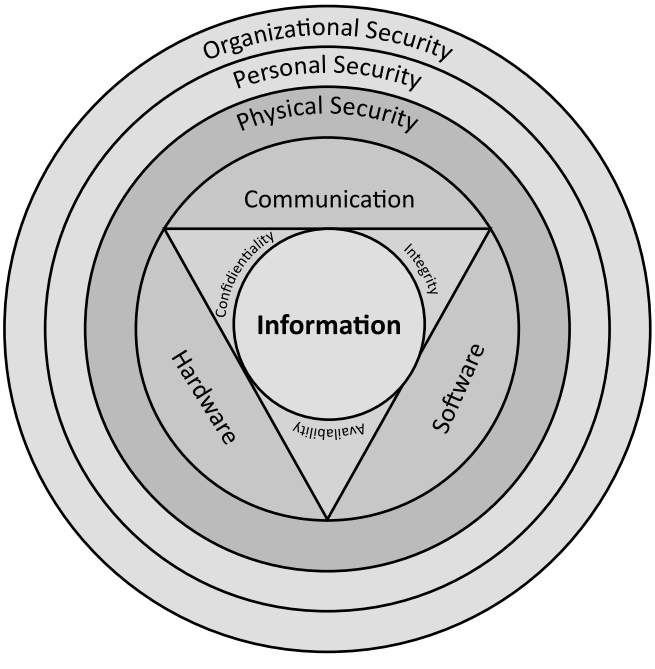
Lesson Outline

- Cyber Security
- Significance of Cyber Security
- Cyber Security Fundamentals
- Cyber Security Techniques
- Challenges and Restrictions
- Cyber Security Policies - National and International
- Requirement of Cyber Security Policies
- National Cyber Security Policy -2013: A Brief
- National Cyber Security Strategy: Recent Trends
- Cyber Security Policy: International Standards
- International Convention on Cyberspace
- Cyber Security: Legal and Compliance Assessment
- Cyber Security: Legal Assessment
- Cyber Security: Major Regulating Bodies and Compliance Requirements
- Cyber Security: Recent Government Initiatives in India
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

CYBER SECURITY

The quick development of Information and Communication Technologies (ICT) has revolutionized the Information Infrastructure (II). This facilitated swifter communications and easy interaction among people and organizations. With the people across the globe using ICT as the major mode of communication and transaction, we are witnessing the prevalence of information at all levels of a society, be it individual, organizational and state. Though the information revolution (*precisely to be called as "Information Era*") has created new opportunities, improved organizational efficiency and extraordinary global connectivity. Yet it has brought about new unconventional vulnerabilities and threats bearing social, economic, political and security implications. Among many banes suffered in ICT era, cyber security is a serious concern of individuals and organizations, public and private as well as national and international.

Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.



Alternatively, "Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system.

Further, it can also be said that Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber-attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

Hence, in simple words cyber security means protection of computers, networks and data from all possible threats.

Significance of Cyber Security

As discussed above, cybersecurity is the process of defending against malicious intrusions on networks, computers, servers, mobile devices, electronic systems, and data. It is also referred to as information technology security or electronic information security. With this detailed meaning itself, we understand that cybersecurity is crucial since it guards against some of the biggest challenges in cyber security, such as the theft and destruction of many data types. This covers delicate information, Personally Identifiable Information (PII), Protected Health

Information (PHI), personal data, data about intellectual property, and information systems used by the government and businesses. Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber-attack.

It has to be noted that an organization or an individual can develop a proper response plan only when he has a good grip on all the fundamentals of cyber security. Therefore, for an all-compassing cyber security in the interest of business growth and progression, following fundamental categories need to be ensured:

- Network security,
- Data integrity and privacy,
- Operational security.

Cyber Security Fundamentals

Confidentiality

Confidentiality is about preventing the disclosure of data to unauthorized parties. It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous. Often confidentiality is compromised by cracking poorly encrypted data, Man-in-The-Middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

Integrity

Integrity refers to protecting information from being modified by unauthorized parties. Standard measures to guarantee integrity include:

- Cryptographic checksums
- Using file permissions
- Uninterrupted power supplies
- Data backups

Availability

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

- Backing up data to external drives
- Implementing firewalls
- Having backup power supplies
- Data redundancy

CYBER SECURITY TECHNIQUES

There are many cyber security techniques to combat the cyber security attacks. The para discusses some of the popular techniques to counter the cyber-attacks.

1. Authentication

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber-crime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password (OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two types of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password. The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access which is present in a centralized sever. Or an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network. The system needs to authenticate the user and based on the credentials of that user, may or may not provide access to the used to the information he requested. The process of giving access to an individual to certain resources based on the credentials of an individual is known as authorization and often this process is gone hand-in-hand with authorization. Now, one can easily understand the role of strong password for authorization to ensure cyber security as an easy password can be a cause of security flaw and can bring the whole organization at high risk. Therefore, the password policy of an organization should be such that employees are forced to use strong passwords (more than 12 characters and combination of lowercase and uppercase alphabets along with numbers and special characters) and prompt user to change their password frequently. In some of the bigger organizations or an organization which deals in sensitive information like defense agencies, financial institutions, planning commissions, etc. a hybrid authentication system is used which combines both the username and password along with hardware security measures like biometric system, etc. Some of the larger organizations also use VPN (Virtual Private Network), which is one of the methods to provide secure access via hybrid security authentication to the company network over internet.

2. Encryption

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.

In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security of key while transmission is itself an issue. To avoid the transfer of key a method called asymmetric key encryption, also known as public key encryption, is used. In asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user possesses two keys viz. public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the

key only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B's public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be sent to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

3. Digital Signatures

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication.

The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is possess only by the original sender, is required for this purpose.

As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.

4. Antivirus

There are verities of malicious programs like virus, worms, trojan horse, etc. that are spread over internet to compromise the security of a computer either to destroy data stored into the computer or gain financial benefits by sniffing passwords etc. To prevent these malicious codes to enter to your system, a special program called an anti-virus is used which is designed to protect the system against virus. It not only prevents the malicious code to enter the system but also detects and destroys the malicious code that is already installed into the system.

There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

5. Firewall

It is a hardware/software which acts as a shield between an organizations network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you. There are two type of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organizations network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

- Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations network.

In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow “rules” and “policies” and based on these defined rules the firewalls can follow the following filtering mechanisms.

- Proxy- all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.
- Packet Filtering- based on the rules defined in the policies each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers.
- Stateful Inspection- rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.
- The firewalls are an essential component of the organizations network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use their network infrastructure to launch DOS attacks.

6. Steganography

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.

There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft, digital watermarks for IPR issues, etc.

Additionally following steps also ensures effective cyber security:

Source: https://www.conceptdraw.com/

CHALLENGES AND RESTRICTIONS

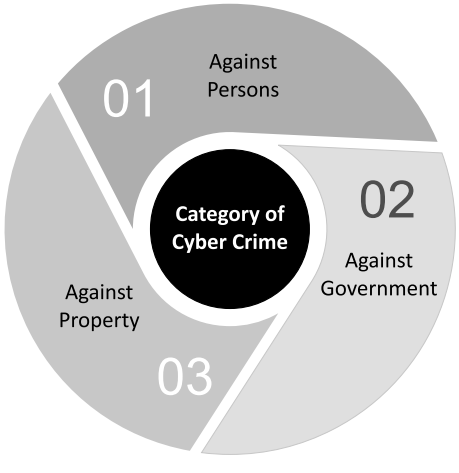
Cybercrime as one of the major challenges

Cyber security plays a vital role in the discipline of information security. Protecting the information against any probable has become one of the major challenges in the current scenario. The increased and innovative form of cybercrimes are one of the significant challenges in cyber security.

On one hand, technology has transformed the society towards inclusive development, on the other hand, this technology only has become vulnerable to cybercrime. It is worth to mention that with day to day innovated technology, newer kind of cybercrimes are taking place. Hence, technology and its innovation itself has become a major challenge and restriction to cyber security. Our first question in the context must be that how the technology is vulnerable at all and how the technology itself is one of the challenges of cyber security. The answer is simple: our dependability and trust on technology. Therefore, the intruders exploit the technology to create threat for our cyber security. From its inception, the protocols that drive Internet, by and large, were not designed for a future that involved exploitation. Indeed, there was little expectation at its birth that one day we might require to mitigate against attacks such as a Distributed Denial of Service (DDoS), or that a webcam you buy off the shelf might need security protocols to prevent it being hacked and used to spy on you. As per the study titled Cybersecurity: Threats, Challenges and Opportunities published by Australian Computer Society (ACS)[1] – it is claimed that in the recent times though there is much greater awareness to cyber security, yet devices as well as software connected to the internet either have poor security measures or no security at all built-in. For some, the security simply wasn't part of the design scope.

It is further claimed by ACS in the above-mentioned study that *"in many cases, the idea that a device might be used for nefarious purposes isn't even considered. And the result is that today cybercrime almost exclusively leverages the lack of security-focused design in everything from your smartphone and web browser through to your credit card and even the electronic systems in your car. The nature of threats Cybercrime comes in a variety of forms ranging from denial-of-service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransomware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers). It's no surprise then that the sheer scope of possible attacks is vast, a problem compounded by what's known as the attack surface: the size of the vulnerability presented by hardware and software. This is further compounded by the fact that hardware and software may provide multiple vectors for attacks, such that an iPhone might have multiple different vulnerabilities, each of them a possibility for exploitation."*

From the above, we can deduce that cybercrime has to do with wrecking of havoc on computer data or networks through interception, interference or destruction of such data or systems.



1. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Cyber-crime involves committing crime against computer systems or the use of the computer in committing crimes[2]. This is a broad term that describes everything from electronic cracking to denial-of-service attacks that cause electronic commerce sites to lose money.

Generally, cybercrimes can be basically divided into 3 major categories:

1. Cybercrimes against persons.
2. Cybercrimes against property.
3. Cybercrimes against government.

Snap-Shot of Common Kinds of Cyber-attacks[3]

- ***Denial of Service Attacks (DOS):*** DOS is one of the attack where an attacker creates a memory resource or computing too full or too engaged to handle legitimate queries, thus denying legitimate user access a machine.
- ***Remote to Local Attack:*** A Remote to Local (R2L) attack is a kind of attack where an attacker sends packets to a machine over networks, then exploits the machine's vulnerability to illegitimately increase local access to a machine. It happens when an attacker who has the capability to send packets to a machine over a network but who does not have an account on that machine develops some vulnerability to achieve local access as a user of that machine.
- ***User to Root Attacks:*** User to root attacks is a kind of attacks where an attacker initiates with access to a moderate user account on the system and is able to expand vulnerability to grow root access to the system in which the attacker starts out with access to a normal user account on the system and is able to exploit some vulnerability to gain root access to the system.
- ***Probing:*** Probing is another kind of attack where an attacker scans a network to gather information or discover known vulnerabilities. An attacker with map of machine and services that are available on a network can use the information to notice for exploit.
- ***Attacks Detection Strategies:*** Attacks Deletion Strategies is one of the attacks. Modern cyber-attack detection systems monitor either host computers or network links to capture cyber-attack data.
- ***Signature based Approach:*** Signature based approach of mishandling discovery works just comparable to the existing anti-virus software. In this approach the semantic description of an attack is analyzed and details is used to structure attack signatures. The attack signatures are structured in such a way that they can be searched using information in audit data logs produced by computer systems.
- ***Misuse/Misbehavior:*** Misuse (signature) recognition is based on the awareness of system vulnerabilities and known attack patterns. Misuse detection is concerned with discovering intruders who are attempting to break into a system by exploiting some known vulnerability. Ideally, a system security administrator should be aware of all the acknowledged vulnerabilities and eradicate them.
- ***Reconnaissance Attacks:*** Reconnaissance attacks is the type of attack which involve unauthorized detection system mapping and services to steal data.
- ***Access Attacks:*** An attack where intruder increase access to a device to which he has no right for access.

2. Aaron J. Burstein. Towards a culture of cybersecurity research. Harvard Journal of Law and Technology, 22:230_240, 2008
3. Dr. V.Kavitha et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.11, November- 2019, pg. 1-6

- ***Cyber-crime:*** The use of computers and the internet to exploit users for materialistic gain.
- ***Cyber Espionage:*** The act of using the internet to spy on others for gaining benefit.
- ***Cyber Terrorism:*** The use of cyber space for creating large scale disruption and destruction of life and property.
- ***Cyber War:*** The act of a nation with the intention of disruption of another nation's network to gain tactical and military.
- ***Active Attacks:*** An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise.
- ***Passive Attacks:*** An attack which is primarily eaves dropping without meddling with the database.
- ***Malicious Attacks:*** An attack with a deliberate intent to cause harm resulting in large scale disruption.
- ***Non-Malicious Attacks:*** Unintentional attack due to mishandling or operational mistakes with minor loss of data.
- ***Attacks in Mobile Ad Hoc Network*** (**MANET**): Attacks which aim to slow or stop the flow of information between the nodes.
- ***Attacks on Wireless Sensor Network*** (**WSN**): An attack which prevents the sensors from detecting and transmitting information through the network.

To be precise, cybercrime and its increased frequency are one of the major challenges in cyber security. Handling cyber security is still a very huge concern of present-day Governments and private sectors throughout the globe are taking many measures in order to secure these cybercrimes.

Major reasons confirming significance of Cyber Security in a predominant digital world:

- Cyber-attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive.
- Cybercriminals are using more sophisticated ways to initiate cyber-attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Solution – Confrontation Strategy to Challenges and Limitations

In order to confront the challenges of cyber security, we must adhere to following cyber security parameters:

- Identify threats
- Identify vulnerabilities
- Access risk
- Explore possible loss and contingency plan
- Respond to cyber security accident
- Establish contingency plan

Additional Challenges and Limitations: Recent Trends[4]

In addition to the cybercrimes as discussed above, recently new forms of challenges and limitations are identified in cyber world. Let's discuss the challenges as well as their probable solution as below:

Sr. No.	***Challenges***	***Solution***
1.	*Adapting to A Remote Workforce* In recent times, most frequent security issues associated with working from home. People working from home may accidentally provide cybercriminals access to their computers or company files due to negligence, fatigue, or ignorance. Hence, safeguarding remote and hybrid working environments will continue to be the biggest challenge in cyber security.	The key to secure remote working is cloud-based cybersecurity solutions that protect the user's identity, device, and the cloud.
2.	*Emerging 5G Applications* The cybersecurity is aggressively endangered with characteristics of 5G networks. Though the nation attempting to adopt 5G, yet much research is needed to evaluate and handle its hazards.	It is required to build a mechanism for protecting users' data, their privacy and trust in the firms they are working with.

4. Preethiga Narasimman (2022), Most Extensive Cyber Security Challenges and Solutions in 2023, Knowledgehut, upGrade.

Sr. No.	Challenges	Solution
3.	*Blockchain and Cryptocurrency Attack* Both insiders and outside attackers can launch attacks on blockchain-based systems. Numerous of these attacks are attempted with well-known techniques like phishing, social engineering, attacking data in transit, and focusing on coding errors.	In order to prevent these attacks blockchain can be combined with other cutting-edge technologies like Artificial Intelligence (AI), Internet of Things (IoT), and Machine Learning (ML).
4.	*Ransomware Evolution* A form of virus known as ransomware locks down files on a victim's computer until a ransom is paid.	It is imperative to regularly backing up their devices and also utilizing the most recent and updated anti-malware and anti-phishing solutions.
5.	*IoT Attacks* IoT attacks are cyberattacks that employ any IoT device to access sensitive data belonging to users. Attackers typically damage a gadget, implant malware on it, or gain access to additional information belonging to the firm.	To implement the increase in security of IoT devices, one must look for robust security analysis and maintain communication protection methods like encryption.
6.	*Cloud Attacks* A cyberattack that targets remote service providers using their cloud infrastructure to offer hosting, computing or storage services is called a cyberattack. SaaS, IaaS, and PaaS service delivery paradigm attacks on service platforms are examples of this.	Awareness of the fundamentals as well as the most widespread vulnerabilities related to cloud security shall be increased.
7.	*Phishing And Spear-Phishing Attacks* This kind of email assault involves an attacker pretending to be from a relevant, reputable company to get sensitive information from users through electronic communication fraudulently.	Using anti-phishing tools such as Antivirus software and Anti-phishing Toolbar, sandboxing the E-mail attachments, and training to users – are few solutions to tackle phishing and spear-phishing attacks.
8.	*Software Vulnerabilities* Software flaws (including mistake in software coding) which may provide an attacker access to a system are known as vulnerabilities in software.	Software that manages vulnerabilities has a cybersecurity strategy. It proactively scans the network for vulnerabilities, identifies them, and offers remedial advice to lessen the likelihood of future security breaches.
9.	*Machine learning and AI Attacks* AI attacks can also threaten cyber security.	Software must be secured coding techniques, and the entire software development process must incorporate automatic security testing.

Sr. No.	Challenges	Solution
10.	*Bring Your Own Device Policies (BYOD)* BYOD are more likely to breach business networks since they are less secure and more likely to have security flaws than corporate devices. Therefore, enterprises of all sizes must comprehend and address BYOD security.	Services for BYOD are among the management alternatives, and the process begins with an enrollment app that adds a device to the network. It is always advisable to either configure company-owned devices individually or in bulk.
11.	*Insider Attacks* Sometimes current or former employee or business acquaintance gains unauthorized access on an organization's system. They are challenging to stop, hard to find, and take forever to clean up.	The danger of insider attacks could be lessen by combining strict procedures and cleverly used technologies.
12.	*Outdated Hardware* Many firms might not be aware of the severe security risk posed by old gear. Businesses that put off upgrading their gear because of the additional cost may spend more money than necessary to recover from a cyberattack. Additionally, security breaches can harm an organization's reputation and result in a decline in business.	Outdated software shall be ignored and updated time to time. It is essential for preventing cybercrime.
13.	*Serverless Application Vulnerability* Serverless computing, event-driven nature and lack of persistent data run may threaten cyber security.	To seek timely assistance of cybersecurity professionals.
14.	*Supply Chain Attacks* A supply chain assault occurs when someone compromises your digital infrastructure by using an external supplier or partner who has access to your data and systems.	One shall maintain a highly secure build infrastructure and upkeep secure software updates.
15.	*Mobile Malware* Attackers are focusing more on smartphones and tablets, which has led to an increase in mobile malware.	The best strategies for enterprises frequently entail implementing an official Bring Your Device (BYOD) or Enterprise Mobility Management (EMM) framework.
16.	*Attacks on Application Programming Interface (APIs)* The malicious or attempted use of an API by automated threats, such as access violations, bot assaults, or abuse, is known as an API attack. Mass data losses, theft of personal information, and service interruption can all be caused by an API attack.	To protect from attacks on API, organizations can promote the use of push notifications, apply two-factor authentication, and encrypt the data.

Sr. No.	Challenges	Solution
17.	*Drone-Jacking* Business security and related law enforcement (specially aviation laws) are threatened with drones hacked by the attackers.	Fortunately, there are various ways to increase the security of any drone against the risk of drone hacking. You must regularly update the drone's firmware.
18.	*Growth of Hacktivism* Hacktivists carry out obstructive or harmful actions in support of a cause, whether political, social, or spiritual.	The solutions for Hacktivism include a comprehensive plan - ● Creating a response plan ● Check-in the vulnerabilities ● Improving the security system ● Monitoring the social media to know Hacktivists' public agendas.
19.	*Preventive Measures of Social Engineering* Cybercriminals utilize social engineering to successfully get important information from their targets by manipulating their psychology. It causes users to commit security errors and steal important information, like banking passwords, login information, system access, and other similar data.	Organizations should use a technology-and-training-based strategy to prevent this kind of cyberattacks. Some examples are integrated strategy, including multi-factor identification, email gateways, reputable antivirus software, employee training, and others, to prevent such social engineering attacks.
20.	*Security of Remote Work and Hybrid Workforces* A comprehensive examination of access techniques is required, especially for distant users. It is imperative to provide secure access to programs for both on-premises and remote workers. The same issues with remote work also arise with hybrid work, such as the absence of a network boundary, the requirement to support access from a wide range of devices, and the need to secure on-premises infrastructure.	Identifying shadow IT, lowering risk via URL and web category filtering, implementing virus protection, and establishing data loss prevention (DLP) are just a few of the approaches to securing remote workers and their applications.
21.	*Firmware Attack Weaponization* In the recent past, the number of firmware vulnerabilities has increased approximately five-fold, while making it one of the grave cyber security issues and challenges. Mobile and distant workers who use public networks and non-company devices may be particularly exposed.	In order to address this issue, it is significant to buy equipment with additional firmware security layers, keeping current PCs as up-to-date as possible, and, as always, never putting in non-recognizable USB devices.

Sr. No.	Challenges	Solution
22.	*Deep Fake Technology* Deep fake threats can be classified into societal, legal, personal, and traditional cybersecurity.	There have typically been two solutions proposed to address the issues caused by deep fakes – (a) either employ technology to identify fake technology or (b) increase literacy and/or skill in this regard.

RISE OF AI THREATS AND CYBERSECURITY: PREDICTIONS FOR 2024[5]

Rise of Specialized Language Models

One thing can be safely predicted is that artificial intelligence (AI) is not going anywhere. A case in point: large language models have transformed organizational cybersecurity. Large language models arm security teams with the incredible power to sift large amounts of data into actionable insights through simple queries. These sophisticated models have demonstrated remarkable capabilities in understanding and generating human-like text, fostering advancements across various domains.

Yet, while large language models have certainly had a huge impact, they are still limited in their ability to understand and interpret the intricacies of specialized cybersecurity datasets. Therefore, in 2024, security teams will transition to small language models. These agile, specialized models will offer security teams access to tailored and actionable insights. Real-time data training will be the secret weapon, empowering security teams to adapt swiftly to the ever-shifting threat landscape.

Threat Actors will use AI to get ahead

As mentioned, AI will likely be a permanent fixture in our lives; it's how cybersecurity defenders respond to it that matters. The emergence of generative AI has sparked a heated debate concerning its uses and the ethical dilemma it presents.

Organizations must work quickly to harness generative AI before threat actors can exploit it to their advantage. From present perspective, it appears that threat actors will take the upper hand in 2024.

It may take the form of sophisticated phishing campaigns, a barrage of deepfakes and hackers gaining access to detailed information about their targets while also getting around endpoint security defenses. Security leaders are advised to prepare for the coming wave of AI-generated threats.

Spike in Third-Party Data Breaches

Beyond AI, 2024 could see record-breaking data breaches. In 2023, the landscape of global data breaches significantly intensified from previous years, including a 72% increase in the number of data compromises over the previous high in 2022.

Future breaches will primarily affect major tech companies with vast amounts of customers (and, by extension, sensitive data). This targeting is due to a number of factors, including API proliferation, data digitization and undetected zero-day vulnerabilities. Organizations should establish and enforce clear and actionable key performance indicators to manage and measure these risks effectively.

5. Aleksandra Yampolskiy (February 15, 2024) What does 2024 have in store for the world of cybersecurity? Cyber Security, World Economic Forum

"Threat actors will continue evolving their tactics, techniques and procedures and organizations must pivot accordingly."

— Alex Yampolskiy, CEO, Security Scorecard

Cyber expertise is coming to the Boardroom

Earlier this year, the US Securities and Exchange Commission released a set of regulations requiring publicly traded companies to disclose new details about cyberattacks as well as cybersecurity oversight at the board level. These disclosure requirements will empower chief information security officers (CISOs) to engage in meaningful discussions with their board members, cultivating a culture of cybersecurity literacy.

These regulations highlight the importance for executive boards to approach and address cybersecurity risks like any other material business risk. It is a timely reminder of the importance of boards, the C-suite and other business leaders aligning on specific metrics for cyber risk and increasing the cadence and substance of ongoing strategic risk management.

This new governance is an opportunity for both the CISO and board members to refine their communication skills in order to bring cyber-literacy to the boardroom and increase their organization's cyber resilience.

Managing Third-Party risk to stay resilient

Threat actors will continue evolving their tactics, techniques and procedures and organizations must pivot accordingly. This year, we witnessed several massive supply chain attacks whose effects are still being felt today. As a result, organizations must re-examine not only their own security practices but also those of their vendors and third-party suppliers. Staying proactive is the key to staying cyber resilient.

As we look towards a cybersecure 2024, it's important to remember that there are as many opportunities as challenges and we are presented with more tools to combat the threats at our door. Leveraging advanced technologies, fostering global collaboration and prioritizing cybersecurity education and awareness can mitigate risks and ensure a secure digital future.

Under this perspective and with ever evolving is very clear is that it is increasingly important to stay ahead in the ever-evolving world of cybersecurity.

CYBER SECURITY POLICIES - NATIONAL AND INTERNATIONAL

Cyberspace: Boon as well as Bane[6]

As discussed, cyberspace[7] is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to powering India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics),

6. Source: National Cyber Security Policy, Ministry of Electronics and Information Technology, Government of India
7. ISO / IEC 27032-2012

Education (eLearning, virtual classrooms, etc.) and financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large-scale IT infrastructure with corporate / private participation.

In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation and Inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

Owing to the numerous benefits brought about by technological advancements, the cyberspace in latest times is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace has become and is further expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

Indeed, cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-state actors. Cyber-attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures.

Requirement of Cyber Security Policies

A cyber related incident of national significance may take any form; an organized cyber-attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, and for the required unified action, the Government of India has enacted a National Cyber Security Policy, with an integrated vision and a set of sustained & coordinated strategies for implementation.

NATIONAL CYBER SECURITY POLICY -2013[8]: A BRIEF

The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also

8. Source:https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy2013%281%29.pdf

enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

Vision

To build a secure and resilient cyberspace for citizens, businesses and Government.

Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

Objectives

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.
- To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
- To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.
- To develop suitable indigenous security technologies through frontier technology research, solution-oriented research, proof of concept, pilot development, transition, diffusion and commercialization leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.
- To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.
- To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.
- To provide fiscal benefits to businesses for adoption of standard security practices and processes.
- To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft.
- To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.
- To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy.

- To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Strategies

A. Creating a secure cyber ecosystem

- To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.
- To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.
- To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.
- To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.
- To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.
- To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.
- To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

- To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.
- To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (e.g. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).
- To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.
- To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.
- To encourage secure application / software development processes based on global best practices.
- To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

- To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

- To encourage use of open standards to facilitate interoperability and data exchange among different products or services.
- To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

- To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.
- To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.
- To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

- To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
- To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.
- To operationalize 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.
- To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well-coordinated, multi-disciplinary approach at the National, Sectoral as well as entity levels.
- To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

- To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.
- To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.
- To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

- G. Protection and resilience of Critical Information Infrastructure
- To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.
- To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.
- To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.
- To encourage and mandate as appropriate, the use of validated and certified IT products.
- To mandate security audit of critical information infrastructure on a periodic basis.
- To mandate certification for all security roles right from CISO / CSO to those involved.
- in operation of critical information infrastructure.
- To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

- To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long-term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.
- To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.
- To facilitate transition, diffusion and commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.
- To set up Centers of Excellence in areas of strategic importance for the point of security of cyber space.
- To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution-oriented research.

I. Reducing supply chain risks

- To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.
- To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.
- To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

- To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.
- To establish cyber security training infrastructure across the country by way of public private partnership arrangements.
- To establish cyber security concept labs for awareness and skill development in key areas.
- To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

- To promote and launch a comprehensive national awareness program on security of cyberspace.
- To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.
- To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

- To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.
- To create models for collaborations and engagement with all relevant stakeholders.
- To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

- To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.
- To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.
- To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

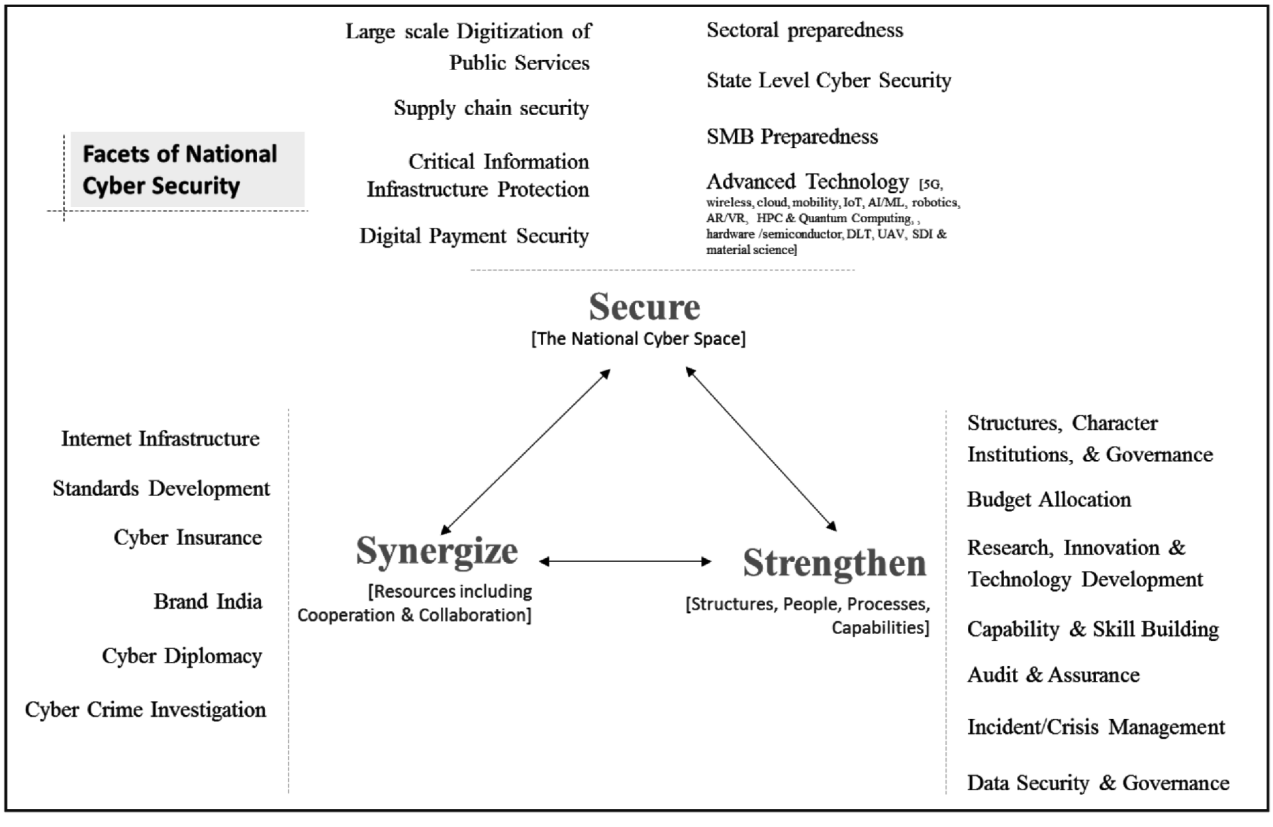
N. Prioritized approach for implementation

- To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.
- **Operationalization of the Policy**

  This policy shall be operationalized by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

NATIONAL CYBER SECURITY STRATEGY: RECENT TRENDS

In 2020, the National Cyber Security Strategy was conceptualized by the Data Security Council of India (DSCI). The report[9] focused on 21 areas to ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India.



Source: Data Security Council of India

Key highlights of DSCI – National Cyber Security Strategy Report, 2020 are as follows:

- Concerted and well-thought-through effort for ensuring security right from design to entire phases of life cycle of large-scale digitization of public services projects.
- Two-pronged approach for supply chain security, for product procured/deployed and product developed in India.
- Empowered and resourced security function in critical information infrastructure sector, with specific attention to SCADA/OT security.
- Index for sectoral preparedness and monitoring performance.
- Given the urgency created by rising cyber threats, Government should carve out separate budget for cybersecurity.
- Critical infrastructure protection demands fixing the structural problem by empowering security leadership and strengthening security in both IT and OT environment.
- Synergize role and functions of various agencies and restructure them with role and functional responsibility aligned to the national strategy and execution blueprint.

9. Available at https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%20 2020%20DSCI%20submission.pdf

- Orchestrate all efforts of Government in bilateral, multilateral, regional cyber cooperation, and participation in Global forums and influence and drive the agenda aligned to India's interests in Cyber Space and Security.
- Bootstrap the Cyber Security Capability building program in states through central funding on lines of e-Government.
- Capacity building, managing risks arising from technology innovation, R&D and commercialization of insights, digitization of SMB sector, state and sector preparedness, data security governance and securing digital payments have become fundamentals of securing a nation and hence Government must leverage cybersecurity strategy 2020 to strengthen these fundamental components.
- Attracting bright young minds to the field of cyber security through awareness, targeted campaigns, and providing enticing career opportunities.
- Incentivization contributions to for developing cybersecurity technology, development of training infrastructure, investing in the testing labs, active participation in technology standards making, demonstration of India's capabilities in the global market, and for improving preparedness of SMB sector.
- Calling for development of an index of preparedness of states in cybercrime investigations that would factor investment made, reach and scale of the effort, undertaken experimentations, timeliness in the resolution of the cases, and improvement in the conviction rate.

Draft National Cyber Security Strategy

In the wake of recent cyber-attacks as well as of urgent necessity of cyber security, the National Security Council Secretariat (NSCS) has formulated a draft National Cyber Security Strategy, which holistically looks at addressing the issue of security of national cyberspace.[10]

Responding to a query from Lok Sabha members Minister of Electronics and Information Technology Ashwini Vaishnaw said the NSCS had formulated a draft strategy. However, the timeline for its implementation and other details were not mentioned.

National Cyber Security Strategy 2023: Latest Updates[11]

Lt Gen Rajesh Pant (retd), national cyber security coordinator, National Security Council Secretariat, said that the National Cyber Security Strategy 2023 is in final stages of approvals.

National Cyber Security Strategy 2023 is an important document that supersedes the 2013 policy. From 2013 till 2023, the world has changed as new threats have emerged calling for new strategy. The document will be put in public domain after a final check by the committee to ensure that nothing confidential is released.

The government has been consistently working on providing structured guidance on cyber security to critical sectors of the nation which include telecom, power and energy, transportation, finance, strategic entities, government entities and health. This major initiative is driven by the National Critical Information Infrastructure Protection Centre under a project funded by the National Security Council Secretariat.

Organizations can use the NCRF to improve their cybersecurity posture, reduce data breach risk or any cybersecurity incident, ensure compliance with regulations and enhance operational efficiency.

10. The Hindu (December 14, 2022) Draft cybersecurity strategy has been formulated: Centre However, the timeline for its implementation and other details were not mentioned.

11. Reproduced from Inamdar Nadeem (June 13, 2023), National Cyber Security Strategy 2023 to be released soon, The Hindustan Times. Available at https://www.hindustantimes.com/cities/pune-news/sena-ubt-firm-on-contesting-sangli-seat-101712345210167.html

The official said that the Centre has spent ₹700 crore on national cyber awareness and cyber skilling programme initiative.

There are two aspects to cyber security. First is cyber hygiene for all of us and cyber skilling of the cyber workforce i.e. the people who enforce cyber security. For the first part we have a programme ISEA (Information Security Education and Awareness) programme which is now in phase II, implemented by the ministry of electronics and IT and CDAC, Hyderabad is the nominated agency for spreading public awareness. Cyber skilling is another programme run in government and private universities where syllabus has changed as per the changing needs. I agree that a lot more needs to be done.

Bharat National Cyber Security Exercise 2023: Elevating India's Cybersecurity Preparedness to New Heights[12]

The prestigious SCOPE Convention Centre in New Delhi bore witness to the Bharat National Cyber Security Exercise (NCX) 2023, an event of monumental significance spanning from October 9th to 20th October 2023. This momentous occasion is a remarkable milestone in India's unwavering quest for cybersecurity excellence.

This flagship event served as a unifying platform for over 300 participants, representing a diverse spectrum of government agencies, public organizations, and the private sector, all resolutely committed to the safeguarding of critical information infrastructure.

Organized by the National Security Council Secretariat (NSCS), Government of India(GoI), in strategic partnership with Rashtriya Raksha University(RRU), Bharat NCX 2023, has been stressed upon the importance of cyber security in today's world and mentioned that future battle will be fought primarily in the cyber domain. Experts also stressed on the importance of operational technology in the domain of cyberspace.

Bharat NCX 2023 represents a defining moment in India's unwavering commitment to cybersecurity excellence, underscoring the paramount importance of collaboration and knowledge-sharing among stakeholders from government, public, and private sectors.

Bharat NCX 2023, organised intense training for the participants over six days and a red on blue Live Fire cyber exercise over five days, wherein participants challenged their cyber skills against a determined adversary. The exercise also had a Strategic Track for leadership level discussions on cyber threat landscape, incident response, crisis management to handle real world cyber challenges.

Bharat NCX 2023 while making endeavours to fortify our cyber defences also highlighted the need for a National Cyber Security Strategy resulting in governance structures supported by legal frameworks, efficient processes for threat intel sharing and enhancing Public Private Partnership.

In an era characterized by burgeoning digitalization, Bharat NCX 2023 serves as a compelling reminder of the paramount importance of collective vigilance and preparedness in safeguarding our nation's invaluable digital assets.

CYBER SECURITY POLICY: INTERNATIONAL STANDARDS

Considering the global flow of the information and communication technology, states now a days are giving increased attention to the governance of cyberspace.[13] Accordingly, in order to ensure effective governance

12. Reproduced from Bharat National Cyber Security Exercise 2023 Concludes: Elevating India's Cybersecurity Preparedness to New Heights (October 23, 2023), Press Information Bureau of India. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1970225#:~:text=Bharat%20NCX%202023%20while%20making,and%20enhancing%20Public%20Private%20Partnership.

13. The technical architecture that allows the global internet to function.

The Hindu (December 14, 2022) Draft cybersecurity strategy has been formulated: Centre However, the timeline for its implementation and other details were not mentioned.

in cyberspace[14] the role of international law in the cyber context has gained increased prominence. There are certain standards which effectively ensure cyber security and open for international adoption. A brief list of such international standard is as below:

- **ISO 22301**

  ISO 22301 is an international standard that outlines how organizations can ensure business continuity and protect themselves from disaster. The Standard provides a framework for a comprehensive BCMS (business continuity management system). It can be used by any organization, regardless of size, industry, or location.

- **ISO/IEC 27001**

  ISO 27001 is an international standard for information security that provides a framework for managing sensitive company information. The Standard includes requirements for developing an ISMS (information security management system), implementing security controls, and conducting risk assessments. The Standard's framework is designed to help organizations manage their security practices in one place, consistently and cost-effectively.

- **ISO/IEC 27002**

  ISO 27002 is the code of practice for information security management. It provides guidance and recommendations on how to implement security controls within an organization. ISO 27002 supports the ISO 27001 standard, which provides the requirements for an ISMS.

- **ISO/IEC 27031**

  ISO 27031 is a standard for ICT (information and communications technology) preparedness for business continuity. It provides guidance on how organizations can use ICT to protect their business operations and ensure continuity in the event of an incident or a disaster. Achieving compliance with ISO 27031 helps organizations understand the threats to ICT services, ensuring their safety in the event of an unplanned incident.

- **ISO/IEC 27032**

  ISO 27032 is an internationally recognized standard that provides guidance on cybersecurity for organizations. The Standard is designed to help organizations protect themselves against cyber-attacks and manage the risks associated with the use of technology. It is based on a risk management approach and provides guidance on how to identify, assess, and manage cyber risks. The Standard also includes guidance on incident response and recovery.

- **ISO/IEC 27701**

  ISO 27701 specifies the requirements for a PIMS (privacy information management system) based on the requirements of ISO 27001. It is extended by a set of privacy-specific requirements, control objectives, and controls. Organizations that have implemented ISO 27001 can use ISO 27701 to extend their security efforts to cover privacy management. This can help demonstrate compliance with data protection laws such as the California Privacy Rights Act (CPRA) and the EU General Data Protection Regulation (GDPR).

14. How states, industry, and users may use this technology.

INTERNATIONAL CONVENTION ON CYBERSPACE[15]

Duncan Hollis in his work – A Brief Primer on International law and Cyberspace (2021)[16] have stated that "*With few exceptions - most notably, the Budapest Convention on Cybercrime and African Union Convention on Cyber Security and Personal Data Protection (yet to be notified), international law does not have tailor-made rules for regulating cyberspace. Moreover, the technology is both novel and dynamic. Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations, including the UN General Assembly's First Committee on Disarmament and International Security, the G20, the European Union, ASEAN, and the OAS have affirmed that existing international law applies to the use of information and communication technologies (ICTs) by states. As such, the current discourse centers not on whether international law applies, but rather how it does so.*

Elements of Effective Cyber Security Policy[17]

A cybersecurity policy, however, can vary organization to organization or state to state. It can take different shapes or forms, depending on the type of organization, nature of business, operational model, scale, regulatory requirement of a state and alike. Yet, there are certain factors which helps in the effective use of cybersecurity policies:

Acceptable Use Policy (AUP)

Access control policy

Business continuity plan

Data breach response policy

Disaster recovery plan, and

Remote access policy

Asoke Mukerji[18] in his paper on "The Need for an International Convention on Cyberspace" has also highlighted the signification of global regulation on cyberspace and need of global standards of cyber security. He further stated that Emerging concepts related to the application of cyber technologies alike Internet of Things (IoT), Artificial Intelligence (AI), and robotics - are propelling the world into the Fourth Industrial Revolution. Though these phenomena are currently being tested and applied within a few countries, yet their impact will be felt globally due to the complex interlinkages of cyberspace. These interlinkages revolve around cyber technologies and infrastructure. Hence, he highlighted that all four stakeholders—governments, businesses, academia, and civil society—play a critical role in identifying the strengths and vulnerabilities of cyberspace. In varying degrees around the world, all four have expressed interest in creating the building blocks for a multi-stakeholder international framework for cyberspace.

INTERNATIONAL CONVENTION ON CYBERSPACE: A BRIEF TIMELINE

At the global level, issues in cyberspace require effective international cooperation and the same have been raised by the five multi-stakeholder Global Conferences on Cyber Space held so far since 2011.

15. Students to Note: As the global context of cyber security is quite wide, therefore the brief of international convention and latest development is discussed in this chapter. This is only indicative and not descriptive. Students may also refer – Duncun B. Hollis (2021) A Brief Primer on International law and Cyberspace, Carnegie Endowment for International Peace.

16. Published with Carnegie Endowment for International Peace.

17 Source: How to Create An Effective Cybersecurity Policy (2022) Cyber Management Alliance

18. India's former Permanent Representative to the United Nations in New York and supervised India's participation in negotiations that resulted in the adoption of the UN 2030 Agenda for Sustainable Development.

- 2011 - The London Conference - the first conference on cyberspace - identified five broad themes for international cooperation in cyberspace. These were economic growth and development, social benefits, international security, tackling cybercrime and ensuring safe and reliable access to cyberspace.
- 2012 - Subsequently, Budapest Conference highlighted the importance of capacity building in cyberspace, the linkage between internet security and internet rights, as well as the role of civil society in cyberspace policies;
- 2013 - Seoul Conference highlighted the need for universal access to cyberspace to accelerate development;
- 2015 - Hague Conference established a Global Forum on Cyber Expertise (GFCE) to promote capacity-building.
- 2017 - The Fifth Global Conference on Cyber Space was hosted by India in 2017, with a focus on "a secure and inclusive cyberspace for sustainable development." The intent of the conference was to promote the importance of inclusiveness and human rights in global cyber policy, to defend the status quo of an open, interoperable and unregimented cyberspace, to create political commitment for capacity building initiatives to address the digital divide and assist countries, and to develop security solutions in a balanced fashion that duly acknowledge the importance of the private sector and technical community.
- 2017 onwards - UN General Assembly ("UNGA") adopted a resolution in December 2018 to enhance "broad international cooperation" and accordingly Group of Governmental Experts ("GGE") were advised to focus on how international law applies to cyberspace and mandated the GGE to engage in multi-stakeholder consultations to generate greater acceptability for its eventual recommendations. The reconvened 25-member GGE mandated by the aforementioned resolution held its first meeting December 2019. Apart from its core mandate for recommending norms for cyber-security, the GGE discussions encouraged the identification of voluntary confidence-building measures and capacity-building to enhance cyber-security. The outcome of this GGE were reported to the UNGA in 2021, and accordingly urgency being felt by governments for effective international cooperation in securing cyberspace.
- It is to be noted that in addition to the original UN Group of Governmental Experts forum, UN processes now also encompass an Open-Ended Working Group in the UN General Assembly's First Committee, as well as a Third Committee process on a UN cybercrime convention.
- The 2030 Agenda of Sustainable Development Goal has also emphasized a "people-centered, inclusive, and development oriented" cyberspace, including for the application of cyber technologies to accelerate sustainable development.

CYBER SECURITY: LEGAL AND COMPLIANCE ASSESSMENT

Recently, in a reply to the set of queries raised in Lok Sabha, the Minister of State for Electronics and Information Technology has informed[19] – that *the policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. With the borderless cyberspace coupled with the anonymity, along with rapid growth of Internet, rise in cyber-attacks and cyber security incidents is a global phenomenon. Indian Government is fully cognizant and aware of various cyber security threats. The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India.*

CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing

19. Source: Lok Sabha Questions (December 14, 2022), Government of India. Available on http://164.100.24.220/loksabhaquestions/annex/1710/AU1374.pdf

tailored alerts with organizations across sectors for proactive threat mitigation actions by them. According to the analysis by CERT-In, the Internet Protocol (IP) addresses of the computers from where the attacks appear to have originated from a number of countries.

In the recently notified cyber security direction CERT-In has now made it mandatory for all incidents to be mandatorily reported to CERT-In. As per the information reported to and tracked by CERT-In, year-wise number of cyber security incidents areas below :

S. No.	*Year*	*Number of Incidents*[20]
1.	2017 (April to December)	41,378
2.	2018	2,08,456
3.	2019	3,94,499
4.	2020	11,58,208
5.	2021	14,02,809
6.	2022 (till November)	12,67,564

The above information clearly states that on one hand where cybercrimes are on rise, on the other hand, Indian government is actively regulating the cyberspace to ensure high level of cyber security.

Under the above backdrop, let's discuss the legal and regulatory regime of cyber security in India

CYBER SECURITY: LEGAL ASSESSMENT[21]

A. The Information Technology Act, 2000

The Information Technology Act enacted in 2000. The IT was set to be administered by the Indian Computer Emergency Response Team (CERT-In) so that the contemporary advise is available for Indian cybersecurity legislation, and accordingly government can timely institute apt data protection policies, and govern cybercrime. It also protects e-governance, e-banking, e-commerce, and the private sector, among many others.

It is to be noted that IT Act does not exclusively deal with cyber security, but it along with multiple other sector-specific regulations promote cybersecurity standards. It also provides a legal framework for critical information infrastructure in India.

For example, in Section 43A of the IT Act, Indian businesses and organizations must have "reasonable security practices and procedures" to protect sensitive information from being compromised, damaged, exposed, or misused.

Under Section 72A of the IT Act, any intermediaries or persons that disclose personal data without the owner's consent (with ill intention and causing damages) are punishable by imprisonment of up to three years, a fine of up to Rs.500,000, or both.

B. Information Technology (Amendment) Act, 2008

The Information Technology Amendment Act, 2008 (IT Act 2008) added updated and redefined terms for current use, expanding the definition of cybercrime and the validation of electronic signatures. It also

20. Source: Lok Sabha Questions (December 14, 2022), Government of India. Available on http://164.100.24.220/loksabhaquestions/annex/1710/AU1374.pdf
21. Source: Chin Kyle (2022), Top Cyber Security Regulations in India, UpGuard.

strongly encourages companies to implement better data security practices and makes them liable for data breaches.

The IT Act of 2008 applies to any individual, company, or organization (intermediaries) that uses computer resources, computer networks, or other information technology in India. With regard to cyber security in specific, the IT Act of 2008 includes the following responsibilities:

- Improving cybersecurity measures and forensics.
- Requiring intermediaries and body corporates to report cybersecurity incidents to CERT-In.
- Preventing unauthorized/unlawful use of a computer system.
- Protecting private data and information from cyber terrorism, DDoS attacks, phishing, malware, and identity theft.
- Legal recognition for cybersecurity of organizations.
- Safeguarding e-payments and electronic transactions and monitoring and decryption of electronic records.
- Establishing a legal framework for digital signatures.
- Recognizing and regulating intermediaries.

C. *Information Technology Rules, 2011*

Under the IT Act, another important segment of the cybersecurity legislation is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules).

The most significant amendments include provisions for the regulation of intermediaries, updated penalties and violation fees for cybercrime, cheating, slander, and nonconsensual publishing of private images, as well as censoring/restriction of certain speech.

Both the Information Technology Act (ITA) and the IT Rules aim to govern how Indian entities and organizations process sensitive info, data protection, data retention, and collection of personal data and other sensitive information.

Other Indian sectors, like banking, insurance, telecom, and healthcare, also include data privacy provisions as part of their separate statutes.

D. *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and Cyber Security*

The IS/ISO/IEC 27001 regulations are identified by the Indian Sensitive Personal Data and Information Rules as international standards. As such, Indian companies are not obligated but highly advised to implement these standards, which can help meet the “reasonable security practices” under Indian jurisdiction.

E. *National Cyber Security Policy, 2013*[22]

Ministry of Electronics and Information Technology (Meity) released the National Cyber Security Policy, 2013 as a security framework for public and private organizations to better protect themselves from cyber-attacks. The goal behind the National Cyber Security Policy is to create and develop more dynamic policies to improve the protection of India’s cyber ecosystem. The policy aims to create a workforce of over 500,000 expert IT professionals over the following five years through skill development and training.

22. Students to note that National Cyber Policy 2013 has been discussed in detail in the previous parts of this chapter, hence a brief of this policy is provided herein.

F. Information Technology Rules, 2021

On February 25, 2021, the Ministry of Electronics and Information Technology introduced the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 as a replacement for IT Rules, 2011. A little over a year later, on June 6, 2022, the newly updated draft amendments were published by the Indian MeitY (Ministry of Electronics and IT) to improve the IT Act to keep up with the challenges of the ever-changing digital landscape.

The new amendments aim to allow ordinary users of digital platforms to seek compensation for their grievances and demand accountability when their rights are infringed upon, as well as institute additional due diligence on organizations.

Additionally, there are changes to the privacy and transparency requirements of intermediaries, such as:

- Requiring intermediaries to inform users about rules and regulations, privacy policy, and terms and conditions for usage of its services.
- Requiring intermediaries to designate a grievance officer that can address and resolve user complaints about violations of IT Rules, 2021.

G. National Cyber Security Strategy 2020

The National Cyber Security Strategy of 2020 was the long-awaited follow-up plan by the Indian government to further improve cybersecurity efforts. This strategy is under review by the National Security Council Secretariat. The strategy aims to improve cybersecurity audit quality so organizations can conduct better reviews of their cybersecurity architecture and knowledge. Its main goal is to serve as the official guidance for stakeholders, policymakers, and corporate leaders to prevent cyber incidents, cyber terrorism, and espionage in cyberspace.

H. Reserve Bank of India (RBI) Regulations on KYC (Know Your Customer) vide electronic means

KYC (Know Your Customer) processes are standards and practices used worldwide and mandated by the RBI (Reserve Bank of India). KYC is the tracking and monitoring of customer data security for improved safeguarding against fraud and payment credential theft. It requires banks, insurance companies, and any other digital payment companies that carry out financial transactions to verify and identify all of their customers.

For proper e-KYC compliance and to meet financial regulatory requirements, businesses need to include the following cybersecurity steps:

- Having a knowledge-based questionnaire test for verifying customer identities.
- Implementing pre-screening KYC verification methods like email verification, phone verification, Device ID intelligence, and reputational data, among others.
- Using AI-based technology and machine learning for verifying documents and government-issued IDs.
- Using biometrics like fingerprinting and facial recognition to verify a user's identity.
- Maintaining a database of customers for verification purposes.
- Businesses with KYC policies assure customers they have the relevant compliance management and anti-fraud solutions to protect their digital identities and payment transaction data.

Digital Personal Data Protection Act, 2023: New Paradigm of Data Privacy and Compliance[23]

After receiving approval from both houses of Parliament and obtaining the President's assent, the Digital Personal Data Protection Bill of 2022 has officially become the Digital Personal Data Protection Act of 2023. This Act is now in effect and governs the processing of digital personal data in India, regardless of whether the data was originally collected in digital or non-digital format and subsequently digitized. Under the DPDP Act, state agencies may be exempted from its provisions at the government's discretion. This legislation is designed to bolster data protection and accountability for entities such as internet companies, mobile apps, and businesses that handle citizens' data. Furthermore, it's worth noting that the DPDP Act will have implications for India's trade negotiations with other nations. It aligns with global data protection standards, taking inspiration from models like the EU's GDPR and China's PIPL.

At its core, the DPDP Act aims to establish a higher level of accountability and responsibility for entities operating within India, including internet companies, mobile apps, and businesses involved in the collection, storage, and processing of citizens' data. With a strong emphasis on the "Right to Privacy," this legislation seeks to ensure that these entities operate transparently and are answerable when it comes to handling personal data, thus prioritizing the privacy and data protection rights of Indian citizens.

The DPDP Act's scope extends beyond the borders of India, encompassing digital personal data processing activities abroad. This extension applies specifically to organizations offering goods or services to individuals in India or engaging in the profiling of Indian citizens. In doing so, the Act fortifies data protection measures not only within India but also concerning Indian citizens' data handled abroad.

The Telecommunications Act, 2023: Added Leg in Cyber Security

The Telecommunications Act, 2023 amended and consolidated the laws relating to development, expansion and operation of telecommunication services and telecommunication networks; assignment of spectrum; and for matters connected therewith or incidental thereto.

Lawful Interception and Security[24]

The Telegraph Laws empowered Government to intercept messages under a mechanism, which has survived judicial review for decades[25], and inspired similar regimes[26]. Interception directions are required to be in writing, on specified grounds and are subject to review by a committee[27].

The Telecommunications Act, 2023 contains provisions empowering Government to take possession of Services or networks and direct interception or disclosure of messages, in the event of a public emergency or in the interest of safety, with measures to be specified in rulemaking. To the extent that existing safeguards flow through to the new regime, especially given that right is couched in "public safety", it should continue to provide a robust and constitutional basis for lawful interception and monitoring.

The Act introduces 'critical telecommunication infrastructure', along the lines of 'critical information infrastructure' under the Information Technology Act, 2000 ("IT Act").[28] Regulations in relation to the protection of critical telecommunications infrastructure will be prescribed under the rules.

---

23. Reproduced from Khyati Anand and Melissa Cyrill (September 18, 2023), India's Digital Personal Data Protection Act, 2023: Data Privacy Compliance India Briefing. Available at https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/

24. Reproduced from Arun Prabhu, Anirban Mohapatra & Anoushka Soni (January 23, 2024) The Telecommunications Act, 2023, Indian Corporate Law, Cyril Amarchand Mangaldas. Available at https://corporate.cyrilamarchandblogs.com/2024/01/the-indian-telecommunications-bill-2023/#:~:text=Lawful%20Interception%20and%20Security&text=The%20Act%20contains%20provisions%20empowering,to%20be%20specified%20in%20rulemaking.

25. People's Union of Civil Liberties v. Union of India, (2003) 2 SCR 1136

26. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2)

27. Indian Telegraph Rules, 1951, Rule 419A(2)

28. Information Technology Act, 2000, Section 70

The Government's power to notify standards, which were introduced in the Bill, have been:

- modified to notify standards and conformity assessment measures for services in consonance with relevant TRAI regulations; and
- expanded to include prescription of standards for telecommunication security, including identification, analysis and prevention of intrusion in services and networks, cyber security and encryption and data processing in telecommunication.

These powers may impact entities not falling within the contours of the Act through contractual flow-down obligations in their capacity as service providers.

Appointments to TRAI have been broad based to enable appointments from the private sector.

Digital Personal Data Protection (DPDP) Rules, 2025 (November 17, 2025)

1. Introduction

The Government of India notified the Digital Personal Data Protection (DPDP) Rules, 2025 on 14 November 2025. This marks the full operationalisation of the Digital Personal Data Protection Act, 2023 (DPDP Act). Together, the Act and the Rules form a clear and citizen-centred framework for the responsible use of digital personal data. They place equal weight on individual rights and lawful data processing.

The Ministry of Electronics and Information Technology invited public comments on the draft Rules before finalising them. Consultations were held in Delhi, Mumbai, Guwahati, Kolkata, Hyderabad, Bengaluru and Chennai. A wide range of participants took part in these discussions.

Startups, MSMEs, industry bodies, civil society groups and government departments all offered detailed suggestions. Citizens also shared their views. In total, 6,915 inputs were received during the consultation process. These contributions played a key role in shaping the final Rules. With the notification of the Rules, India now has a practical and innovation-friendly system for data protection. It supports ease of understanding, encourages compliance and strengthens trust in the country's growing digital ecosystem.

2. Understanding the Digital Personal Data Protection Act, 2023

Parliament enacted the Digital Personal Data Protection Act on 11 August 2023. The law creates a full framework for the protection of digital personal data in India. It explains what organisations must do when they collect or use such data. The Act follows the SARAL approach. This means it is Simple, Accessible, Rational and Actionable. The text uses plain language and clear illustrations so that people and businesses can understand the rules without difficulty.

The law rests on seven core principles. These include consent and transparency, purpose limitation, data minimisation, accuracy, storage limitation, security safeguards and accountability. These principles guide every stage of data processing. They also ensure that personal data is used only for lawful and specific purposes. A central feature of the Act is the creation of the Data Protection Board of India. The Board functions as an independent body that oversees compliance, inquiries into breaches and ensures that corrective measures are taken. It plays a key role in enforcing the rights granted under the Act and maintaining trust in the system.

The Act places clear responsibilities on Data Fiduciaries to keep personal data safe and to stay accountable for its use. It also gives Data Principals the right to know how their data is handled and the right to seek correction or removal when needed. Together, the Act and the Rules create a strong and balanced system. They strengthen privacy, build public trust and support responsible innovation. They also help India's digital economy grow in a secure and globally competitive way.

3. Penalties Under the DPDP Act, 2023

The DPDP Act imposes substantial financial penalties for non-compliance by Data Fiduciaries. The highest penalty up to ₹250 crore applies to failure of a Data Fiduciary to maintain reasonable security safeguards. Not notifying the Board or affected individuals of a personal data breach as well as violations of obligations relating to children can each attract penalties of up to ₹200 crore. Any other violation of the Act or Rules by a Data Fiduciary may attract penalties up to ₹50 crore.

4. Overview of the Digital Personal Data Protection Rules, 2025

The Digital Personal Data Protection Rules, 2025 give full effect to the DPDP Act, 2023. They build a clear and practical system to protect personal data in a fast-expanding digital environment. The Rules focus on the rights of citizens and on responsible data use by organisations. The Rules aim to curb unauthorized commercial use of data, reduce digital harms and create a safe space for innovation. They will also help India maintain a strong and trusted digital economy. In carrying this vision forward, the Rules outline several core provisions that follow:

- **Phased and Practical Implementation**

  The Rules introduce an eighteen-month period for phased compliance. This gives organisations enough time to adjust their systems and adopt responsible data practices. Every Data Fiduciary must issue a separate consent notice that is clear and easy to understand. The notice must explain the specific purpose for which personal data is collected and used. Consent Managers, who help people manage their permissions, must be companies based in India.

- **Clear Protocols for Personal Data Breach Notification**

  The Rules set out a simple and timely process for reporting personal data breaches. When a breach takes place, the Data Fiduciary must inform all affected individuals without delay. The message must be in plain language and must explain what happened, the possible impact and the steps taken to address the issue. It must also include contact details for help.

- **Transparency and Accountability Measures**

  The Rules require every Data Fiduciary to display clear contact information for queries related to personal data. This may be the contact of a designated officer or a Data Protection Officer. Significant Data Fiduciaries face stronger duties. They must conduct independent audits and carry out impact assessments. They must also follow stricter checks while using new or sensitive technologies. In some cases, they must follow government directions on restricted categories of data, including local storage where needed.

- **Strengthening Rights of Data Principals**

  The Rules reinforce the rights already provided under the Act. Individuals can ask to access their personal data or seek corrections and updates. They may also request the removal of data in certain situations. They can choose someone else to exercise these rights on their behalf. Data Fiduciaries must respond to such requests within ninety days.

- **Digital-First Data Protection Board**

  The Rules establish a fully digital Data Protection Board of India, which will consist of four members. Citizens will be able to file complaints online and track their cases through a dedicated portal and mobile application. This digital system supports quicker decisions and simplifies grievance redressal. Appeals against the Board's decisions will be heard by the Appellate Tribunal, TDSAT.

5. How the DPDP Rules Empower Individuals

The DPDP framework places the individual at the centre of India's data protection system. It aims to give every citizen clear control over personal data and confidence that it is being handled with care. The rules are written in

plain language so that people can understand their rights without difficulty. They also ensure that organisations act responsibly and remain accountable for how they use personal data.

Rights and protections for citizens include:

- **Right to Give or Refuse Consent**

  Every person has the choice to allow or deny the use of their personal data. Consent must be clear, informed and easy to understand. Individuals may withdraw their consent at any time.

- **Right to Know How Data is Used**

  Citizens can seek information on what personal data has been collected, why it has been collected and how it is being used. Organisations must provide this information in a simple form.

- **Right to Access Personal Data**

  Individuals can ask for a copy of their personal data that is held by a Data Fiduciary.

- **Right to Correct Personal Data**

  People may request corrections to personal data that is inaccurate or incomplete.

- **Right to Update Personal Data**

  Citizens can ask for changes when their details have altered, such as a new address or updated contact number.

- **Right to Erase Personal Data**

  Individuals may request the removal of personal data in certain situations. The Data Fiduciary must consider and act on this request within the permitted time.

- **Right to Nominate Another Person**

  Every individual can appoint someone to exercise their data rights on their behalf. This is helpful in cases of illness or other limitations.

- **Mandatory Response within Ninety Days**

  Data Fiduciaries are required to address all requests related to access, correction, updating or erasure within a maximum of ninety days, ensuring timely action and accountability.

- **Protection During Personal Data Breaches**

  If a breach takes place, citizens must be informed at the earliest. The message must explain what happened and what steps they can take. This helps people act quickly to reduce harm.

- **Clear Contact for Queries and Complaints**

  Data Fiduciaries must provide a point of contact for questions relating to personal data. This may be a designated officer or a Data Protection Officer.

- **Special Protection for Children**

  When a child's personal data is involved, verifiable consent from a parent or guardian is required. This consent is needed unless the processing relates to essential services such as healthcare, education or real-time safety.

- **Special Protection for Persons with Disabilities**

  If a person with a disability cannot make legal decisions even with support, their lawful guardian must give consent. This guardian must be verified under the relevant laws.

6. How DPDP Aligns with the RTI Act

Since the DPDP Act and the DPDP Rules expand citizens' privacy rights, they also clarify how these rights work alongside the access to information guaranteed by the Right to Information (RTI) Act. The changes introduced through the DPDP Act revise Section 8(1)(j) of the RTI Act in a way that respects both rights without diminishing either. The amendment reflects the Supreme Court's affirmation of privacy as a fundamental right in the Puttaswamy judgment. It brings the law in line with the reasoning already followed by courts, which have long applied reasonable restrictions to safeguard personal information. By codifying this approach, the amendment prevents uncertainty and avoids any conflict between the transparency regime of the RTI Act and the privacy safeguards introduced under the DPDP framework. The revision does not prevent the disclosure of personal information. It simply requires that such information be assessed with care and shared only after considering the privacy interests involved. At the same time, Section 8(2) of the RTI Act remains fully operative. This provision allows a public authority to release information when the public interest in disclosure is strong enough to outweigh any possible harm. This ensures that the essence of the RTI Act, which is to promote openness and accountability in public life, continues to guide decision making.

7. Conclusion

The Digital Personal Data Protection Act and the DPDP Rules mark an important step in building a trustworthy and future-ready digital environment for the country. They bring clarity to how personal data must be handled, strengthen the rights of individuals and create firm responsibilities for organisations. The framework is practical in design and backed by wide public consultation, which makes it both inclusive and responsive to real needs. It supports the growth of India's digital economy while ensuring that privacy remains central to its progress. With these measures now in place, India moves towards a safer, more transparent and innovation-friendly data ecosystem that serves citizens and strengthens public confidence in digital governance.

Digital Personal Data Protection Act 2023

The Government of India notified the Digital Personal Data Protection (DPDP) Rules, 2025 on November 13, 2025, Section 40 (1) and (2) of the Digital Personal Data Protection Act, 2023, the Central Government has notified the Digital Personal Data Protection Rules, 2025. (1) Rules 1, 2 and 17 to 21 shall come into force on the date of their publication in the Official Gazette. (2) Rule 4 shall come into force one year after the date of publication of this Gazette. (3) Rules 3, 5 to 16, 22 and 23 shall come into force eighteen months after the date of publication of this Gazette. Digital Personal Data Protection Rules, 2025 inter alia provides the provisions relating to Notice given by Data Fiduciary to Data Principal; Registration and obligations of Consent Manager; Processing of personal data for provision or issue of subsidy, benefit, service, certificate, licence or permit by State and its instrumentalities; Reasonable security safeguards etc.

CYBER SECURITY: MAJOR REGULATING BODIES AND COMPLIANCE REQUIREMENTS

Compliance related to cyber security involves meeting various controls (usually enacted by a regulatory authority, law, or industry standards) to protect the confidentiality, integrity, and availability of data. Though compliance requirements may vary by industry and sector, but typically involve using an array of specific standards, technology and process to safeguard data. Hence, this part of the chapter aims to understand main regulating bodies that ensure laws, policies and standards related to cyber security are duly enforced in cyberspace.

A. Computer Emergency Response Team (CERT-In)

The Computer Emergency Response Team (CERT-In) is the national nodal agency for collecting, analyzing, forecasting, and disseminating non-critical cybersecurity incidents.

In addition to cybersecurity incident reporting and notifying, the CERT-In cybersecurity directive helps with issuing guidelines for Indian organizations guidelines as well, offering the best information security

practices for managing and preventing cybersecurity incidents. As per IT Act and related Rules under it, all intermediaries are required to report any cybersecurity incidents to CERT-In. CERT-In roles and functions were later clarified in an additional amendment under Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (IT Rules, 2013).

CERT-In acts as the primary task force that:

- Analyzes cyber threats, vulnerabilities, and warning information
- Responds to cybersecurity incidents and data breaches
- Coordinates suitable incident response to cyber-attacks and conducts forensics for incident handling
- Identify, define, and take suitable measures to mitigate cyber risks
- Recommend best practices, guidelines, and precautions to organizations for cyber incident management so that they can respond effectively.

B. National Critical Information Infrastructure Protection Center (NCIIPC)

The National Critical Information Infrastructure Protection Center (NCIIPC) was established on January 16, 2014, by the Indian government, under Section 70A of the IT Act, 2000 (amended 2008).

Based in New Delhi, the NCIIPC was appointed as the national nodal agency in terms of Critical Information Infrastructure Protection. Additionally, the NCIIPC is regarded as a unit of the National Technical Research Organization (NTRO) and therefore comes under the Prime Minister's Office (PMO).

The Indian Parliament divides cybersecurity into two segments: "Non-Critical Infrastructure (NCI)," which CERT-In is responsible for, and "Critical Information Infrastructure (CII)," which NCIIPIC is responsible for. CII is defined by the Indian Parliament as "facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation."

NCIIPC is required to monitor and report national-level threats to critical information infrastructure. The critical sectors include:

- Power and energy
- Banking, financial services, and insurance
- Telecommunication and information
- Transportation
- Government
- Strategic and public enterprises

NCIIPC successfully implemented several guidelines for policy guidance, knowledge sharing, and cybersecurity awareness for organizations to conduct preemptive measures of these important sectors, especially in power and energy. The guidelines represent the first means for regulating such sectors and requiring "mandatory compliance by all responsible entities."

Additionally, the Indian government approved the Revamped Distribution Sector Scheme in August 2021. The main goal of this regulation is to improve the operations of DISCOMs (distribution companies) by enhancing the cyber infrastructure with AI-based solutions. This will ultimately aid organizations and companies in meeting the framework's goals.

C. Cyber Regulations Appellate Tribunal (CRAT)

Under the IT Act, 2000, Government of India created the Cyber Regulations Appellate Tribunal (CRAT) as a chief governing body and authority for fact-finding, receiving cyber evidence, and examining witnesses. As per IT Act, CRAT has powers of civil court as defined under Code of Civil Procedure, 1908.

D. Securities and Exchange Board of India (SEBI)

Established in 1988, the SEBI (Securities and Exchange Board of India) is the regulatory body for securities and commodity markets in India. In addition to ensuring the needs of market intermediaries, investors, and issuers of securities in compliance with applicable laws, SEBI also focus on safeguarding their data, customer data, and transactions.

As of April 2022, SEBI has six committee members that are required to oversee guidance for cybersecurity initiatives for the Indian market and advise SEBI to develop and maintain cybersecurity requirements following global industry standards.

E. Insurance Regulatory and Development Authority (IRDAI)

The insurance sector of India is regulated by IRDAI, which issues information security guidelines for insurers and addresses the importance of maintaining data integrity and confidentiality.

With this new Information and Cyber Security for Insurers Guidelines, the IRDAI:

- Mandates insurance companies to have a CISO (chief information security officer)
- Puts together an information security committee
- Creates plans for managing cyber crises
- Creates and implements cybersecurity assurance programs
- Implements proper methods for protecting data
- Maintains risk identification and risk mitigation processes.

On October 9, 2022, IRDAI introduced an improved cybersecurity framework focused on the insurers' main security concerns. It aims to encourage insurance firms to establish and maintain a robust risk assessment plan, improve mitigation methods of internal and external threats, prevent ransomware attacks and other types of fraud, and implement a strong and robust business continuity.

F. Telecom Regulatory Authority of India (TRAI) & Department of Telecommunications (DoT)

The Telecom Regulatory Authority of India, along with the DoT (Department of Telecommunication)[29], have tightened regulations for protection of data privacy and also mandates guidelines under which users' date has to be used.

Although TRAI has been granted more regulatory powers, both work together to govern and regulate telephone operators and service providers.

On June 16, 2018, TRAI released recommendations for telecom providers on "Privacy, Security and Ownership of the Data in the Telecom Sector." In the newest guidelines, TRAI addresses newer responsibilities governing consumer data because most digital transactions in India are done via cell phones.

29. TRAI is a regulatory body, and DoT is a separate executive department of the Ministry of Communications in India.

TRAI addresses data protection with the following objectives:

- Define and understand the scope of "Personal data, Ownership, and Control of Data," namely, the data of users of the telecom service providers.
- Understand and Identify the "Rights and Responsibilities of Data Controllers".
- Assess and identify the efficiency of how data is protected and which data protection measures are currently in place in the telecommunications sector.
- Identify and address critical issues regarding data protection.
- Collect and control user data of TISP (traffic information service providers) services.
- The DoT has collaborated with the Indian IT ministry to impose layered data consent rules that safeguard personal data processing. This gives users the freedom to decide whether or not they will consent to the usage of their personal data and the right to withdraw consent at any time.

The new rules state that organizations and companies will only have to collect the necessary user details and that the data may be retained only for as long as required. Additionally, Indian telecommunications service providers comply with common standards like ISO 27000, 3GPP and 3GPP2, and ISO/IEC 15408.

CYBER SECURITY: RECENT GOVERNMENT INITIATIVES IN INDIA

- Cyber Surakshit Bharat Initiative.
- Cyber Swachhta Kendra.
- Online cybercrime reporting portal.
- Indian Cyber Crime Coordination Centre (I4C).
- National Critical Information Infrastructure Protection Centre (NCIIPC).

Concluding Remarks: Need of the Hour

The above discussion briefly explains that with the innovation of cyberspace, new challenges in the form of cybercrimes are threatening cyber security. Through government is actively taking step to uproot the menace of cybercrimes and vulnerabilities, yet it is recommended that following kinds of actions (both in form of security, education and legislation) shall be ensured in utmost coordination for enhancing the standards of global legal protection against cybercrimes.[30]

A. Legislation approach

- Laws should apply to cyber-crime—National governments still are the major authority who can regulate criminal behavior in most places in the world. Hence a conscious effort by government to update existing laws and to introduce specific sector laws to tackle cyber-crimes would be quite necessary.
- Review and enhance Indian cyber law to address the dynamic nature of cyber security threats;
- Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions;
- Establish progressive capacity building programmes for national law enforcement agencies;

30. Source: https://www.asianlaws.org/press/cybercrime.htm

- There should be a symbiotic relationship between the firms, government and civil society to strengthen legal frameworks for cyber-security.

B. Security approach

- Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the information society and for building confidence among users of ICTs;
- A global culture of Cyber security needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies;
- Streamlining and improving the co-ordination on the implementation of information security measures at the national and international level;
- Establishment of a framework for implementation of information assurance in critical sectors of the economy such as public utilities, telecommunications, transport, tourism, financial services, public sector, manufacturing and agriculture and developing a framework for managing information security risks at the national level;
- Establishment of an institutional framework that will be responsible for the monitoring of the information security situation at the national level, dissemination of advisories on latest information security alerts and management of information security risks at the national level including the reporting of information security breaches and incidents;
- Promote secure e-commerce and e-government services;
- Safeguarding the privacy rights of individuals when using electronic communications;
- Develop a national cyber security technology framework that specifies cyber security requirement controls and baseline for individual network user;
- Firms should secure their network information. When organization provides security for their networks, it becomes possible to enforce property rights laws and punishment for whoever interferes with their property.

C. Education/Research

- Improving awareness and competence in information security and sharing of best practices at the national and international level through the development of a culture of cybersecurity;
- Formalize the coordination and prioritization of cyber security research and development activities; disseminate vulnerability advisories and threat warnings in a timely manner;
- Implement an evaluation/certification programme for cyber security product and systems;
- Develop, foster and maintain a national culture of security standardize and coordinate cybersecurity awareness and education programmes.

LESSON ROUND-UP

- Though the information revolution (*precisely to be called as "Information Era"*) has created new opportunities, improved organizational efficiency and extraordinary global connectivity. Yet it has brought about new unconventional vulnerabilities and threats bearing social, economic, political and security implications.
- Among many banes suffered in ICT era, cyber security is a serious concern of individuals and organizations, public and private as well as national and international.
- Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
- Cybersecurity is the process of defending against malicious intrusions on networks, computers, servers, mobile devices, electronic systems, and data. It is also referred to as information technology security or electronic information security.
- For an all-compassing cyber security in the interest of business growth and progression, following fundamental categories need to be ensured:
  - Network security,
  - Data integrity and privacy,
  - Operational security.
- There are many cyber security techniques to combat the cyber security attacks including Authentication, Encryption, Digital Signatures, Firewall and alike.
- On one hand, technology has transformed the society towards inclusive development, on the other hand, this technology only has become vulnerable to cybercrime. It is worth to mention that with day to day innovated technology, newer kind of cybercrimes are taking place. Hence, technology and its innovation itself has become a major challenge and restriction to cyber security.
- To be precise, cybercrime and its increased frequency are one of the major challenges in cyber security.
- Handling cyber security is still a very huge concern of present-day Governments and private sectors throughout the globe are taking many measures in order to secure these cybercrimes.
- In addition to the cybercrimes as discussed in this chapter, recently new forms of challenges and limitations are identified in cyber world.
- There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space.
- Due to the dynamic nature of cyberspace, and for the required unified action, the Government of India has enacted a National Cyber Security Policy, with an integrated vision and a set of sustained & coordinated strategies for implementation.
- Cyber Security Policy also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

- In 2020, the National Cyber Security Strategy was conceptualized by the Data Security Council of India (DSCI).
- In the wake of recent cyber-attacks as well as of urgent necessity of cyber security, the National Security Council Secretariat (NSCS) has formulated a draft National Cyber Security Strategy, which holistically looks at addressing the issue of security of national cyberspace.
- Considering the global flow of the information and communication technology, states now a days are giving increased attention to the governance of cyberspace.
- Accordingly, in order to ensure effective governance in cyberspace the role of international law in the cyber context has gained increased prominence.
- There are certain standards which effectively ensure cyber security and open for international adoption.
- In the recently notified cyber security direction CERT-In has now made it mandatory for all incidents to be mandatorily reported to CERT-In.
- On one hand where cybercrimes are on rise, on the other hand, Indian government is actively regulating the cyberspace to ensure high level of cyber security.
- In addition to Information Technology Act, 2000 and its relevant IT Rules, 2011, there are many regulatory bodies which ensure the effective enforcement of cyber security in India.
- National Cyber Security Strategy 2023 is an important document that supersedes the 2013 policy. From 2013 till 2023, the world has changed as new threats have emerged calling for new strategy.
- The document will be put in public domain after a final check by the committee to ensure that nothing confidential is released.
- There are two aspects to cyber security. First is cyber hygiene for all of us and cyber skilling of the cyber workforce i.e. the people who enforce cyber security.
- Bharat NCX 2023 represents a defining moment in India's unwavering commitment to cybersecurity excellence, underscoring the paramount importance of collaboration and knowledge-sharing among stakeholders from government, public, and private sectors.
- In an era characterized by burgeoning digitalization, Bharat NCX 2023 serves as a compelling reminder of the paramount importance of collective vigilance and preparedness in safeguarding our nation's invaluable digital assets.
- After receiving approval from both houses of Parliament and obtaining the President's assent, the Digital Personal Data Protection Bill of 2022 has officially become the Digital Personal Data Protection Act of 2023.
- At its core, the DPDP Act aims to establish a higher level of accountability and responsibility for entities operating within India, including internet companies, mobile apps, and businesses involved in the collection, storage, and processing of citizens' data. With a strong emphasis on the "Right to Privacy," this legislation seeks to ensure that these entities operate transparently and are answerable when it comes to handling personal data, thus prioritizing the privacy and data protection rights of Indian citizens.

- The Telecommunications Act, 2023 amended and consolidated the laws relating to development, expansion and operation of telecommunication services and telecommunication networks; assignment of spectrum; and for matters connected therewith or incidental thereto.
- The Act introduces 'critical telecommunication infrastructure', along the lines of 'critical information infrastructure' under the Information Technology Act, 2000 ("IT Act").

TEST YOURSELF

(These are meant for recapitulation only. Answers to this questions are not to be submitted for evaluation)

1. What is Cyber Security and Why Cyber Security is significant in the current cyberspace? Explain with suitable examples.
2. Briefly discuss Cyber Security Techniques.
3. How would you define Cybercrime? Discuss at least 5 cybercrimes, which threatens cyber security.
4. Write a brief on recent government initiatives for ensuring cyber security.
5. Highlight the role of CERT-In in cyber security.
6. Write Short Notes on ANY TWO topics as mentioned below:
    a. National Cyber Security Policy, 2013
    b. National Cyber Security Strategy, 2020
    c. Cloud Attacks
    d. Digital Personal Data Protection Act, 2023
    e. Telecommunication Act, 2023
7. Define Cybersecurity. Elucidate the difference between IDS and IPS?
8. What is the difference between stored and reflected XSS?
9. List the common types of cybersecurity attacks.
10. What is a cybersecurity risk assessment?
11. Which is more secure SSL or HTTPS?
12. How to protect data in *transit* vs. *rest*?

LIST OF FURTHER READINGS

- Aditi Subramaniam and Sanuj Das (2022) The Privacy, Data Protection and Cybersecurity Law Review: India, The Law Reviews
- DSCI Report – National Cyber Security Strategy, 2020
- Gautam Sen (2022) Cyber Security and Cyberspace in International Relations: A Roadmap for India's Cyber Security Policy, A USI of India Publications
- Mayank Bhushan et al (2020) Fundamentals of Cyber Security (Principles, Theory and Practices), BPB Publications, India
- Sandeep Shukla and Manindra Agrawal (2020) Cyber Security in India – Education, Research and Training, SpringerLink.

LIST OF OTHER REFERENCES

- Charles Brookson (2016) Tackling the Challenges of Cyber Security First edition – December 2016 ETSI White Paper No. 18, ISBN No. 979-10-92620-12-2.
- Chin Kyle (2022), Top Cyber Security Regulations in India, UpGuard.
- Cyber Security Division, Ministry of Electronics and Information Technology, Government of India.
- Cybersecurity Laws and Regulations India 2023, ICLG.com (Published in 2022).
- Cyber Security: Threats, Challenges and Opportunities (2016), Australian Computer Society, Sydney, Australia.
- Dr. Rajasekharaiah K.M. et al, Cyber Security Challenges and its Emerging Trends on Latest Technologies, IOP Conf. Series: Materials Science and Engineering 981 (2020) 022062, ICRAEM 2020.
- Dr. V. Kavitha et al, Cyber Security Issues and Challenges – A Review International Journal of Computer Science and Mobile Computing, Vol. 8 Issue 11, November-2019, pg. 1-6.
- K.M. Rajasekharaiah et al (2020) Cyber Security Challenges and its Emerging Trends on Latest Technologies , IOP Conference Series.: Material Science and Engineering 981 022062.

Cyber Threats and Cyber Laws

Lesson 3

KEY CONCEPTS

■ Cyber Threats ■ Cyber Warfare ■ Cyber Crime ■ Cyber Terrorism ■ Cyber Threat Hunting ■ Digital Forensics ■ Digital Intellectual Property ■ Data Protection

Learning Objectives

To understand:

- Meaning and Types of Cyber Threats
- What is Cyber Warfare
- Meaning and Kinds of Cyber Crimes
- What constitute Cyber Terrorism
- Significance of Cyber Security and its Mechanism
- Types of Cyber Threats
- Meaning and Process Cyber Threat Hunting
- What is Digital Forensics?
- Concept of Digital Intellectual Property
- Legal purview of the Liability of online platform/intermediaries
- Artificial Intelligence vis-à-vis Data Protection
- Other inter-related concepts

Lesson Outline

- Introduction
- Cyber Threats Cyber Warfare
- Cyber Crime
- Cyber Terrorism
- Types of Cyber Threats/ Attacks
- Cyber Threat Hunting and Digital Forensics
- Digital Intellectual Property
- Liability of online platforms
- Laws applicable to AI and Cyber Laws
- Cyber Security Framework (NCFS)
- Data Protection and AI: Laws and Regulations
- Case Studies
- Lesson Round-Up
- Test Yourself
- List of Further Readings

REGULATORY FRAMEWORK

- Information Technology Act, 2000
- Overview of IT Act, 2000
- The important provisions of IT Act, 2000
- Positive and negative aspects of IT Act, 2000
- Information Technology Rules (IT Rules), 2011
- Companies Act, 2013
- Indian Penal Code, 1860

INTRODUCTION

It was around 900 BC, when for the first time, postal service was introduced in China for governmental use and in 14 BC, the Romans established their 'Postal Services' as means of communication.[1] Since that time, information has continued to be transferred and conveyed through traditional means of communication like postal communication, telephone and fax etc. The development of electronic computers with the support of internet in 1950 has elevated the process of transfer of information from one end to the other. The beginning of point-to-point communication[2]; development of Telnet in 1960s and 1970s; the release of governmental control over internet by America in 1994 and the birth of 'www' i.e. the World Wide Web in 1994 has globally changed the entire process of transferring, sharing and relocating the information.[3] The shift from traditional modes of information to information technology, i.e. a term used to denote the use of technology to communicate, transfer data and process information, has been swift owing to digitalization, which has led to emergence of unprecedented growth of data.

Such developments in the field of information technology have gone a long way towards enhancing the ability of individuals to transfer information liberally and without bottlenecks such as time consumption, congestion of roots, non-connectivity etc., from which postal communication, telecommunication, fax and other modes of communication often suffered. Additionally, information technology has ensured instant access and relocation of information while avoiding the limits and fetters encountered in the traditional means of communication.

Advent of information technology has not only provided us the assorted means of communicating our information at an inclusive platform but it has also ensured quick communication of information. Information technology can be described as any technology that helps us to produce, manipulate, store, communicate, and/or disseminate information. Usually 'Information' refers to data that has been organized and then communicated.[4] In general terms, information technology is a broad term used to refer to any form of technology used to create, transfer, or store information in all of its various forms, be it text, images, sound, multimedia files.[5]

In the system of information and communication technology, it is the use of internet[6] that serves the major function of conveying information at global level. Internet is said to be one of the greatest developments in the province of information and communication advancement. Internet[7] as a backbone of information technology has

1. The History of Communication. (Jan. 2, 2013), http://inventors.about.com/library/inventors/bl_history_of_communication.htm.

2. In telecommunications, a point-to-point connection refers to a communications connection between two nodes or endpoints. An example is a telephone call, in which one telephone is connected with one other, and what is said by one caller can only be heard by the other.

3. Brief History of Internet. (Sept. 9th 2013), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

4. Allen and Morton, Information Technology and the Corporation of the 1990s, New York, Oxford University Press (1994).

5. Longley et al., Dictionary of Information Technology, Macmillan Press, 164 (2nd ed. 2012).

6. In legal parlance, Internet can be defined as an electronic communications network that connects computer networks and organizational computer facilities around the world. (Jan. 7, 2013), http://www.statelawyers.com/Practice/Practice_Detail.cfm/PracticeTypeID:56.

7. Internet is an arrangement of connected computers, which lets the computer users all over the globe exchange data.

touched almost every aspect of life including telecommunication, finance, governance, health care, education etc.[8] at a global platform. India is not an exception to the revolutionary effects of internet and information technology; as per Internet World Statistics, India alone has an internet user base of over 100 million.[9] Internet has not only facilitated the easy exchange and management of information but also proved a far easier medium of transferring data on a global platform just in blink of an eye. In this way, information technology has brought revolutionary changes in the approach of social interactions among people, business world, government agencies, regulatory perspective and control mechanism to an entirely new synchronization.

Information technology has served various advantages to human kind[10] in the form of (i.) speedy social interaction;[11] (ii.) growth of business; (iii.) enhancing the educational capacity of youth[12] etc. Additionally, advantages of information and communication technology can also be seen in terms of email (an essential communication tool for individuals as well as for businesses), availability of information and resources (availability of huge amount of information about every subject like law, government services etc.), services (like banking, insurance etc.), e-commerce (sale and purchase over internet), software downloads etc., which provide ease to the human community in almost all spheres of life.

Pros and Cons of Information Technology	
PROS:	**CONS:**
• Globalization	• Digital Divide
• Communication	• Cyber crime
• Cost effectiveness	• Security threat
• Comfortable life	• Privacy concerns
• Bridging cultural gap	• Unemployment
• Easy accessibility of information	• Intellectual property crime
• Unlimited data storage and backup	• Cyber terrorism
• Online booking of ticket	• Computer related diseases

However, it has been righty said that '*with boon goes the bane'*, and this phrase is also true for information technology. At one side, this easy medium of transferring data and facilitating quicker flow of communication has given birth to numerous modes of communication and transaction; on the other side, various dark sides are being observed under IT enabled and electronic transactions. The major threats among them are Cyber Crimes and Cyber Attacks. Hence, in order to control the mechanism of cyber-crimes and cyber-attacks, cyber law has evolved gradually which ensures cyber security in cyber sphere. Hence this chapter inter-alia aims to provide understanding on the following:

8. Shyam, R. and Bhoria, A., Information Technology (Internet): Effects on Social Participation and Well-Being of Users, Journal of Indian Academy of Applied Psychology, Vol. 37, No.1, 157-162 (2011).

9. Internet Usage Stats and Telecommunications Market Report. (Mar. 27, 2012), http://www.internetworldstats.com/asia/in.htm.

10. Scott et al., Internet Benefits: Consumer Surplus and Net Neutrality, Institute of Policy Integrity, New York University School of Law, (2011). (Jan.7, 2013), http://policyintegrity.org/files/publications/Internet_Benefits.pdf; See also, Gary James on Advantages and Disadvantages of Online Learning. (Jan. 7, 2013), http://www.leerbeleving.nl/wbts/nieuw_basics/addis.pdf.

11. Through internet, communication is faster and easier in comparison to the traditional means of communication, so people on opposite sides of the world can speak to each other over the internet as if they were speaking in person. Apart from this the internet boosts the spread of culture, since all type of communications are made possible through internet.

12. Latchman et al., Information Technology Enhanced Learning in Distance and Conventional Education, IEEE Transactions on Education, Vol. 42, No. 4 (1999).

- Cyber Threats;
- Cyber Warfare;
- Cyber Crimes;
- Cyber Terrorism;
- Cyber Security;
- Cyber Laws;
- AI vis-à-vis Data Protection; and
- Other inter-related concepts.

Source: Remya Ravindran

CYBER THREATS

Cyber security is a serious concern of present times as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the network and security systems. Individuals, small-scale businesses or large organizations, are all being impacted. Therefore, all of these firms, whether IT or non-IT firms, have understood the importance of Cyber Security and focus on adopting all possible measures to deal with cyber threats.

Definition of Cyber Threats

A cyber threat (*also known as cybersecurity threat*) is defined as a malicious act that seeks to steal or damage data or disrupt the digital wellbeing and stability in general. Cyber threats include a wide range of attacks including but not limited to data breaches, computer viruses, denial of service, and numerous other attack vectors. Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data.

Sources of Cyber Threats

Cyber threats may come from a variety of places, people, and contexts. In general, following are the major sources of cyber threats:

- Nation-states
- Terrorists
- Industrial spies
- Organized crime groups
- Unhappy insiders
- Hackers
- Business competitors

CYBER WARFARE

As per Britannica Dictionary, Cyberwar (also called cyberwarfare or cyber warfare) is defined as a war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is usually a war waged against government and military networks in order to disrupt, destroy, or deny their use of systems to disrupt operations, particularly for tactical, military and cyberespionage reasons.

AIIMS cyber attack raises red flags in national security

India News

Published on Dec 07, 2022 07:21 AM IST

The government has been informed that China was testing the resilience of the Indian system as part of hybrid warfare when Indian Air Force attacked Balakot on February 26, 2019 as a retaliation for the Pulwama terror strike by the Pakistan- based Jaish-e-Mohammed terror group.

Computers and the networks that connect them are collectively known as the domain of cyberspace. Everything that modern society needs to function—from critical infrastructures and financial institutions to modes of commerce and tools for national security—are dependent to a major extent upon cyberspace. Therefore, the threat of cyberwar and its purported effects are a source of great concern for governments and militaries around the world. With the dependability on cyberspace, the day is not far where cyber war is expected to be as fatal as a real war between the nations.

Source: The Hindustan Times, December 07, 2022

CYBER CRIME[13]

With the help of Information and Communication Technology (ICT), people are more interconnected than ever before. Though the dependability on ICT is full of advantages, yet connectivity leaves us vulnerable to the risks of fraud, theft, abuse including cyber-attack. Cyber-crime is any criminal activity that involves a computer, networked device or a network. In general, most cybercrimes are carried out in order to generate profit for the cybercriminals, yet some of cybercrimes are carried out against computers or devices directly to damage or disable them. It can be briefly state that the spectrum of cyber threats is limitless and cyberattacks can come in the form of viruses, malware, email phishing, social media fraud and alike. Cybercrime can have wide-ranging impacts, at the individual, local, state, and national levels. A brief description of the impact of cyber-crime is as below:

- Organized cybercrime, state-sponsored hackers, and cyber espionage (a type of cyber-attack in which an unauthorized user attempts to access sensitive data or intellectual property for economic gains, competitive advantage or political reasons) can pose national security risks to our country and our critical infrastructure.
- Transportation, power, and other services may be disrupted by large scale cyber incidents. The extent of the disruption is highly uncertain as it will be determined by many unknown factors such as the target and size of the incident.
- Vulnerability to data breach and loss increases if an organization's network is compromised. Information about a company, its employees, and its customers can be at risk.
- Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the Internet are vulnerable to intrusion. Personal information may be at risk without proper security.

CYBER TERRORISM

Cyber terrorism is the convergence of terrorism and cyberspace. The term 'cyber terrorism' was first coined by Banny C. Collin of the Institute for Security and Intelligence (ISI) in the late 1980s. But its usage was better understood during the 9/11 attacks that took place in the United States of America. In general, it is difficult to define cyber terrorism. Yet, U.S. Federal Bureau of Investigation has defined cyber terrorism as a premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence

13. Students to note that Cyber Crime is descriptively discussed in Chapter 4 of this Study Material. Hence under this sub-section, we are only providing brief views on Cyber Crime.

against clandestine agents and subnational groups. The main aim behind cyberterrorism is to cause harm and destruction. Hence, in brief cyber terrorism signifies use of the internet to carry out violent activities that result in or threaten the loss of life or substantial physical injury to accomplish political or ideological advantages through threat or intimidation.

Cyber Terrorism vis-à-vis Cyber Crime[14]

Cyber terrorism is also named as electronic terrorism, information warfare or Cyber warfare. The basic objective of cyber-attack is hacking, generally to satisfy the ego of hackers of creating terror. The objective of Cyber terrorism is to generate the feeling of terror in the mind of the cyber victims. Cyber terrorism includes commission of acts of destruction, alteration, acquisition and acts of transmission of information systems, programs, computers and networks against the following:

- Defence forces
- Financial Infrastructure
- Civilians
- Destructions of supervisory control and data acquisition system of smart cities
- Exploration of smart army etc.

Basic elements of Cyber Terrorism

- Perpetrator (which may include a group of people) i.e. Cyber Criminal
- Place - Cyber Space
- Action/Method or mode of action – Any Cyber technique
- Tools - Cyber Arsenal or Armory
- Targets - e.g. Government, Company, Place, Individuals, Administration or Digital Infrastructure
- Affiliations-actual or claimed
- Motivations-social, religious, communal or revenge.

Legal Provisions dealing with Cyber terrorism

There is no specific legislation or law which deals with cyber terrorism in India. In 2018, amendments were made to the Information Technology Act, 2000 (hereinafter referred to as 'IT Act'), which led to insertion of Section 66F, which deals with Cyber Terrorism, in the Act. Section 66F is the only provision which deals with and covers any act committed with intent to threaten 'unity, integrity, security or sovereignty of India or promoting terror with Denial of Service Attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty and integrity of India, the security, friendly relations with other states, public order, decency, morality or relating with contempt of court, defamation or incitement to an offence or to advantage of any foreign nation or group of individuals[15]. A brief outline of legal provisions under the IT Act aimed at providing legal protection against cyber terrorism is discussed below:

14. Raman and Sharma (2019) Cyber Terrorism in India: A Physical Reality Orvirtual Myth, Indian Journal of Law and Human Behavior Volume 5 Number 2 (Special Issue), May - August 2019

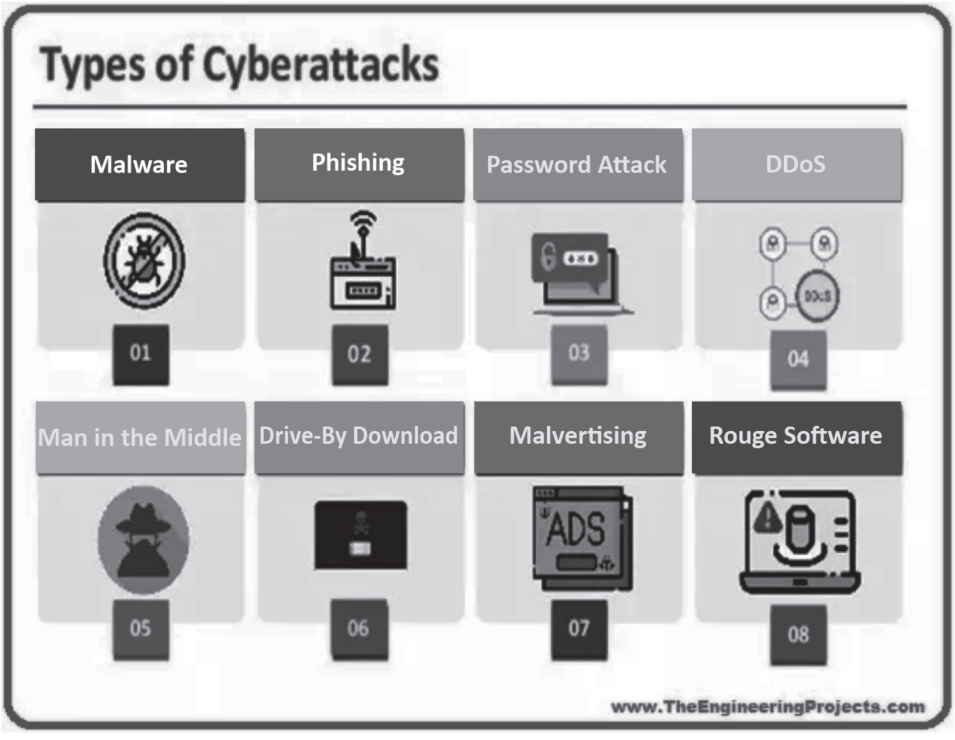
15. Shiv Raman, Nidhi Sharma, "Cyber terrorism in India: A physical reality or virtual myth" 5 Indian Journal of Law and Human Behaviour (2019), available at: https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf .

- Sec. 66: Computer related offences including Hacking.
- Sec. 66A: Punishment for sending "false and offensive messages" through communication service etc. This section also made sending messages deemed 'annoying or inconvenient' an offence. It is pertinent to note that this section has been struck down as being unconstitutional for violating freedom of speech and expression guaranteed under Art. 19(1)(a) of the Constitution of India by the Hon'ble Supreme Court in *Shreya Singhal vs. Union of India (2015) 5 SCC 1*.
- Section 66C: Punishment for Identity theft, i.e. dishonestly and using electronic signature, password or any other unique identification feature of any other person.
- Section 66D: Punishment for cheating by personation by using computer resource.
- Section 66F: Punishment for Cyber Terrorism.
- Section 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- Section 69B: Power to authorize to monitor and any computer resource for cyber security.
- Section 70B: Indian Computer Emergency Response Team (CERT) to serve as national agency for incident response.
- Section 84B: Punishment for abetment of offences.
- Section 84C: Punishment for attempt to commit offences.
- Implementation of Information Technology (IT) Security Guidelines, 2000.
- The Information Technology (Procedure and Safeguard for Interception Monitoring and Decryption of Information) Rules, 2009.
- The Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.
- The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- The Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
- The Information Technology (Electronic Service Delivery) Rules, 2011.
- The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties Rules, 2013.

TYPES OF CYBER THREATS/ ATTACKS

As discussed above, a cyber-attack or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

Cyber threats also refer to the possibility of a successful cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.



Source: Medium.com

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. Cyber-attacks can be classified into the following categories:

1) Web-based attacks
2) System-based attacks.

Web-Based Attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows

1. **Injection attacks:** It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information. Example- SQL Injection, code Injection, log Injection, XML Injection etc.
2. **DNS Spoofing:** DNS spoofing is a type of computer security hacking. Whereby data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers' computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.
3. **Session Hijacking:** It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.
4. **Phishing:** Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication. For example: an email-borne attack that involves tricking the email

recipient into disclosing confidential information or downloading malware by clicking on a hyperlink in the message.

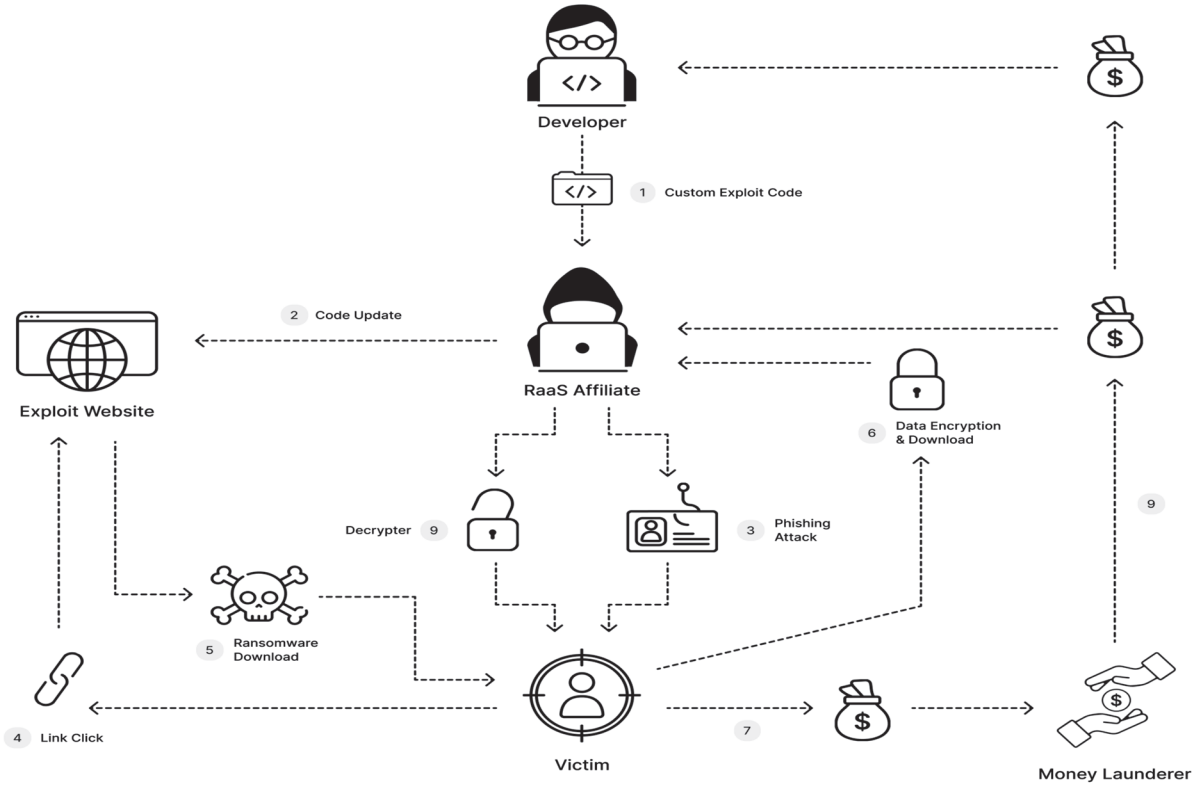
5. **Spear Phishing:** A more sophisticated form of phishing where the attacker learns about the victim and impersonates someone he or she knows and trusts.
6. **Malware:** Malware (malicious software) is software that has been specifically designed to perform malicious tasks on a device or network, such as corrupting data or taking control of a system.
7. **Malware on Mobile Apps:** Mobile devices are vulnerable to malware attacks just like other computing hardware. Attackers may embed malware in app downloads, mobile websites, or phishing emails and text messages. Once compromised, a mobile device can give the malicious actor access to personal information, location data, financial accounts, and more.
8. **Spyware:** Spyware is a form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.
9. **Wiper Attacks:** A wiper attack is a form of malware whose intention is to wipe the hard drive of the computer it infects.
10. **Brute force:** It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.
11. **Denial of Service:** It is an attack which is meant to make a server or network resource unavailable to the user. It accomplishes this task by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following:

    Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

    Protocol attacks- It consumes actual server resources, and is measured in a packet.

    Application layer attacks- Its goal is to crash the web server and is measured in request per second.
12. **Dictionary attacks:** These type of attacks store the list of a commonly used passwords and validate them to get the original password.
13. **URL Interpretation:** It is a type of attack where we can change certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.
14. **File Inclusion attacks:** It is a type of attack that allows an attacker to access unauthorized or essential files which are available on the web server or to execute malicious files on the web server by making use of the include functionality.
15. **Man in the Middle Attacks:** It is a type of attack that allows an attacker to intercept the connection between client and server and act as a bridge between them. This will enable the attacker to read, insert and modify the data in the intercepted connection. In short, here, an attacker establishes contact between the sender and recipient of electronic messages and intercepts them, perhaps changing them in transit, making the sender and recipient believe that they are communicating directly with one another. A MitM attack may be utilized by the military to confuse an enemy.
16. **Trojans:** Named after the Trojan Horse of ancient Greek history, the Trojan is a type of malware that enters a target system looking like one thing, e.g. a standard piece of software, but then releases the malicious code once inside the host system.

17. **Ransomware:** Ransomware is a type of malware that denies access to a computer system or data until a ransom is paid. Ransomware is one of the most dangerous types of cyber security threats. Some ransomware attack techniques involve stealing sensitive information before the target system is encrypted. Such added processes could classify some ransomware attacks as data breaches.



Source: https://www.upguard.com/blog/cyber-threat

18. **Attacks on IoT Devices:** IoT devices like industrial sensors are vulnerable to multiple types of cyber threats. These include hackers taking over the device to make it part of a DDoS attack and unauthorized access to data being collected by the device. Given their numbers, geographic distribution, and frequently out-of-date operating systems, IoT devices are a prime target for malicious attacks.

> ***Note:***
>
> IoT is an umbrella term that refers to the billions of physical objects or things connected to the Internet, all of which collect and exchange data with other devices and systems over the internet.
>
> IoT Devices are hardware devices such as sensors, gadgets, appliances and other devices/machines that collect and exchange data over the internet.

19. **Data Breaches:** A data breach is a theft of data by a malicious attacker. Motives for data breaches include crime (i.e., identity theft), a desire to embarrass an institution (e.g., Edward Snowden or the DNC hack), and espionage.

20. **Data Manipulation:** Data manipulation is a form of cyber-attack that doesn't steal data but aims to change the data to make it harder for an organization to operate.

21. **Data Destruction:** Data destruction is when a cyber attacker attempts to delete data.
22. **Malvertising:** Malvertising is the use of online advertising to spread malware.
23. **Rogue Software:** Rogue software is malware that is disguised as real software.
24. **Unpatched Software:** Unpatched software is software that has a known security weakness that has been fixed in a later release but not yet updated.

System-Based Attacks

These are the attacks which are intended to compromise a computer or a computer network.

Some of the important system-based attacks are as follows:

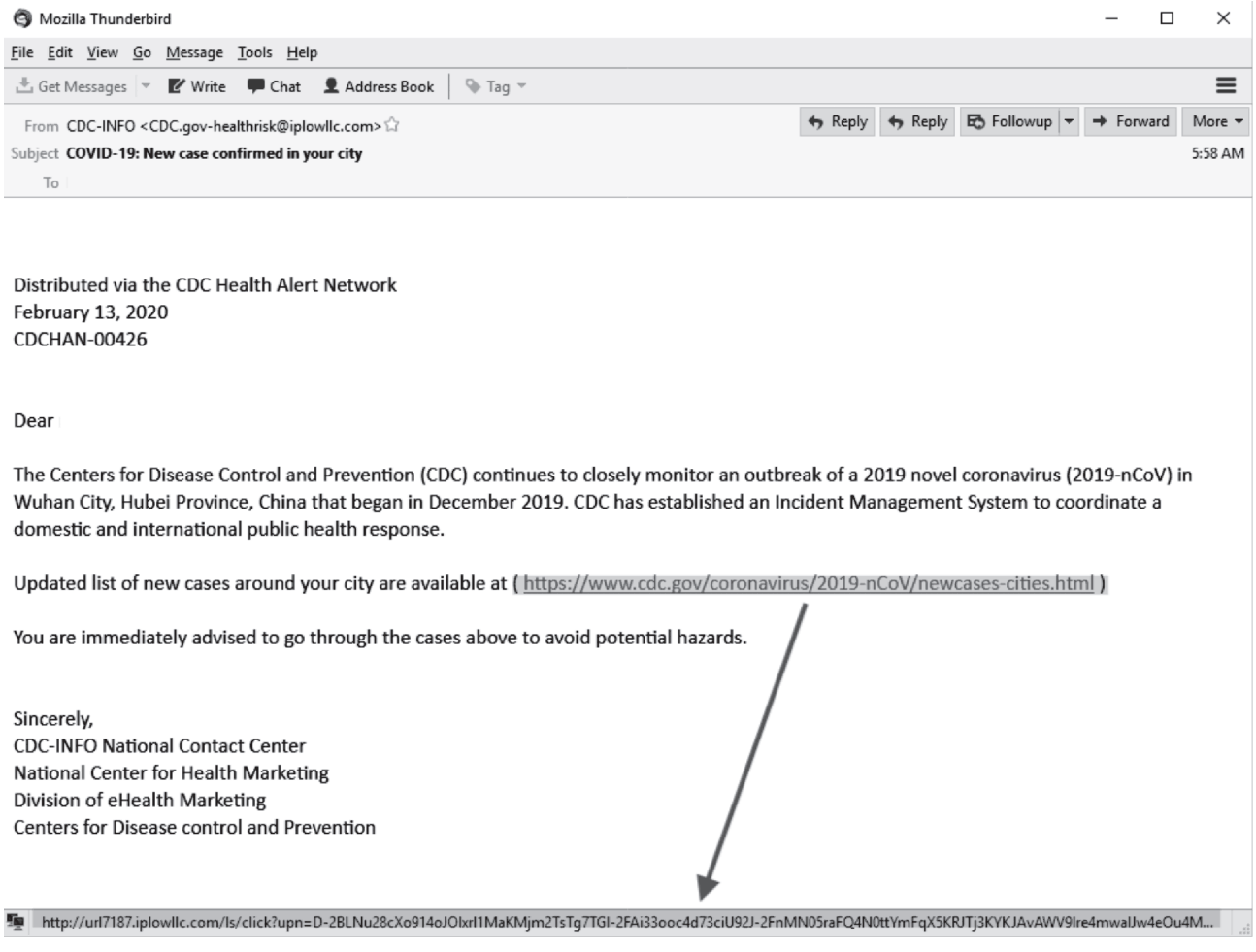
1. **Virus:** It is a type of malicious software program that spreads throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.
2. **Worm:** It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works in the same manner as a computer virus. Worms often originate from email attachments that appear to be from trusted senders.
3. **Trojan horse:** It is a malicious program that makes unexpected changes to computer settings and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.
4. **Backdoors:** It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.
5. **Bots:** A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.
6. **Zero-Day Exploits:** A zero-day exploit is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching the flaw.
7. **Advanced Persistent Threats:** advanced persistent threat is when an unauthorized user gains access to a system or network and remains there without being detected for an extended period of time.
8. **Data Centre Disrupted by Natural Disaster:** The data center your software is housed in could be disrupted by a natural disaster like flooding.
9. **Drive-by Downloads:** A drive-by download attack is a download that happens without a person's knowledge often installing a computer virus, spyware, or malware into the system.
10. **Intellectual Property Theft:** Intellectual property theft is stealing or using someone else's intellectual property without permission.
11. **Supply Chain Attacks:** A supply chain attack is when a cybercriminal hacks an organization by compromising a third-party vendor in its supply chain.

Recent Cybers Threats[16] - 2022

Example of some of the common cyber threats are as follows:

Covid-Themed Phishing Attacks

Since the coronavirus pandemic, Covid-themed phishing attacks have spiked, preying upon the virus-related anxieties of the public.

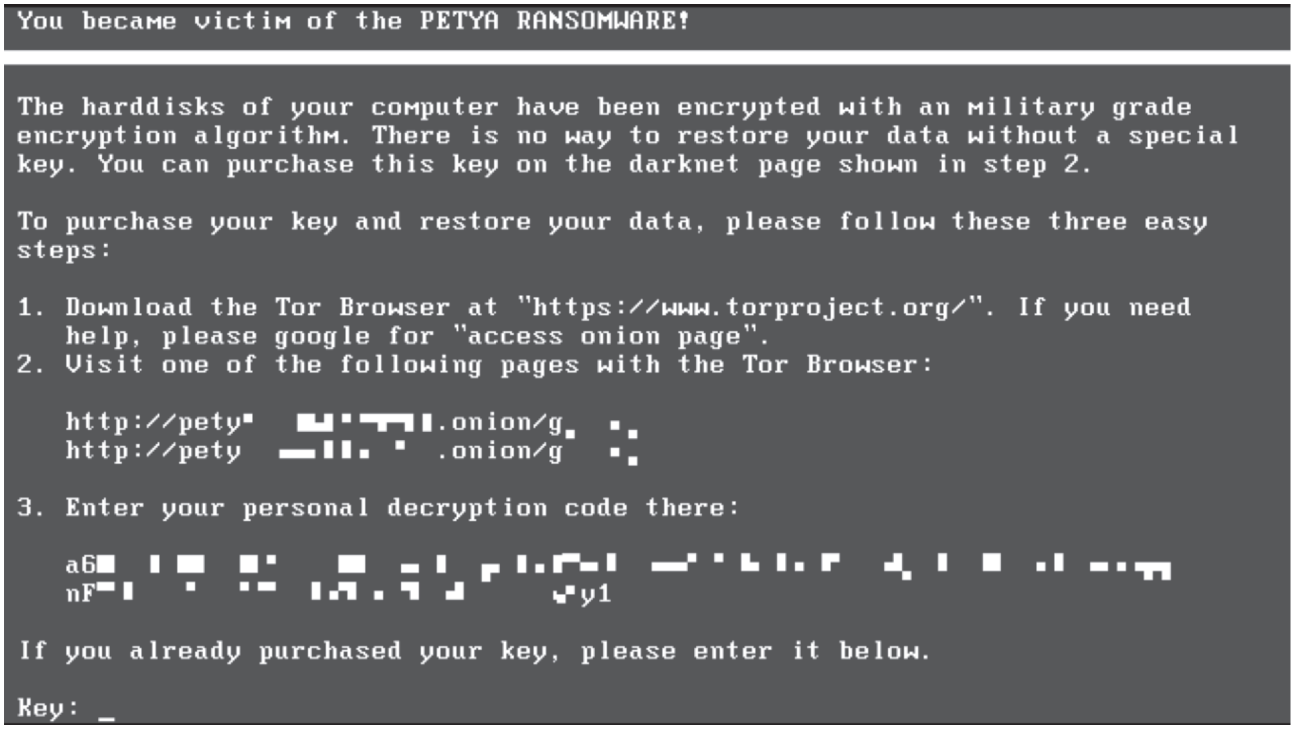


Source: ncsc.org

Ransomware Attacks

Ransomware attacks are one of the most frightening cyber threats. During these attacks, a victim's sensitive data is encrypted and only decrypted if a ransom price is paid. Victims only become aware that they've been compromised when they are presented with a formidable message announcing the successful attack. Sometimes these messages are falsely attributed to law enforcement agencies.

16. For more details, kindly read Tunggal Abi Tyas (2022) Cybersecurity: What is a Cyber Threat, UpGuard.



Source: nytimes.com.

Insider Threats

Insider threats includes the security threats and attacks made by the insiders like employers, outsourcing vendors and alike. Unlike phishing attacks, this type of security-bypassing cyber threat cannot be mitigated with a control strategy.

Supply Chain Attacks

According to the Cost of a Data Breach Report, 2022 by IBM[17] and the Ponemon Institute, it was revealed that third-party software vulnerabilities are gaining popularity as a primary attack method.

Polyglot Files

Polyglot are files that can have multiple file type identities. Polyglot files as such are not hostile by nature. Cybercriminals package malicious code into polyglot files to bypass file-type security controls.

Distributed Denial of Service (DdoS) Attacks

As the adoption rate of IoT devices in both the home and office continues to rise, the risk of DDoS attack rises accordingly. During a DDoS attack, cybercriminals direct a high concentration of network requests from multiple compromised IoT devices at a targeted website. This causes the victim's servers to overload, forcing them offline. All forms of DDoS are illegal, even if it is used to gain an advantage during a friendly online gaming session.

17. Complete Report is available at https://www.ibm.com/downloads/cas/3R8N1DZJ

Social Engineering

Social engineering, in the context of cyber threats, is an effort to obtain login credentials through manipulation and trickery. Phishing campaigns are the usual attack vectors of social engineering, but these cyber threats can also be presented in person. For example, threat actors posing as IT professionals asking for your password.

Phishing

Phishing attacks are a subcategory of social engineering, the differentiator is that they most commonly deployed via email, whereas a social engineering attack could occur through a telephone conversation.

According to the 2022 cost of a data breach report by IBM[18] and the Ponemon Institute, in 2022, Phishing was the second most expensive data breach attack vector, averaging US$ 4.91 million per breach, increasing from US$ 4.65 million in 2021.

Malvertising

The year 2022 has seen an increase in the instances of Malvertising. An example of a malvertising attack is the Latin American banking trojan known as MIspadu. The trojan was embedded in a Facebook ad campaign for McDonald's coupons. When users interacted with the ad, a zip file containing the bank credential-stealing trojan was downloaded and installed on their system.

Mispadu malvertising campaign - Source: welivesecurity.com

Zero-Day Exploits

A zero-day exploit is a software vulnerability or flaw that is discovered and exploited by hackers before it is known to software creators or sellers. The term "zero-day" refers to the fact that programmers have no time to address or patch the issue given that they too only recently noticed it.

Zero-day exploits are security vulnerabilities that are exploited by cybercriminals before a patch is released for them. These exposures are usually associated with ubiquitous software providers. A recent example is a zero-day exploit impacting Microsoft Exchange servers.

18. Complete Report is available on https://www.ibm.com/downloads/cas/3R8N1DZJ

CYBER THREAT HUNTING[19] AND DIGITAL FORENSICS

Cyber Threat Hunting

Cyber Threat Hunting is a proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools.

It has to be clearly noted that there is a distinction between cyber threat detection versus cyber threat hunting. Threat detection is a somewhat passive approach to monitoring data and systems for potential security issues. In the present-day information technology era, it is still a necessity to take the aid of threat hunter. Proactive cyber threat hunting tactics have evolved to use new threat intelligence on previously collected data to identify and categorize potential threats in advance of attack.

In the current times, when security of information technology and its systems are imperative, we cannot sit back and wait for threats to strike our technologies, systems and networks; hence cyber threat hunting is required for developing hypotheses based on knowing the behaviors of threat actors and validating those hypotheses through active searches in the environment.. In threat hunting, experts don't wait for alarms or obvious signs of trouble. Instead, they use their skills to investigate deeply using forensic methods. Basically, they take a proactive and thorough approach to find and handle cybersecurity threats. Cyber threat hunting aggressively assumes that a breach in the enterprise has or will occur. Security personnel hunt down threats in their environment rather than deploy the latest tool.

Threat Hunting Investigations

Traditional cyber threat hunting is based on a manual process in which a security analyst scrutinizes data based on their knowledge of the network and systems to build assumptions about potential threats. Cyber threat hunting has advanced in effectiveness and efficiency through the addition of automation, machine learning, and User and Entity Behavior Analytics (UEBA) to alert enterprise security teams of potential risks.

Once the risk or potential risk, as well as frequency of a hunt has been determined, an investigation is initiated. Examples of Cyber Threat Hunting investigations include:

- *Hypothesis Driven Investigations*: When significant information of a new, imminent threat vector is discovered, cyber threat hunting will delve deeper into network or system logs in search of hidden anomalies or trends that could signal the new threat. Analytics Driven Investigation: Searches based on information gathered from Machine Learning (ML) and Artificial Intelligence (AI) tools.

  > ***Note:*** Machine Learning is a growing technology which enables computers to learn automatically from past data.

- *Tactics, Techniques, and Procedures (TTP) Investigation*: Hunting for attack mannerisms typically use the same operational techniques. This is helpful to source or attribute the threat and to leverage existing remediation methods that worked with these behaviors. Tactics, Techniques, and Procedure (TTP) investigation is an organised method of evaluating and comprehending the techniques and procedures employed attackers or adversaries in executing cyber attacks or harmful actions. It entails examining their approaches (overall strategy or plan), techniques (particular methods or instruments employed), and procedures (step-by-step processes or activities conducted) in order to acquire knowledge about their motivations, abilities, and potential effect.

19. Source: Trellix – What is Cyber Threat Hunting? Available at https://www.trellix.com/en-us/security-awareness/operations/what-is-cyber-threat-hunting.html

Threat Hunting Techniques

Though threat hunting is specific to each environment, yet some techniques can be applied to almost any environment. Some of the core threat hunting techniques include:

1. ***Baselining:*** Baselining helps the hunter understand what "normal" looks like within an organization. It is similar to developing an established or usual behaviour guide. This allows the hunter to immediately notice anything unusual or beyond the norm.
2. ***Attack-Specific Hunts:*** Baselining aids the hunter in understanding the overall hunt environment, but attack-specific hunts can help track malicious activity faster. Attack-specific hunts typically focus on a specific threat actor or threat. However, the limits of their specific hunt model can throw off false positives. Attack-specific hunts combine with baselining often produce good results.
3. ***Time Sensitivity:*** All hunts are time sensitive, and therefore require hunters to validate their baseline terms periodically. Keeping up with attackers' shifting to new techniques – or reverting back to old techniques – require hunters to validate intelligence-based hunts and even hunt again if legacy techniques are detected.
4. ***Third-Party Sources:*** Hunting for needles in a data haystack can overwhelm teams of hunters. Third-party providers can help guide hunters to more successful hunts. Following benefits can be gathered from third-party sources:
    - Ruling out false positive leads
    - Focus on interesting leads
    - IP lookups
    - Geolocation
    - Encrypted traffic metadata
    - Log detection
    - Attacker technique overlays
    - Link analysis of *internal* vs. *external or host* vs. *network data points*

Hunting Steps

A cyber threat hunt is composed of steps or processes designed for an efficient, successful hunt. These steps include:

Step 1: Hypothesis

Threat hunts begin with a hypothesis or a statement about the hunter's ideas of what threats might be in the environment and how to go about finding them. A hypothesis can include a suspected attacker's tactics, techniques, and procedures (TTPs). Threat hunters use threat intelligence, environmental knowledge, and their own experience and creativity to build a logical path to detection.

Step 2: Collect and Process Intelligence and Data

Hunting for threats requires quality intelligence and data. A plan for collecting, centralizing, and processing data is required.

Step 3: Trigger

A hypothesis can act as a trigger when advanced detection tools point threat hunters to initiate an investigation of a particular system or specific area of a network.

Step 4: Investigation

Investigative technology aids in the detection of anomalies in a system or network. It digs deep to find any unexpected activity that might be hazardous. It determines if these discoveries are harmless or actually malicious. So, it's like a tool that examines and distinguishes the harmless stuff from the harmful one.

Step 5: Response/Resolution

Data gathered from confirmed malicious activity can be entered into automated security technology to respond, resolve, and mitigate threats. Actions taken can include getting rid of harmful files, bringing back changed or deleted files to their original condition, updating rules for firewalls or intrusion prevention systems, installing security updates, and adjusting system settings. Throughout this process, there is also a focus on learning from the incident to enhance security and be better prepared against similar attacks in the future.

DIGITAL FORENSICS[20]

Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime. The term digital forensics was first used as a synonym for computer forensics. From legal perspective, digital forensics is the process of identifying, preserving, analysing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.[21] As per Techopedia - "*Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events. The context is most often for the usage of data in a court of law, though digital forensics can be used in other instances*."

Steps of Digital Forensics

In order for digital evidence to be accepted in a court of law, it must be handled in a very specific way so that there is no opportunity for cyber criminals to tamper with the evidence.

Steps of Digital Forensics

Identification - First, find the evidence, noting where it is stored.
Preservation - Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.
Analysis - Next, reconstruct fragments of data and draw conclusions based on the evidence found.
Documentation - Following that, create a record of all the data to recreate the crime scene.
Presentation - Lastly, summarize and draw a conclusion.

DIGITAL INTELLECTUAL PROPERTY

As per the definition given by the Law Insider, Digital Intellectual Property means any and all of the following that is owned by Digital on, or any time after, the date hereof : (i) trade secrets, unpatented formulations, manufacturing methods and other know-how, (ii) copyrights, (iii) all patents on and pending applications to

20. Source: https://www.eccouncil.org/what-is-digital-forensics/#:~:text=SQL%20Injection%20Attack%3F-,What%20Is%20Digital%20Forensics%3F,a%20synonym%20for%20computer%20forensics.

21. Also access write up on digital forensics available at https://www.sentinelone.com/cybersecurity-101/what-is-digital-forensics-and-incident-response-dfir/?utm_content=demo-request&utm_medium=paid-search&utm_source=google-paid&utm_campaign=apj-t1-en-g-s-dsa-rlsa&utm_term=&utm_campaignid=19582401347&gclid=EAIaIQobChMI4MfN3p-D_QIVjZNmAh1yVAq0EAAYAiAAEgKf0fD_BwE

patent any technology or design; (iv) all registrations of and applications to register copyrights; and (v) computer software, including systems, applications, program listings, manuals and documentation (whether owned by Digital Electronics or licensed by Digital Electronics from third parties).

In simple words, Digital Intellectual Property (Digital IP) is intellectual property in digital format. Throughout the globe, the businesses and the individual stores, create, or otherwise handle some sort of digitalized information. Though protecting digital intellectual property encourages increased levels of innovation and creativity, resulting in the acceleration of progress, yet reality of digital information poses problems surrounding the use and re-use of information, and the rights and responsibilities of rights holders and consumers under existing laws.

While Digital IP encourages innovation, creativity, and economic growth, protecting it poses a challenging task, and is difficult for a number of reasons. Digital products are not tangible, and can be reproduced at a very low cost with the potential for immediate delivery via the Internet across virtually unlimited geographic markets. There are many stakeholders that can represent a broad range of legitimate concerns. Hence, it is important to understand what are different concerns for protecting Digital IP and the strategies to protect digital IP.

Ways for Protection of Digital / Intellectual Property:[22]

Digital Rights Management (DRM) technologies (also known as Electronic Rights Management Systems) ensure copyright through identifying and protecting the content, controlling access of the work, protecting the integrity of the work and ensuring payment for the access. DRM technologies prevent illegal users from accessing the content. User ID and password are used to protect access, along with licensing agreements. Another way to protect digital content is through Technical Protection Measures (TPM). These technologies allow publishing companies in securing and protecting content such as music, text and video from unauthorized use. If an author wishes to collect fee for use of his or her work, then DRM technology can be used.

The TPM and DRM technologies are increasingly employed to sell and distribute content over the Internet.

1. **Cryptography:** Cryptography is the oldest mechanism employed to ensure security and privacy of information over networks.. This process involves encrypting or scrambling the information to make it unreadable or in a language that is difficult to understand. Only the authorized user has the ability to decrypt or unscramble it. However, cryptography protects the work during transmission or distribution only. After the work is decrypted, it loses its protective measures.
2. **Digital Watermark Technology:** A digital watermark is a digital signal or pattern inserted into a digital document. It is similar to the electronic on-screen logo used by TV channels. A unique identifier is used to identify the work. The message might contain information regarding ownership, sender, recipient etc. or information about copyright permission. The system consists of a watermark generator, embedder and a watermark detector decoder. The legal user can remove these watermarks with a predetermined algorithm. The watermarking technology is extensively used in protecting multimedia works.
3. **Digital Signature Technology:** Digital signature includes identity of the sender and/or receiver date, time, any unique code etc. This information can be added to digital products. This digitally marks and binds a software product for transferring to a specified customer. Digitally signed fingerprints guarantee document authenticity and prevent illegal copying.
4. **Electronic Marking:** In this technique, the system automatically generates a unique mark that is tagged to each of the document copies. This technique is used to protect copyright as well as in electronic publishing where documents are printed, copied or faxed.

22. Source: http://eprints.rclis.org/28939/1/Intellectual%20Property%20Rights%20in%20Digital%20Environment_ISI.pdf

5. **Security Features of Operating System:** For protection of files, data etc. the operating system of computer such as Windows 2000 Professional, Windows 2000 Server, MS-SQL Server has some unique special security and integrity features.

LIABILITY OF ONLINE PLATFORMS

With the rise of e-commerce and online trading, online platforms are increasingly exposed to claims of intellectual property ("IP") infringement. Their visibility and deep pockets often make them a more worthy target as compared to individual users of platforms, whose obscure identities and business scale seldom justify protracted legal proceedings.

Indeed internet has revolutionized the way we interact; however, it has also bought with it a host of problems such as hate speech, fake news, illegal lobbying and personal data theft. The number of these issues not only make the criminal/offender liable, yet many a times, online platforms are also made liable for the cyber security threat.

As per Section 2 (1)(w) of Information Technology Act, 2000 - *Unless the context otherwise requires - "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.*

As the per the above definition, online platforms fall under the definition of intermediary. Hence, lets us understand the liability of intermediaries and the legal provisions governing the same.

Intermediaries are widely recognized as essential cogs in the wheel of exercising the right to freedom of expression on the Internet. Most major jurisdictions around the world have introduced legislations for limiting intermediary liability in order to ensure that this wheel does not stop spinning. With the 2008 amendment of the Information Technology Act 2000, India joined the bandwagon and established a 'notice and takedown' regime for limiting intermediary liability.

> "Intermediary liability, which is based on the legal principle of vicarious liability, means that the service providers shall be held accountable for any illegal act of the user on their platform. As Rebecca MacKinnon has said, "Intermediary liability means that the intermediary, a service that acts as 'intermediate' conduit for the transmission or publication of information, is held liable or legally responsible for everything its users do."

But in the recent times, considering the abuse of online platforms, it is demanded time and again to create an efficient regulatory regime for all the intermediaries including online platforms.[23]

1. 26 Leading E-Commerce Platforms Declare Compliance with Self-Audit to Eliminate Dark Patterns

In a major step towards protecting consumer interest in the digital marketplace, 26 leading e-commerce platforms have voluntarily submitted self-declaration letters confirming compliance with the *Guidelines for Prevention and Regulation of Dark Patterns, 2023*. This development marks a significant milestone in India's efforts to curb deceptive online design practices that mislead or manipulate consumers. These platforms have conducted internal self-audits or third-party audits to identify, assess and eliminate any presence of dark patterns. All 26 companies have declared that their platforms are free from dark patterns and do not deploy any manipulative user interface designs. The proactive industry-wide compliance demonstrates a

23. Sur Aihik (August 12, 2022): India needs legislation to hold platform liable for online harms: IT for change. Available at https://www.moneycontrol.com/news/business/india-needs-legislation-to-hold-platforms-liable-for-online-harms-it-for-change-9018861.html

strong commitment towards consumer transparency, fair trade practices, and ethical digital ecosystems. This voluntary alignment underscores the fact that consumer protection and business growth can go hand-in-hand, strengthening brand trust and long-term credibility.

1. CCPA Acknowledges Compliance; Calls It Industry-Best Practice

The Central Consumer Protection Authority (CCPA) has appreciated these declarations, terming them exemplary and encouraging other companies to adopt similar self-regulation. CCPA had earlier directed the companies to upload their self-audit declarations prominently on their websites for easy public access. The CCPA strongly urges all other e-commerce platforms, marketplace entities, service providers, and app developers to follow the example set by these companies. Every business operating in India's digital space must recognize that manipulative practices are short-sighted strategies that harm both consumers and businesses in the long run. Through the National Consumer Helpline (NCH), social media campaigns, informative videos, and outreach programmes, consumers have been educated about identifying dark patterns and reporting them. Such complaints are being systematically addressed, and enforcement action is being contemplated wherever necessary. The CCPA has reaffirmed that it is maintaining a close watch on potential violations and will not hesitate to act against errant platforms.

2. Background

The Guidelines for Prevention and Regulation of Dark Patterns, 2023, notified on 30 November 2023, identify and prohibit 13 dark patterns including:

1. False Urgency	8. Drip Pricing
2. Basket Sneaking	9. Disguised Advertisements
3. Confirm Shaming	10. Nagging
4. Forced Action	11. Trick Wording
5. Subscription Trap	12. SaaS Billing
6. Interface Interference	13. Rogue Malwares
7. Bait & Switch	

These guidelines, issued under the Consumer Protection Act, 2019, form a key part of the Government's strategy to build a transparent, trustworthy and consumer-centric digital marketplace. To strengthen compliance, CCPA issued an Advisory on 5 June 2025, instructing all e-commerce platforms and online service providers to conduct a mandatory self-audit within three months to detect and eliminate dark patterns. The advisory emphasized transparency, explicit consent, clear disclosures, and non-manipulative design. Following multi-stakeholder consultations with industry, academia and consumer bodies, CCPA has built a robust regulatory framework that aims to eliminate deceptive digital design at its core.

3. List of Platforms That Submitted Self-Audit Declarations as follows:

1. Page Industries (Jockey, Speedo) – Self-audit conducted; platform free from dark patterns.
2. William Penn Pvt. Ltd. (Sheaffer, Lapis Bard) – Self-audit conducted; no dark patterns detected.
3. Pharm Easy (Axelia Solutions Pvt. Ltd.) – Internal audit confirms compliance with guidelines.
4. Zepto Marketplace Pvt. Ltd. – Platform UI/UX audited; ongoing monitoring in place.
5. Curaden India (Curaprox) – Self-audit confirms absence of dark patterns.

6. Duroflex Pvt. Ltd. – Self-audit confirms platform compliance.
7. Flipkart Internet Pvt. Ltd. – Third-party audit confirms no dark patterns.
8. Myntra Designs Pvt. Ltd. – Third-party audit confirms compliance.
9. Cleartrip Pvt. Ltd. – Third-party audit confirms platform is dark-pattern-free.
10. Walmart India Pvt. Ltd. – Third-party audit concludes no dark patterns.
11. MakeMyTrip (India) Pvt. Ltd. – Declared platforms require explicit consumer consent; no pre-ticked boxes.
12. BigBasket (Innovative Retail Concepts Pvt. Ltd.) – Internal review completed; remedial measures implemented.
13. Tira Beauty (Reliance Retail Ltd.) – Internal review confirms compliance.
14. JioMart (Reliance Retail Ltd.) – Platform declared free of dark patterns; continued monitoring.
15. Reliance Jewels – Declared fully compliant.
16. Ajio – No dark patterns; ongoing platform checks.
17. Reliance Digital – Internal review ensures full compliance.
18. Netmeds – Declared free of dark patterns.
19. Hamleys – Internal review confirms compliance.
20. MilBasket – Platform declared compliant.
21. Swiggy Ltd. – Self-audit completed; committed to enhancing consumer experience.
22. Tata 1mg – Comprehensive self-audit; platform designed for consumer-centric behaviour.
23. Zomato – Internal assessment aligns platform with CCPA advisory.
24. Blinkit – Internal review affirms transparent, responsible design.
25. Ixigo – Declared free of dark patterns, adhering to highest compliance standards.
26. Meesho Ltd. – Declared free from all 13 CCPA-identified dark patterns; regular self-checks ongoing.

Legal/Regulatory regime of "Intermediary/Online Platform Liability" in India

Kapoor Saumya (Chadha and Chadha Intellectual Property Law Firm) in her article titled *Tracking the development of "Intermediary Liability" in India in India*[24], has meticulously discussed the regulation regime of intermediaries vide various laws and sub-legislations incorporated in India. Further, some landmark cases in India are also discussed wherein Indian courts have been proactive in adjudicating on these issues. A brief of that article is mentioned as below:

Information Technology Act, 2000 (IT Act)

Under the IT Act, initially only network service providers were protected "for any third-party information or data made available by them if they proves that the offence or contravention was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such offence or contravention." Thus, the original IT Act provided little or no safe harbour protection to intermediaries.

24. Available at https://s3.amazonaws.com/documents.lexology.com/8db09138-482a-4951-b255-6513ca1eaad3.pdf?AWSAccessKeyId=AKIAVYILUYJ754JTDY6T&Expires=1675854906&Signature=tF9cQSg9FZoCzslcQj%2Ft%2BvoDPtA%3D

Safe Harbour Protection

The safe harbour protection for e-commerce marketplaces is an important aspect that deserves careful consideration. The concept of safe harbour under Section 79 of the IT Act, 2000, acts as a defence for the intermediaries, but there are some instances where Intellectual Property Rights (IPR) are openly violated by the intermediaries. Safe harbour protection acts as an inherent security granted to intermediaries against the imposition of liability for acts done by third parties.

Safe harbour provisions were introduced to protect intermediaries from becoming liable for the acts of third parties, provided the intermediary observed 'due diligence'. Intermediaries are shielded from liability under Section 79 of the IT Act for data, material, and information shared by users through them but over which they have no direct knowledge. Under the safe harbour, intermediaries are protected from third-party information and data made available or hosted by them thereby acting as a defence. Intermediaries are protected by safe harbour from all legal consequences unless they knew that illicit content was being broadcast on their platform.

Avnish Bajaj vs. State[25] and the Amendment to the IT Act 2008

In this case, the Managing Director (and not the company Baazee.com) was charged with criminal provisions under the Indian Penal Code, 1860 (Hereinafter referred to as 'IPC') as well as the Information Technology Act, 2000 (Hereinafter referred to as 'IT Act'), for content circulated by a third party on its ecommerce platform. However, the Managing Director escaped liability since the company was not added as an accused either before the High Court or before the Supreme Court. Further, the Delhi High Court also observed that companies bear the risk of acquiring knowledge if the content uploaded escapes the filters which are meant for blocking pornographic content.

In this case, it was also observed that there was a requirement for widening the scope of protection given to intermediaries, and thus, the IT Act was amended in 2008 to include a safe harbour regime under Section 79 of the IT Act and to amend the definition of intermediaries (as it reads presently). Section 79 of the Information Technology Act 2000[26] introduced the 'safe harbour' immunity clause that protected an intermediary from being held liable for third-party content on its platform and affords broad-ranging legal immunity – provided the intermediary observed 'due diligence' and followed certain 'guidelines' as prescribed by the Central Government. Only if due diligence laid down by the government is not followed by the intermediary, it would be made liable for a third party's actions, even if the same were done without the knowledge of the intermediary.

The Information Technology (Intermediaries Guidelines) Rules, 2011 ("Intermediary Guidelines") (2011)[27]

After the amendment to the IT Act in 2008, the Government of India introduced the Intermediary Guidelines,

25. Avnish Bajaj vs. State, 150 (2008) DLT 769

26. Section 79 of Information Technology Act reads as : Exemption from liability of intermediary in certain cases. - (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. (2) The provisions of sub-section (1) shall apply if- (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary does not- (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf. (3) The provisions of sub-section (1) shall not apply if- (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or othorise in the commission of the unlawful act; (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner. Explanation. -For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

27. The Intermediaries Guidelines Rules, https://meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf

which were mandatory for all intermediaries to follow for claiming safe harbour protection. These are to be read in consonance with the IT Act and the due diligence requirements that must be observed by intermediaries, provided under Rule 3, are:

- Intermediaries to publish rules and regulations, privacy policy and user agreement;
- Rules and regulations, terms and conditions or user agreement shall specify all prohibited acts, i.e. belonging to other persons, grossly harmful, harassing or unlawful, harms minors, infringes any intellectual property rights, violates any law, is deceiving or misleading, impersonates any person, contains virus, threatens India etc. and the intermediary should inform users that violation of same shall lead to termination of access,
- Intermediaries to not knowingly host or publish information as specified in sub-rule (2),
- Intermediaries to disable such information within 36 hours and storage of same for 90 days for investigation purposes,
- Intermediaries to provide assistance to authorised government agencies,
- Intermediaries to take all reasonable measures to secure its computer resource,
- Intermediaries to report cyber security incidents to the Indian Computer Emergency Response Team and
- Intermediaries to appointment and publish the details of a Grievance Officer on its website.

However, the IT Act and the Intermediary Guidelines were inundated by various issues such as ambiguity in prohibited content and forced decision by intermediaries. Further, any person could request the intermediaries to take down the unlawful content. However, these issues were mostly resolved in the Shreya Singhal judgement.

Shreya Singhal vs. Union of India (2015)[28]

In 2015, in the landmark Shreya Singhal judgement, the Supreme Court for the first time recognized the Indian citizen's free speech rights over the Internet by striking down and declaring unconstitutional the draconian Section 66A of the IT Act, which provided for punishment for sending offensive messages through communication services.

Further, regarding intermediary liability, the Court held that "*Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material.... Similarly, the Information Technology Intermediary Guidelines Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment*."

The Court also observed that "*it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.*" Subsequently, in the case of Kamlesh Vaswani v Union of India (Writ Petition (Civil) No. 177 of 2013), the Supreme Court issued directions to intermediaries to disable specific content where website operating child pornography was sought to be restricted.

My Space Inc. vs. Super Cassettes Industries Ltd. (2017)[29]

In this case, the division bench of the Delhi High Court distinguished Copyright matters and held that if

28. Shreya Singhal vs. Union of India, [(2015) 5 SCC 1]

29. My Space Inc. vs Super Cassettes Industries Ltd., [236 (2017) DLT 478]

intermediaries were given the responsibility of identifying illegal content, it could have a chilling effect on free speech and will lead to private censorship. This judgment dealt with uploading of music on myspace.com and a copyright infringement suit was brought by Super Cassettes India Ltd.

The Court also gave the concept of 'actual or specific knowledge' and held that intermediaries can be held liable if they have actual or specific knowledge of the existence of infringing content on their website from content owners and despite such notice, they do not takedown the content. There is no necessity of a court order in such cases. The two-judge bench of the Delhi High Court further pronounced that "*in case of internet intermediaries, interim relief has to be specific and must point to actual content, which is being infringed*".

Kent Ro Systems Ltd & Anr vs. Amit Kotak & Ors (2017)[30]

In this case, the Petitioner, in a suit for permanent injunction against the Respondent for infringing its intellectual property rights by copying its designs, also added eBay India as a party for permitting the Respondent to advertise, offer to sell and sell its product on its website.

The Court held that "*to hold that an intermediary, before posting any information on its computer resources is required to satisfy itself that the same does not infringe the intellectual property rights of any person, would amount to converting the intermediary into a body to determine whether there is any infringement of intellectual property rights or not... The IT Rules, according to me do not oblige the intermediary to, of its own, screen all information being hosted on its portal for infringement of the rights of all those persons who have at any point of time complained to the intermediary... Merely because intermediary has been obliged under the IT Rules to remove the infringing content on receipt of complaint cannot be read as vesting in the intermediary suo motu powers to detect and refuse hosting of infringing contents... I am of the view that to require an intermediary to do such screening would be an unreasonable interference with the rights of the intermediary to carry on its business*." Thus, the Court reiterated the specific knowledge principle of the Myspace case.

Subsequently, *in Lifestyle Equities C.V. and Ors v Amazon Sellers Service Private Limited & Another[31]*, the Court directed Amazon to share the details about the person who had uploaded the links as well as to remove the links advertising the infringing and counterfeit goods.

Christian Louboutin SAS vs. Nakul Bajaj and Ors (2018)[32]

In this case, the Delhi High Court clarified the responsibilities and liabilities of ecommerce intermediaries that were previously undetermined. The Court held that the Defendant was not an intermediary and was an "active participant" and thus, would be liable for infringement. The Court also held that the conduct of intermediaries, in failing to observe 'due diligence', could amount to 'conspiring, aiding, abetting or inducing' unlawful conduct and would disqualify them from the 'safe harbour' exemption, as per Section 79(3)(a) of the IT Act.

Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018, ("Draft Rules") (2018)[33]

On December 24, 2018, Ministry of Electronics & Information Technology released the Draft Rules for amending the existing Intermediaries Guidelines to curb the "Misuse of Social Media and spreading Fake News". These Draft Rules place several obligations on the intermediaries, some of which are enabling traceability to determine the originator of the information for assistance to law enforcement, proactive monitoring of content uploaded on its platform by deploying automated tools, takedown of illegal content within 24 hours, and mandatory incorporation of companies having more than 5 million users in India.

30. Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors, [2017 (69) PTC 551 (Del)].

31. Lifestyle Equities C.V. and Ors v Amazon Sellers Service Private Limited & Anr., [CS (COMM) 1015/2018].

32. Christian Louboutin SAS vs. Nakul Bajaj & Ors, [2018(76) PTC 508(Del)]

33. https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_%20Amendment_24122018.pdf

M/S Luxottica Group S.P.A & Another vs. M/S Mify Solutions Pvt Ltd & Ors (2019)[34]

The Plaintiff filed a trademark infringement suit alleging that the Defendant sells counterfeit products of the Plaintiff's brand 'OAKLEY'. The Court held that the due diligence and care required under the IT Act had not been met and the Defendant was guilty of trademark and copyright infringement. The Court herein applied the tests laid down in the Christian Louboutin case to determine whether the ecommerce platforms claiming to be exempted under Section 79 of the IT Act actually qualify as intermediaries or not. The Court observed that presence of any element which shows active participation could deprive intermediaries of the immunities and factors such as allowing storing of counterfeit goods, using the mark in an invoice, advertising the mark etc., would determine whether the entity in question is an intermediary or not.

Amway India Enterprises Pvt Ltd vs. 1Mg Technologies Pvt Ltd & Another (2019)[35]

One of the main issues in this case was the conflict between Direct Selling Business and ecommerce platforms and whether the intermediary had stepped into the shoes of the seller by setting its own retail prices, discounts, return/refunds policies etc. Thus, the issue was whether the intermediary had violated the Direct Selling Guidelines issued by the Government, which were binding on the Plaintiff. In this regard, the Single Judge held that the Direct Selling Guidelines were binding on ecommerce platforms and the sellers on such platforms. However, the Division Bench held that such guidelines are advisory in nature and are not law and thus, not enforceable.

Further, the Court also gave a detailed reasoning as to why major ecommerce giants are actively involved and thus, do not qualify as intermediaries entitled to protection under the 'safe harbour' provided in Section 79 of the IT Act. It was held that any non-compliance of the due diligence requirements as per the Intermediary Guidelines and failure to adhere to their own policies would make the ecommerce platforms liable. The Division Bench also observed that the value-added services provided by the Defendant as online market places, do not dilute the safe harbour granted to them under Section 79 of the IT Act.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[36]

The Intermediary Guidelines Rules, 2011 were replaced by the Information Technology (IT) Rules, 2021, which were formulated by the Union Government in accordance with Section 87(2) of the IT Act, 2000. As per the said rules, large digital platforms with more than 5 million users would be required to publish periodic compliance reports each month. The Rules prescribe a framework for the regulation of online content in terms of current affairs, news, and audio-visual content. In India, all intermediaries, including OTT platforms and digital portals, must offer a grievance redressal process to address user complaints. These rules aim to empower netizens for the timely resolution of their grievances with a mechanism for redressal and assistance of a Grievance Redressal Officer (GRO) residing in India.

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, Rule 4(1)(d), mandate that social media outlets post monthly compliance reports that include the following information:

- Information about complaints filed and measures undertaken in response, and
- The number of particular communication links or informational components that the social media platform has blocked or erased as part of proactive monitoring.

34. Luxottica Group SPA and Ors v Mify Solutions Pvt Ltd and Ors, [2019(77) PTC 139(Del)]

35. Amway India Enterprises Pvt Ltd v 1Mg Technologies Pvt Ltd & Anr., [CS (OS) 410/2018, CS (OS) 453/2018, CS (OS) 480/2018, CS (OS) 531/2018, CS(OS) 550/2018, CS (OS) 75/2019 and CS (OS) 91/2019]

36. Source: Liability of online marketplaces in India (2021) iPleders.

LAWS APPLICABLE TO AI AND CYBER LAWS

Information Technology Act, 2000 (IT Act, 2000)

Overview of IT Act, 2000

It is the first law to regulate cyberspace which has been approved by the Indian Parliament. The Act defines the following as its object:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

However, as cyber-attacks become dangerous, along with the tendency of humans to misunderstand technology, several amendments are being made to the legislation. It highlights the grievous penalties and sanctions that have been enacted by the Parliament of India as a means to protect the e-governance, e-banking, and e-commerce sectors. It is important to note that the IT Act's scope has now been broadened to include within its ambit all the latest communication devices.

The IT Act states that an acceptance of a contract may be expressed electronically unless otherwise agreed and that the same shall have legal validity and enforceability. In addition, the Act is intended to achieve its objectives of promoting and developing an environment conducive to the implementation of electronic commerce.

The important provisions of IT Act, 2000

The IT Act is prominent in the entire Indian legal framework, as it directs the whole investigation process governing cyber-crimes. Following are some of the relevant sections:

- Section 43: This section of the IT Act applies to individuals who indulge in cyber crimes such as damaging the computers of the victim, without taking due permission of the victim. In such a situation, if a computer is damaged without the owner's consent, the owner is fully entitled to a refund for the complete damage.

  In *Poona Auto Ancillaries Pvt. Ltd., Pune vs. Punjab National Bank, HO New Delhi & Others (2018)*, Rajesh Aggarwal of Maharashtra's IT department (representative in the present case) ordered Punjab National Bank to pay Rs. 45 lakh to Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. In this case, a fraudster transferred Rs. 80.10 lakh from Matharu's account at PNB, Pune after the latter answered a phishing email. Since the complainant responded to the phishing mail, the complainant was asked to share the liability. However, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant.

- Section 66: Applies to any conduct described in Section 43 that is dishonest or fraudulent. The offence under this section is punishable with three years of imprisonment in such instances, or a fine of up to Rs. 5 lakh.

In *Kumar vs. Whiteley (1991),* during the course of the investigation, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added, and modified files. As a result of investigations, Kumar had been logging on to a BSNL broadband Internet connection as if he was an authorized legitimate user and modifying computer databases pertaining to broadband Internet user accounts of subscribers. On the basis of an anonymous complaint, the CBI registered a cyber-crime case against Kumar and conducted investigations after finding unauthorized use of broadband Internet on Kumar's computer. Kumar's wrongful act also caused the subscribers to incur a loss of Rs. 38,248. N G Arun Kumar was found guilty and sentenced by the Additional

Chief Metropolitan Magistrate. The magistrate ordered him to undergo a rigorous year of imprisonment with a fine of Rs. 5,000 under Sections 420 of IPC and 66 of the IT Act.

- Section 66B: This section describes the penalties for fraudulently receiving stolen communication devices or computers, and prescribes a possible three-year prison sentence. Depending on the severity, a fine of up to Rs. 1 lakh may also be imposed upon the accused.
- Section 66C: The focus of this section is to prohibit identity theft, by penalising the act of fraudulently and dishonestly using the electronic signature, password or any other unique identification feature of any person. This section imposes imprisonment up to 3 years along with fine upto one lakh rupees.
- Section 66D: This section penalises cheating by personation using computer resources. Punishment if found guilty can be imprisonment of up to three years and/or up-to Rs. 1 lakh fine.
- Section 66E: Taking pictures of private area of any person, publishing or transmitting them without a person's consent is punishable under this section. Penalties, if found guilty, can be imprisonment of up to three years and/or up-to Rs. 2 lakh fine.
- Section 66F: This section prescribes punishment for the offence of cyber terrorism. An individual convicted of a crime can face imprisonment of up to life. An example: When a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, which challenged the security forces to prevent a terror attack planned on these institutions. The criminal was apprehended and charged under Section 66F of the IT Act.
- Section 67: This section punishes the act of publishing or transmitting obscene material in electronic form. If convicted, the prison term is up to five years and the fine is up to Rs. 10 lakh.

Positive and negative aspects of IT Act, 2000

This legislation confers the following benefits:

- Until recently, the development of electronic commerce in our country was hindered primarily due to a lack of legal infrastructure to govern commercial transactions online. Due to the enactment of this legislation, several companies are now able to conduct e-commerce activities without any fear.
- Digital signatures are officially recognized and sanctioned by the Act. Therefore, corporations and organizations are now able to use digital signatures to conduct online transactions.
- Additionally, the Act also paves the way for corporate entities to also act as Certification Authorities for the issuance of Digital Signature Certificates under the Act. There are no distinctions in the Act as to what legal entity may be designated as a Certifying Authority, provided the government's standards are followed.
- Furthermore, the Act permits the companies to electronically file any of their documents with any office, authority, body or agency owned or controlled by the appropriate government by using the electronic form prescribed by the concerned government.
- The use of electronic records and digital signatures in government and its agencies has been approved as a policy matter within the meaning of the IT Act. A digital signature is a mechanical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature enables the recipient to believe that the message was created by a known sender and has not been altered in transit, i.e., the message is tamper-proof. The Government has thus started using digital signatures across all platforms such as granting of licenses, permits, filing of applications, payment of charges and other financial transactions through electronic means.

- Hacking is a common threat faced by most companies nowadays. However, the IT Act changed the landscape completely. A statutory remedy is now provided to corporate entities in case anyone attempts to breaches their computer systems or network and damages or copies data. Damages can be claimed from anyone who uses a computer, computer system or computer network without the permission of the owner or other person in charge of the computer/system or network.

However, the said Act has a few drawbacks:

- Section 66A is considered to be in accordance with Article 19(2) of the Constitution of India since it does not define the terms 'offensive' and 'menacing'. It did not specify whether or not these terms involved defamation, public order, incitement or morality. As such, these terms are open to interpretation.

> ***Note:*** Article 19(2) of the Constitution curtails the freedom of speech and expression to some extent by enabling the State to impose restrictions in the interests of security and sovereignty of India, friendly relations with foreign states, public order, decency or morality, among other things.

- Considering how vulnerable the internet is, the Act has not addressed adequately issues such as privacy and content regulation, which are essential.
- A domain name is not included in the scope of the Act. The law does not include any definition of domain names, nor does it state what the rights and liabilities of domain name owners are.
- The Act doesn't make any provision for the intellectual property rights of domain name proprietors. In the said law, important issues pertaining to copyright, trademark, and patent have not been addressed, therefore creating many loopholes.

INFORMATION TECHNOLOGY RULES (IT RULES)

There are several aspects of the collection, transmission, and processing of data that are covered by the IT Rules, including the following:

- *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:* According to these rules, entities holding individuals' sensitive personal information must maintain certain security standards that are specified.
- *The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021:* To maintain safety over the web of users' data, these rules govern the role of intermediaries, including social media intermediaries, to prevent the transmission of harmful content on the internet.
- *The Information Technology (Guidelines for Cyber Cafe) Rules, 2011:* According to these guidelines, cybercafés must register with an appropriate agency and maintain a record of users' identities and their internet usage.
- *The Information Technology (Electronic Service Delivery) Rules, 2011:* Basically, these regulations give the government the authority to regulate the delivery of certain services, such as applications, certificates, and licenses, by electronic means.
- *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules):* CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. In accordance with rule 12 of the CERT-In rules, a 24-hour incident response helpdesk must be operational at all times. Individuals, organisations and companies can report cybersecurity incidents to Cert-In if they experience a Cybersecurity Incident or threat. The Rules provide an Annexure listing certain Incidents that must be reported to Cert-In immediately.

- Another requirement under Rule 12 is that service providers, intermediaries, data centres, and corporate bodies inform CERT-In within a reasonable timeframe of cybersecurity incidents. As a result of the Cert-In website, Cybersecurity Incidents can be reported in various formats and methods, as well as information on vulnerability reporting, and incident response procedures. In addition to reporting cybersecurity incidents to CERT-In in accordance with its rules, Rule 3(1)(l) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 also requires that all intermediaries shall disclose information about cybersecurity incidents to CERT-In.

Proposed Digital India Act: An Act in Progress to replace Information Technology Act, 2000

With digital transformation at its high in India, March 2023 has witnessed a magnificent move with the official announcement of enacting Digital India Act (DIA) while replacing a 24-year-old Information Technology Act of 2000 (IT Act). This proactive move by the Ministry of Electronics and Information Technology (MeitY) aligns with India's ambitious "Digital India" initiative.

On 9th March 2023, the Minister of State for the Ministry of Electronics and Information Technology (MEITY), held a consultation to officially announce that the Information Technology Act of 2000 (IT Act) will be replaced with a new Digital India Act (DIA), a future-ready legislation. The contents of the new act were laid down in the presentation. The MEITY is conducting rounds of consultations in the coming months and soliciting feedback from various stakeholders. This draft has generated debates and discussions on the regulation of the Internet today.[37]

Nine Pillars of Digital India

1. Broadband Highways
2. Universal Access to Mobile Connectivity
3. Public Internet Access Programme
4. e-Governance: Reforming Government through Technology
5. e-Kranti - Electronic Delivery of Services
6. Information for All
7. Electronics Manufacturing
8. IT for Jobs
9. Early Harvest Programmes

Necessity for Digital India Act (DIA)

The proposed Digital India Act (DIA) *inter-alia* with an aim to provide a *future ready legislation* opts "*principles and rule-based approach*" for regulating digital transactions including the evolving era of Artificial Intelligence and Machine Learning. With this background, we aim to discuss the salient features of DIA and its possible impact on industries for aligning their compliance calendar with principle and rule-based approach.

Need for Digital India Act

- Outdated Regulations: The existing IT Act of 2000 was crafted in an era when the internet had only 5.5 million users, and is ill-equipped to handle the internet's current state.
- Today, with 850 million users, various intermediaries, and new forms of user harms like cyberstalking and doxing, the IT Act falls short of addressing these complexities.
- Inadequacy of Current Regulations: Despite the existence of regulatory elements like Intermediary

37. Reproduced from Sanhita Chaurita (8th August 2023) Explained: The Digital India Act 2023, Vidhi Centre For Legal Policy.

Guidelines, Digital Media Ethics Code, and data protection rules, they are insufficient when it comes to governing new-age technologies.

- Need for Legal Adaptation: With technological advancements like AI, Blockchain, and IoT, the legal framework must evolve to address their unique challenges. This includes enhancing cybersecurity measures, data protection, and regulating emerging tech sectors.
- Addressing E-commerce and Online Content: The growth of e-commerce, digital transactions, and online content sharing requires updated regulations. The Digital India Act will tackle issues related to consumer protection, electronic contracts, and content moderation on social media platforms.
- Global Alignment and Best Practices: To engage effectively in the global digital landscape, India's regulations must align with international standards and practices.

On the path of digital economy, we are already witnessing reformative landscape of legal and regulatory regime with major focus on fintech sectors, enterprise and deep technology sectors, e-commerce, consumer protection and data management.

Among other factors, following the major reasons which necessitates the introduction of proposed Digital India Act:

Limitation of IT Act, 2000	Challenges in Cyberspace	Tech-Aligned Regulation
• IT Act is around 24 years old and was enacted in early days of internet. • It does not adequately cover modern internet-based services such e-commerce, social media platforms and alike. • Inadequate principles for data / privacy protection. • Legal recognition of electronic records, transactions and electronic signatures over the electronic medium	• Multiple categories of Intermediaries • Digital Media • Social Media • AI and ML • OTT • Complex forms of user harms – sim-swaps, catfishing, cyber stalking, online gaslighting • Disinformation • Increased flow of data and need to regulate the data at global parameters • Alignment with contemporary regulations including DPDP Act, 2023 and Limitation Act, 1963.	• Need for Global Standards of Cyber Laws • Comprehensive need on user rights, trust & safety. • Emerging Technology • High risk automated-decision making systems. • New forms of cybercrimes. • Requirement of a converged, coordinated & harmonized institutional regulatory body. • To strengthen user rights and security specially women and child safety.

Salient Features of Proposed Digital India Act

The proposed DIA includes following salient features:

- Principle and Rule based Approach
- Digital Governance and Adjudicatory Architecture
- Open Internet

- Safe and Secure Cyberspace
  - *For example - strengthening the penalty framework for non-compliance and issuing advisories on the information & data security practices, etc.*
- Responsible and Ethical Use of Online Technologies
- Safeguard Innovation and Promoting Start-ups
- Digital User Rights
- Regulation of Intermediaries (basis the type of Intermediary) –
  - *for example, enterprise software providers such as cloud service providers should not be subjected to the same set of regulations as that of significant social media intermediaries.*
- *Principle of Safe Harbour*
  - Accountability
  - Inclusive Regulatory Framework – *Balanced with sectoral regulations.*
  - Emerging Technology, Risk (Management) and Guard Rails
  - Ensuring Safety and Privacy of Children (*Industry Specific Requirements*)
  - Algorithmic Transparency and regulation of Artificial Intelligence (*"AI"*)

2. Government notifies amendments to Rule 3(1)(d) of the IT Rules, 2021 to enhance transparency, accountability and safeguards

The Ministry of Electronics and Information Technology (MeitY) has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 to amend the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021"). These amendments strengthen the framework of due diligence obligations of intermediaries under the Information Technology Act, 2000 ("IT Act"). Specifically, the amendments to Rule 3(1)(d) introduce additional safeguards to ensure that removal of unlawful content by intermediaries is carried out in a transparent, proportionate and accountable manner. The amended Rules will come into effect from 15th November, 2025. Background The IT Rules, 2021 were originally notified on 25th February, 2021 and subsequently amended on 28th October, 2022 and 6th April, 2023. They prescribe due diligence obligations on intermediaries, including social media intermediaries, with the objective of ensuring online safety, security and accountability. Under Rule 3(1)(d), intermediaries are required to remove unlawful information upon receiving actual knowledge either through a court order or notification from the Appropriate Government. The review undertaken by MeitY highlighted the need for additional safeguards to ensure senior-level accountability, precise specification of unlawful content, and periodic review of government directions at higher level. Key Features of the Amendments are as follow:

1. Senior-level Authorisation:

- Any intimation to intermediaries for removal of unlawful information can now only be issued by a senior officer not below the rank of Joint Secretary, or equivalent, or, where such rank is not appointed, a Director or an officer equivalent in rank—and, where so authorised, acting through a single corresponding officer in its authorised agency, where such agency is so appointed.
- In case of police authorities, only an officer not below the rank of Deputy Inspector General of Police (DIG), specially authorised, can issue such intimation.

2. Reasoned Intimation with Specific Details:

- The intimation must clearly specify the legal basis and statutory provision, the nature of the unlawful act, and the specific URL/identifier or other electronic location of the information, data or communication link ("content") to be removed.

- This replaces the earlier broad reference to 'notifications' with 'reasoned intimation' to align the Rules with the requirement of 'actual knowledge' as mandated under section 79(3)(b) of the IT Act, bringing clarity and precision.

3. Periodic Review Mechanism:

- All intimations issued under Rule 3(1)(d) will be subject to a monthly review by an officer not below the rank of Secretary of the Appropriate Government.
- This ensures that such actions remain necessary, proportionate, and consistent with law.

4. Balance of Rights and Responsibilities:

- The amendments strike a balance between the constitutional rights of citizens and the legitimate regulatory powers of the State, ensuring that enforcement actions are transparent and do not lead to arbitrary restrictions.

5. Expected Impact

- Transparency & Accountability: Clear guidelines on who can issue directions and how, with periodic review, ensures checks and balances.
- Clarity for Intermediaries: By mandating detailed and reasoned intimations, intermediaries will have better guidance to act in compliance with law.
- Safeguards and Proportionality: The reforms ensure proportionality and uphold the principles of natural justice while reinforcing lawful restrictions under the IT Act, 2000.

Requirement of Industry Alignment towards Goals and Proposed Structure of DIA:

One shall always remember one of powerful legal maxim "*Ignorantia Juris Non Excusat*", which means ignorance of law is not an excuse. Hence, one should stay prepared before the proposed DIA is notified. It is to be noted that separate rules will govern different kinds of industry. Hence ***Industry Specific Compliance Calendars*** will be required. Although pursuant to notification of DIA, a detailed proposal on the requirements under DIA along with strategy and pedology on compliance calendars shall follow.

Challenges Ahead in the Implementation of DIA, 2023[38]

- **Burdensome Compliance Requirements**: The act's regulations may place a significant burden on businesses, particularly small and medium-sized enterprises (SMEs).
- **Freedom of Expression**: The review of the "safe harbor" principle for online platforms could potentially impact freedom of expression. Ensuring that the act doesn't curb this fundamental right is a delicate task.
- **Resource and Infrastructure Requirements**: Effective enforcement of the DIA will require substantial resources, expertise, and infrastructure. Investing in these areas will be crucial.
- **Stakeholder Interests**: Balancing the interests of various stakeholders, including tech giants and citizens' rights, poses a significant challenge. Ensuring that all voices are heard and considered in the implementation process is essential.
- **Surveillance and Privacy Concerns**: Critics argue that certain provisions of the act may grant excessive

38. Reproduced from India's Digital Future: The Digital India Act 2023, Drishti IAS, 2023

surveillance powers to the government, potentially compromising privacy rights. Robust safeguards should be incorporated to protect against abuse of power and violations of privacy.

- **Data Localization and Cross-Border Data Flows**: The act's approach to data localization is a point of contention. While localization can enhance data protection and security, it may also disrupt cross-border data flows, impacting global businesses that rely on efficient data transfers.

Way Forward for Effective Implementation of DIA, 2023[39]

- Stakeholder Engagement: All relevant stakeholders, including government bodies, technology companies, legal experts, and civil society, should be involved in the drafting and implementation process. This will help create a balanced and comprehensive legal framework.
- Balancing Regulation and Innovation: Stricter regulations, particularly in emerging technologies, could inadvertently stifle entrepreneurial initiatives and deter foreign investments. Striking the right balance between regulation and innovation is critical.
- Collaboration and Capacity Building: Invest in building the capacity of law enforcement agencies, judiciary, and regulatory bodies to effectively enforce the DIA.
- Collaborate with other countries and international organizations to align the DIA with global best practices and standards in the digital space.
- Public Awareness: Conduct public awareness campaigns to educate citizens about their rights and responsibilities in the digital realm, fostering a culture of digital literacy.

Way Forward[40]

The intention behind the DIA is laudable and this legislation will be revamping India's technology sector regulations. It is for the first time that consultations are taking place during the pre-draft stage of the bill. Policymakers are aware of the challenges that might arise therefore the opinions of important stakeholders are being valued. The need for comprehensive and relevant legislation was much needed for the evolving technology sector in India.

While the DIA will promote the growth of India's digital economy, and address the challenges which new-age technologies bring with them like data privacy and cyber security. However, doing away with the safe harbour principle will be criticized by Bigtechs. Additionally, it will require specialists and developed infrastructure for law enforcement, tackling the uncertainties of new-age technologies, AI, deep fakes, and dispute resolution in the proposed legislation. Defining territorial jurisdiction is necessary due to the borderless nature of information and interactions over the Internet. While transparency and accountability are the founding pillars of the act it will also have to balance the interests of important stakeholders like users, big techs, government, businesses, and civil society.

Undoubtedly, it will be one of the most landmark legislations in the jurisprudence of the country as it will protect the freedom of expression and the fundamental rights of citizens on social media platforms. Along with enhancing privacy, online safety, and security, it will also safeguard citizen's data. It will foster innovation and growth of new-age technologies which will be beneficial in education, health, and administration. It will be interesting to see how building this proposed legislation plays out in the coming future.

39. Reproduced from India's Digital Future: The Digital India Act 2023, Drishti IAS, 2023

40. Reproduced from Sanhita Chaurita (8th August 2023) Explained: The Digital India Act 2023, Vidhi Centre For Legal Policy

COMPANIES ACT, 2013

The Companies Act, 2013 is a legislation which regulates the framework of companies right from incorporation of companies, registration, responsibilities, directors, dissolution of company, etc. This Act enshrines in law all the techno-legal requirements that need to be met by a company operating in India. As part of the Companies Act 2013, the Serious Fraud Investigation Office (for brevity, 'SFIO') is entrusted with powers to investigate and prosecute serious frauds committed by Indian companies and their directors.

As a result of the 2014 notification of the Companies Inspection, Investment, and Inquiry Rules, the SFIOs have become even more proactive and serious in regard to this. By ensuring proper coverage of all the regulatory compliances, the legislature ensured that every aspect of cyber forensics, e-discovery, and cybersecurity diligence is adequately covered. Moreover, the Companies (Management and Administration) Rules, 2014 prescribe a strict set of guidelines that confirm the cybersecurity obligations and responsibilities of corporate directors and senior management.

INDIAN PENAL CODE, 1860

If the IT Act is not sufficient to cover specific cyber-crimes, law enforcement agencies can apply the following sections of the Indian Penal Code, 1860 (hereinafter referred to as 'IPC'):

- Section 292 and Section 293: Section 292 and 293 of IPC prohibit publication and sale of obscene books, pamphlets, paper, writing, drawing, painting, etc. which shall be deemed to be 'lascivious or appeals to the prurient interests', which can include obscene advertisements. The purpose of this section was to address the sale of obscene materials, however, in this digital age, it has evolved to deal with various cybercrimes as well. Both these provisions also regulate the manner in which obscene material or sexually explicit acts or exploits of children are published or transmitted electronically. The penalty for such acts is imprisonment up to 2 years and fine up to Rs. 2000, respectively. The punishment for any of the above crimes may be up to five years of imprisonment and a fine of up to Rs. 5000 for repeat (second-time) offenders.
- Section 354C: In this provision, cybercrime is defined as taking or publishing pictures of a woman engaging in a private act without her consent. In this section, voyeurism is discussed exclusively since it includes watching a woman's sexual actions as a crime. In the absence of the essential elements of this section, Section 292 of the IPC and Section 66E of the IT Act are broad enough to include offences of an equivalent nature. Depending on the offence, first-time offenders can face up to 3 years in prison, and second-time offenders can serve up to 7 years in prison.
- Section 354D: Stalking, including physical and cyber stalking, is described and punished in this section. As per this section, the act of any man following and contacting a woman to foster personal interaction despite indication of disinterest or monitoring the use by a woman of the internet, email or any other form of electronic communication amounts to the offence of stalking. This offence is punished by imprisonment of up to 3 years for the first offence and up to 5 years for the second offence, along with a fine in both cases.

In the case of *Kalandi Charan Lenka vs. the State of Odisha (2017)* before the Orissa High Court, the victim received a series of obscene messages from an unknown number. The accused also sent emails to the victim and created a fake account on Facebook containing morphed and offensive images of her. The Orissa High Court, therefore, found the accused prima facie guilty of cyberstalking on various charges under the IT Act and Section 354D of IPC.

- Section 379: Under this section, the offence of theft entails punishment, i.e. imprisonment for up to

three years in addition to the fine. This section may come into play in part because many cyber-crimes involve stolen electronic devices like computers, laptops and mobile phones.

- Section 420: This section talks about cheating and dishonestly inducing delivery of property. Seven-year imprisonment in addition to a fine is imposed under this section which may come into play when cybercriminals commit illegal acts like creating fake websites and cyber frauds.
- Section 463: This section involves falsifying documents or records electronically. Spoofing emails is punishable by up to 7 years in prison and/or a fine under this section.
- Section 465: This provision typically deals with the punishment for forgery. Under this section, offences such as the spoofing of email and the preparation of false documents in cyberspace maybe indirectly covered and punished with imprisonment ranging up to two years, or fine or both. In *Anil Kumar Srivastava vs. Addl Director, MHFW (2005),* the accused had forged the signature of the AD and then filed a case that made false allegations against the AD. Since the accused attempted to pass the forged document off as a genuine document, the Court held that the accused was liable under Sections 465 and 471 of the IPC.
- Section 468: Fraud committed with the intention of cheating may result in a seven-year imprisonment and a fine. Email spoofing may be covered within this section.

Furthermore, there are many more sections of the IT Act and the Indian Penal Code, which pertain to cyber-crimes, in addition to the provisions listed above.

Even though there are laws against cyber-crime in place, the rate of cyber-crime is still rising drastically. It has been reported that cyber-crime in India increased by 11.8% in the year 2020, which accounted for reporting around only 50,000 cases. Cyber-crime is one of the toughest crimes for the Police to solve due to many challenges they face including underreporting, the jurisdiction of crime, public unawareness and the increasing costs of investigation due to technology.

Certain offences may end up being bailable under the IPC but not under the IT Act and vice versa or maybe compoundable under the IPC but not under the IT Act and vice versa due to the overlap between the provisions of the IPC and the IT Act. For example, if the conduct involves hacking or data theft, offences under sections 43 and 66 of the IT Act are bailable and compoundable, whereas offences under Section 378 of the IPC are not bailable and offences under Section 425 of the IPC are not compoundable. Additionally, if the offence is the receipt of stolen property, the offence under section 66B of the IT Act is bailable while the offence under Section 411 of the IPC is not. In the same manner, in respect of the offence of identity theft and cheating by personation, the offences are compoundable and bailable under sections 66C and 66D of the IT Act, whereas the offences under Sections 463, 465, and 468 of the IPC are not compoundable and the offences under sections 468 and 420 of the IPC are not bailable.

In *Gagan Harsh Sharma vs. State of Maharashtra (2018),* the Bombay High Court addressed the issue of non-bailable and non-compoundable offences under sections 408 and 420 of the IPC in conflict with those under Sections 43, 65, and 66 of the IT Act that are bailable and compoundable.

Criminal Law is proposed to be replaced from New Legislations

The three new criminal laws that were passed by Parliament in 2023 will come into effect from July 1, 2024, according to a notification by the Ministry of Home Affairs (MHA).[41]

41. Reproduced from The Hindu, Three Criminal Laws to be effective from July 01, 2024. Available at https://www.thehindu.com/news/national/three-newly-enacted-criminal-laws-to-come-into-effect-from-july-1/article67881602.ece

Hon'ble Union Minister of Home Affairs in a conference said that India has abolished the 150-year-old original laws of criminal justice and introduced new laws. He said that two of the major issues in these three laws are related to this conference. First, to deliver timely justice and second, to curb crimes by increasing conviction rate. He said that in all three laws, efforts are being made to take both these issues forward with the help of technology. Home Minister added that we have taken a bold decision and it has been made mandatory for a Forensic Science Officer to visit the crime scene of offences which have punishment of 7 years or more. He said that this will simplify the investigation, it will be easier for the judges and it will also make the prosecution simple. This will also help us in increasing the conviction rate. Along with this, efforts are also being made to modernize the entire process. Hon'ble Minister further said that after 5 years, India's criminal justice system will be the most modern system in the world.[42]

It is to be noted that Section 106(2) of the Bharatiya Nyaya Sanhita (BNS), which provides for punishment of "0-10 years" in "hit and run" cases, has been put on hold. Earlier this year, transporters and drivers across the country struck work to protest the particular provision.

The Bharatiya Nyaya Sanhita, Bharatiya Nagrik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam that will replace the Indian Penal Code, 1860; Code of Criminal Procedure, 1898; and the Indian Evidence Act, 1872, respectively, received President Droupadi Murmu's assent on December 25, 2023.

CYBER SECURITY FRAMEWORK (NCFS)

As the most credible global certification body, the National Institute of Standards and Technology (NIST) has approved the Cybersecurity Framework (NCFS) as a framework for harmonizing the cybersecurity approach. To manage cyber-related risks responsibly, the NIST Cybersecurity Framework includes guidelines, standards, and best practices. According to this framework, flexibility and affordability are of prime importance. Moreover, it aims at fostering resilience and protecting critical infrastructure by implementing the following measures:

- A better understanding, management, and reduction of the risks associated with cybersecurity.
- Prevent data loss, misuse, and restoration costs.
- Determine the most critical activities and operations that must be secured.
- Provides evidence of the trustworthiness of organizations that protect critical assets.
- Optimize the cybersecurity 'Return on Investment' (ROI) by prioritizing investments.
- Responds to regulatory and contractual requirements.
- Assists in the wider information security program.
- Using the NIST CSF framework in conjunction with ISO/IEC 27001 simplifies the process of managing cybersecurity risk. Moreover, NIST's cybersecurity directive also allows for easier collaboration in the organization as well as across the supply chain, allowing for more effective communication.

DATA PROTECTION AND AI: LAWS AND REGULATIONS

In 2019, in a two-day G-20 summit in Osaka in Japan, the Prime Minister of India underscored the significance of Digital Economy & Artificial Intelligence. He emphasized the government's reliance on the 5 'I's that stand for ***Inclusiveness, Indigenization, Innovation, Investment in infrastructure & International*** cooperation in developing these two areas. The concept of Artificial Intelligence is based on the idea of building machines capable of thinking, acting, and learning like humans.

42. Brief from Union Home Minister and Minister of Cooperation Shri Amit Shah address on the 5th International and 44th All India Criminology Conference of National Forensic Science University (NFSU) in Gandhinagar, Gujarat, Press Information Bureau of India. https://pib.gov.in/PressReleasePage.aspx?PRID=1998860

Artificial Intelligence: Brief Description

- It describes the action of machines accomplishing tasks that have historically required human intelligence.
- It includes technologies like machine learning, pattern recognition, big data, neural networks, self-algorithms etc.
- The origin of the concept can be traced back to the Greek mythology, although it is only during modern history when stored program electronic computers were developed.
- Example: Millions of algorithms and codes are there around the humans to understand their commands and perform human-like tasks. Facebook's list of suggested friends for its users, a pop-up page, telling about an upcoming sale of the favourite brand of shoes and clothes that comes on screen while browsing the internet are the work of artificial intelligence.
- A Complex Technology: AI involves complex things such as feeding a particular data into the machine and making it react as per the different situations. It is basically about creating self-learning patterns where the machine can give answers to the never answered questions like a human would ever do.

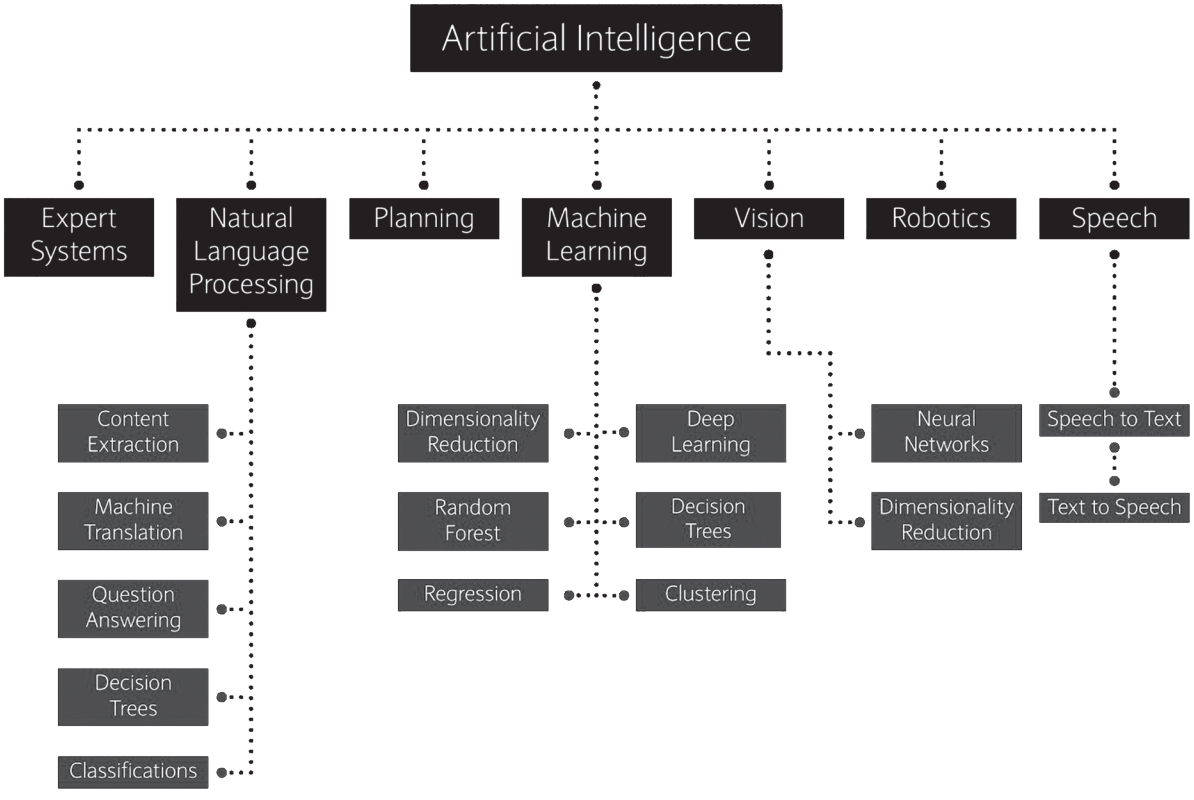
AI is a Different Technology

- AI is different from hardware driven robotic automation. Instead of automating manual tasks, AI performs frequent high volume computerized tasks reliably.
- AI is often misunderstood for machine learning. AI is a broader concept with a bunch of technologies that include machine learning and other technologies like natural language processing, inference algorithms, neutron networks etc.

Evolution

- In the year 1956, American computer scientist John McCarthy organised the Dartmouth Conference, at which the term 'Artificial Intelligence' was first adopted. From then on, the world discovered the ideas of the ability of machines to look at social problems using knowledge data and competition.
- There used to be several dedicated projects on the same and the government was funding the research.
- Every aspect of science and especially when one starts looking at empowering machines to behave and act like human beings, the questions of ethics arise. About 70's and late 80's, there was a time when the governments stopped funding research into AI.
- AI experienced a resurgence following concurrent advances in computer power and large amounts of data and theoretical understanding in the 21st century.
- AI techniques now have become an essential part of the technology industry helping to solve many challenging problems in computer-science. From Apple SIRI to self-driving cars, AI is progressing rapidly.

AI Methods



Source: https://www.drishtiias.com/

India and AI

- According to the Global AI Report 2019 (i.e. a Canada based company's report), India stood at the ninth position in terms of the number of the AI specialists working in the field, while the US, China and the UK topped the list.
- The top ranked countries in this Report have many academic institutes with programs on AI. They have therefore a much greater number of people skilled to do research in the field.
- India, on the contrary, lacks the opportunities in formal education in data science but is slowly trying to encourage the adoption of AI in educational institutes.
- Starting this year, the CBSE has AI as an elective subject for its ninth grade classes.
- The International Institute of Information Technology, Hyderabad (for brevity, 'IIT Hyderabad') has launched a full-fledged Bachelor of Technology (B Tech) program in AI becoming the first Indian educational institution to do so. It is also most likely the third educational institute in the world after Carnegie Mellon University and the Massachusetts Institute of Technology to have a full-fledged B Tech program on AI.
- IIIT Hyderabad is another educational institute that introduced popular executive programs on AI and machine learning and blockchain and distributed ledger technologies.
- Defence forces of India are now venturing into the products and technologies which will aid defence measures using the AI and technologies.

- In India, corporates have started collaborating with academia on AI. IBM's Blue project is an example.
- There are many startups in the country which are doing great work in image analytics, data analytics, predictive intelligence etc.
- It is estimated that AI will add 957 billion dollars to India's GDP by the year 2035 boosting India's annual growth by 1.3% points.

Benefits

- In Policing: India still has a conventional policing. AI based products open a new window of opportunity to do predictive policing in India. With the help of AI, one can predict the pattern of crime, analyze lot of CCTV footage which are available across the country to identify suspects.

> ***Note:*** Policing refers to maintenance of law and order by the police force in a country.

- Government is digitizing all the records, especially the crime records putting it into one single place called CCTNS, i.e. Crime and Criminal Tracking Network & Systems, where all the data including the image, biometrics, or the criminal history of a convict or suspect is available.
- In Agriculture: It has many uses, for example, it can help sense one how much water the crop needs.
- For solving complex issues like efficient utilization of available resources.
- Analyzing the Data: The AI technology helps in analyzing data and thus can improve the efficiency of the systems like power management in cars, mobile devices, weather predictions, video and image analysis.

Steps taken by the Government

- In 2018-19 budget, the government mandated NITI Aayog to establish the National Program on AI with a view to guiding research and development in new and emerging technologies.
- NITI Aayog then adopted a three pronged approach undertaking exploratory proof of concept AI projects in various areas, crafting a national strategy for building a vibrant AI ecosystem in India and collaborating with various experts and stakeholders.
- On 20th March, 2019, NITI Aayog circulated the cabinet note to establish a cloud computing platform called AIRAWAT (Artificial Intelligence Research, Analytics and Knowledge Assimilation Platform).
- The note circulated by NITI Aayog proposes that the government should pump in Rs. 7,500 crore rupees over 3 years as well as set up a high-level task force that will oversee the roll out and implementation of AI.
- The move to create cloud computing platform is part of the government's goal of making India a pioneer amongst emerging economies with regards to AI and transform sectors like education, health, agriculture, urbanization and mobility.
- In Budget 2018, the government announced funds to support the country's AI, machine learning, robotics and IoT sector.
- As part of the initiative, NITI Aayog in the year 2018, published a draft National Strategy for AI, planning its scope for research, adoption and commercialization.
- It envisioned AI use case clearly in the sectors like healthcare, agriculture, education, smart cities and infrastructure, smart mobility and transportation.

- The Ministry of Commerce and Industry has also set up task forces to explore the use of AI and Big Data technologies in the country.
- In the Budget 2019-20, the government has announced setting up of a National Sports Education Board under Khelo India to prepare youth for new age skills, Artificial Intelligence, IoT, Big Data, 3D Printing, Virtual Reality etc.

Data Protection: Indian Legal Perspective

Need of Legal Mechanism

To encounter the challenges of information privacy and to promote legal control over privacy protection in electronic transactions, some legal policies and regulations have already been established at international and national level. At international level, some fair information principles like Notice, Choice, Access, Consent, Enforcement etc. are directed to be followed by the e-commerce companies to ensure the information privacy in the conduct of online transactions. Though at the industry level, even the e-commerce companies are also taking some steps to protect the information privacy of the individuals by adopting and declaring privacy policy, yet much is left to be governed by the nationally and internationally commended regulations.

At national level, countries around the world have enacted different laws to protect privacy of individuals. A Business Week/Harris Poll survey[43] found that over 57% of the online buyers want some legal regulations or law to control the use and disclosure of their information by e-commerce websites and to ensure protection of information privacy. Numerous survey[44] conducted by various researchers (Harris Poll Survey, Georgia Institute of Technology survey, Pew Internet and American life etc.) have discovered the fact that consumers as well as businesses want legal protection to regulate protection of personal data and privacy in the regime of e-commerce transactions.

Enumerations below support the need of legal protection for data privacy in e-commerce transactions:

A. Business Week/Harris Poll survey shows that 86% of their respondents want that online businesses should provide consumers with 'opt-in' and 'opt-out' clauses before collecting their personal and sensitive personal information. This supports the demand for consumers' legal control on personal data collection and further sharing of data.

B. A survey conducted by American Society of Newspaper Editors on privacy concerns (2000)[45] showed that 51% of respondents strongly felt that online companies might violate their personal privacy and same study showed that 52% of the respondents were having 'no confidence at all' in the online company that they use the personal information of their consumers exactly in the same way which they had said they would.

C. Number of surveys conducted by Georgia Institute of Technology's Graphic, Visualization, and Usability (GVU) Center[46] has discovered that a majority of individuals strongly insist upon and support anonymity in electronic transactions.

D. Business Week/Harris Poll (2000)[47] survey found that 89% of their respondents were not comfortable with the online tracking system of online websites and prefer a restriction to be imposed on the web tracking especially in the tracking of their personal information.

43. Harris Poll, Privacy and American Business Press Release (online). (June 24, 2012), http://www.epic.org/privacy/survey/.

44. Harris Poll, Online Privacy: A Growing Threat, Business Week, 96 (2000). (June 22, 2012), http://epic.org/privacy/survey/.

45. See, Public Opinion on Privacy, Supra note 181.

46. Survey Report. (June 22, 2012), http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-04/graphs/#privacy.

47. Public Opinion on Privacy, Supra note 181.

E. Pew Internet and American Life Project[48] (2000) found in their studies that 54% of internet users were objecting to online tracking and they were afraid of the creation of their profile in online transactions. USA Weekend Poll (2000) also showed that 65% of respondents thought that tracking computer usage and creation of users' profile in internet was an invasion of privacy.

F. Pew Internet and American Life Project study showed that 56% of internet users are unaware and unknown about installation and use of cookies and more sophisticated tracking tools, such as 'web bugs' or 'spyware' by online business to access and collect consumers' personal information and thereafter tracking their online behaviour.

G. Pew and American Life Report[49] (2000 and 2008) showed that 94% of internet users believe that privacy violations should be regulated by the State and they want ability to avail remedies against privacy invasions by online companies.

It can be assumed that adequate legal protection over privacy concern and information privacy will ensure individuals' about the protection of their privacy rights in e-commerce transactions.

Indian Laws for Data Protection

Individual's data like name, telephone numbers, profession, family, choices, pan card number, credit card details, social security number etc. are disclosed in the electronic transactions and then are available on various websites.[50] Though the authorized collection and the storage of data may only create probability of the loss of information privacy[51] but the unauthorized access, collection, use, misuse, relocation and transmission of the information to the third party essentially result in the intrusion of information privacy of the individuals. Hence, improper control on transmission of information can be the root cause for privacy challenges in electronic transactions. Law will not only determine, what privacy entails, how it is to be valued, and to what extent it should be endowed with legal protection, but also ensures authorized protection to the circumstances under which individuals can value their privacy and protect it from the violation of unauthorized intrusion by others.[52] Knight Bruce in *Prince Albert v Strange*[53] upheld that a third party intrusion into one's privacy results in grave violation of right to privacy and hence, implies need of legal protection to right to privacy.

To counter the challenges of information and communication technology, the Indian Legislature has enacted Information Technology Act, 2000, Information Technology (Amendment) Act, 2008 and other legislations too, but challenges of information privacy and data privacy are not addressed in an exclusive and specific manner. India is not having a comprehensive legislative framework to deal specifically with privacy issues in electronic transactions.[54] The Information Technology Act, 2000 was enacted chiefly to facilitate e-commerce; hence privacy is not the primary concern of the Act.[55]

---

48. Public Opinion on Privacy, Supra note 181.

49. Report on Trust and Privacy Online: Why American Want to rewrite the rules, Pew Internet and American Life Project. (June 22, 2012), http://www.pewinternet.org/reports/toc.asp?Report=19.

50. Miriam J. Metzger, Privacy, Trust and Disclosure: Exposing Barriers to Electronic Commerce, Journal of Computer Mediated Communication, Vol. 9 No. 4, (2004). (May 27, 2012), http://jcmc.indiana.edu/vol9/issue4/metzger.html.

51. Information privacy is synonym to data privacy. Information Privacy or data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. (May 27, 2012), http://en.wikipedia.org/wiki/Information_privacy.

52. Ruth Gavison, Privacy and the Limits of Law, The Yale Law Journal, Vol. 89, No. 3, 421-471 (Jan. 1980). (May 28, 2012), http://www.jstor.org/stable/795891?origin=JSTOR-pdfand.

53. Prince Albert v Strange (1848) 2 De G and SM 652, 698; 64 ER 293, 314.

54. Shrikant Ardhapurkar et al., Privacy and Data Protection in Cyberspace in Indian Environment, International Journal of Engineering Science and Technology, Vol. 2, No. 5, 942-951 (2010).

55. Mathur, S. K., Indian Information Technology Industry: Past, Present and Future A Tool for National Development, Journal of Theoretical and Applied Information Technology. (2006) (Online). (May 28, 2012), http://perso.univ-rennes1.fr/eric.darmon/floss/papers/MATHUR.pdf.

Information Technology Act, 2000 and Data Protection

Indian legislature has enacted Information Technology Act, 2000 for the purpose of complying with the requirements of UNCLTRAL (United Nations Commission on International Trade Law) model law[56] on electronic commerce[57] on one hand, and for providing legal recognition to the transactions carried out by the means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce.

The Act was brought into existence for the following reasons:[58]

i. To facilitate the development of e-commerce transactions;

ii. To ensure the regulatory environment for the security of e-commerce transactions;

iii. To provide legal structure for governing electronic contracts, security and integrity of electronic transactions;

iv. To facilitate and validate the use of digital signatures for authenticating the electronic records;

v. To facilitate the growth of Indian IT sector across the globe;

vi. To ensure the safety and security of electronic transactions; and

vii. To attract Foreign Direct Investment (FDI) in Information Technology sector.

Note: E-commerce or electronic commerce is the trading of goods and services over the internet.

Under the regime of privacy rights, every individual wants to keep his or her personal affairs to himself, but in the electronic transactions, variety of individual's information are collected and stored, which can easily enable others to identify that individual. Databases collected in the online transactions, when cross-matched can easily create profile of the individuals and can predict their behaviour. This involves the sheer violation of data privacy in electronic transactions. The provisions of the Act for the purpose of data privacy in electronic transactions can be examined as follows:

A. Provisions pertaining to data[59] protection and personal data[60] protection.

In Information Technology, Act, 2000, no such concept as 'personal data' has been discussed. It defines 'data'[61] but does not provide any definition of personal data. Furthermore, the definition of data

56. UNCITRAL Model Law on Electronic Commerce, Guide to Enactment with 1996 (May 27, 2013), http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

57. The UNCITRAL Model Law on E-commerce is a resolution of the U.N. General Assembly which recommends that all States give favorable consideration to the Model Law on Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information.

58. Nasir, M. Ali, Legal Issues involved in E-commerce, Ubiquity (Mazgine), New York, NY, USA (2004). (May 28, 2012), http://ubiquity.acm.org/article.cfm?id=985607.

59. Data means information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by Section 68, or(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d). Source: Information Commission Office, Government of United Kingdom. (May 29, 2012), http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx.

60. Personal data means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and (c) includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Source: Information Commission Office, Government of United Kingdom. (May 29, 2012), http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx.

61. Section 2 (o) of IT Act, 2000 'data' means a representation of information, knowledge, facts, concepts or instructions which are being

is provided with more relevancy to cybercrime.[62] Hence, there is confusion among the researchers whether the Indian IT Act, 2000 deals with 'data protection' or with 'personal data protection' as well.

B. Civil Liability in case of data, computer database theft, privacy violation etc.[63]

The Act has devoted Section 43 (a) to 43 (h) to enlist wide range of cyber contraventions related to unauthorized access to computer, computer system, computer network and resources. Section 43 of the Act[64] covers various issues, which create civil liability against the wrongdoer and provides for damages (not exceeding one crore rupees) to the person so affected from the defined instances.

These instances include:

i. Computer trespass, violation of privacy etc.

ii. Digital copying, downloading and extraction of data, computer database or information; theft of data held or stored in any media,

iii. Data contamination, computer disruption etc.,

iv. Data loss, data corruption etc.,

v. Computer data/database disruption, spamming etc.,

vi. Denial of service attacks, data theft, fraud, forgery etc.

C. Criminal Liability in case of data, computer database theft, privacy violation etc.[65]

The Act also provides (vide Chapter XI) for defining and creating liability for cyber offences. Sections 65 to 74 of the Act cover a wide range of cyber offences related to unauthorized alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, and computer database. Some provisions deal with the data related offences, like Section-65 related to 'Tampering with the computer source' which was not limited to the protection of computer source code but was extending safeguards for computer data base from unauthorized access. Section 66 (Hacking with computer system), was also indirectly protecting data from unauthorized access and misuse. According to Dr. Unni, unauthorized access to any information diminishes its value/utility and hence injures the confidentiality of a document.[66] For example, if any sensitive personal information is transmitted over e-mail or saved in an e-mail, or in computer and if any person accesses the said document without any authority, then the value of the information is completely lost and it will result in loss of personal data and will make the accessing party liable under Section 66.

D. It is noteworthy that to make a person liable under Section 66, his guilty intention to cause such access has to be proved. Further, out of various provisions dealing with cyber offences, it is only Section 72[67]

---

prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. (May 29, 2012), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

62. The Final Report: The First Analysis of the Personal Data Protection Law in India, Prepared by CRID-University of Namur, Report delivered in the framework of contract, JLS/C4/2005/15 between CRID and the Directorate General, Justice, Freedom and Security. (May 29, 2012), http://ec.europa.eu/justice/data-protection/index_en.htm.

63. Sharma, Vakul, Information Technology-Law and Practice, Delhi: Universal Law Publishing Co. Pvt. Ltd (2004).

64. Section 43 of Information Technology Act, 2000: Penalty for damage to computer, computer system, etc. (May 29, 2012), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

65. Sharma, Vakul, Supra note 334.

66. V.K. Unni, Internet Service Provider's Liability for Copyright Infringement-How to clear the Misty Indian Perspective, Richmond Journal of Law and Technology. Vol. 13 (2001). (May 29, 2012), http://jolt.richmond.edu/v8i2/article1.html.

67. Section 72 of Information Technology Act, 2000: Penalty for breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations

of the Act, which is specifically directed at the protection of confidentiality and privacy. Section 72 aimed at the protection of privacy and confidentiality from public (and private) authorities,[68] which have been granted power under the provisions of Information Technology Act, 2000 to secure access to any electronic record, book, register, correspondence, information, document or other material information. The purpose of incorporating this section was to ensure that the person who is legally entitled to secure an access to any information[69] shall not take unfair and unmerited advantage of such information by disclosing it to any unauthorized third party without seeking due consent. This section creates an obligation of confidence between the 'data collectors' and 'data subject'. Section 72 has a limited application, as it is applicable only to the persons who have gained access to the information under some authorized channel and not to the unauthorized access of personal information by available means.[70]

From the above discussion, it can be submitted that Information Technology Act, 2000 is not a data protection legislation per se. The Act does not lay down any specific provisions for data protection and privacy protection. The IT Act, 2000 is a general legislation, which articulates on various subject matters that involves digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offences and confidentiality and privacy. Therefore, the sphere of data protection and privacy in electronic transactions was largely unregulated, which led to amendments in information technology laws in the year 2008.

The Information Technology (Amendment) Act, 2008

The Information Technology (Amendment) Act, 2008 has been enacted to facilitate and legalize e-commerce transactions, e-fund transfers, e-storage of data, e-filling of documents with the Government departments on one side and to increase the protection of personal data and information for national security, countries' economy, public health and safety on the other.[71] Section 43A of this Act directs that all body corporates,[72] which are in possession of data and information of their consumers in their computer source, will implement 'reasonable security practices[73]' to prevent the unauthorized access to the personal data of their consumers. This section further entails that failure to protect the sensitive personal data of the individuals during the processing period by the company will make company liable to compensate the aggrieved person, whose personal data is so compromised. While explaining Section 43A of IT (Amendment Act), 2008, Kamlesh Bajaj[74] has detailed that

made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. (May 29, 2012), http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf.

68. These public and private authorities may be referred as 'data collectors' or 'data users'.

69. Persons conferred under the Act : The Act has conferred powers to : a)The Controller of Certifying Authorities (Ss. 17-18) b) The Deputy and Assistant Controllers of Certifying Authorities (Ss. 17 and 27) c)Licensed Certifying Authorities (S. 31) and Auditors (Rule 312) d) The Adjudicating Officer (S 46) e) The Presiding Officer of the Cyber Appellate Tribunal (Ss. 48-49) f) The Registrar of the cyber Appellate tribunal (S. 56 and rule 263) g)Network Service provider (S. 79) h) Police Officer (Deputy Superintendent of Police) (S. 80). (May 29, 2012), http://www.legalserviceindia.com/article/l288-Breach-of-privacy-and-Confidentiality-.html.

70. Salim Nimitha, Breach of Privacy and Confidentiality under the Information Technology Act, 2000, Legal Service India, (2009). (May 29, 2012), http://www.legalserviceindia.com/article/l288-Breach-of-privacy-and-Confidentiality-.html.

71. Workshop Report, National Seminar on Enforcement of Cyber law, New Delhi, (May 8, 2010). (May 27, 2012) http://catindia.gov.in/pdfFiles/IT_Act_2000_vs_2008.pdf.

72. Section 43 A, Explanation (i) 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

73. Section 43 A, Explanation (ii) 'reasonable security practices and procedures' means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

74. CEO of Data Security Council of India, 2009.

the company will be liable for the loss of data during its processing at company's end and the company cannot seek exemption from their responsibility on the ground that there was no negligence on the part of the company in implementing or maintaining reasonable security practices. He further explained that reasonable security practices and procedure will constitute practices and procedures to protect information from unauthorized access, damage, use, modification, disclosure or impairment as may be specified in an agreement between the parties or as may be specified in any law in force.

The penalty under Section 72 of IT Act, 2000 for the disclosure of information was restricted only to those who are legally authorized to secure access to an electronic record and document under the Act, and hence Section 72-A[75] has been incorporated in IT (Amendment) Act, 2008, which provides liabilities of intermediaries and other persons for breach of privacy and confidentiality under lawful contract. Section 72-A[76] reads as, 'save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract; has secured access to any material containing personal information about another person; with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain; discloses; without the consent of the person concerned, or in breach of a lawful contract; such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. Apart from Sections 43A and 72A, there are some other provisions as well which though not specifically but in one way or other tackle the challenges of data protection and data privacy.

The provisions are:

A. Section 66 – Computer Related Offences.

B. Section 66A – Punishment for sending offensive messages through communication service, etc.

C. Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device.

D. Section 66C – Punishment for identity theft.

E. Section 66D – Punishment for cheating by personation by using computer resource.

F. Section 66E – Punishment for violation of privacy.

G. Section 66F – Punishment for cyber terrorism.

H. Section 67 – Punishment for publishing or transmitting obscene material in electronic form.

I. Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.

J. Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

K. Section 67C – Preservation and Retention of information by intermediaries.

L. Section 69 – Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

M. Section 69A – Power to issue directions for blocking for public access of any information through any computer resource.

N. Section 69B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

O. Section 79 – Exemption from liability of intermediary in certain cases.

75. Penalty for breach of confidentiality and privacy.

76. Section 72A: Punishment for disclosure of information in breach of lawful contract.

P. Section 84A –Modes or methods for encryption.

Q. Section 84B –Punishment for abetment of offences.

R. Section 84C –Punishment for attempt to commit offences.

Personal Data Protection Bill, 2019 - Key Highlights

The Government of India had introduced the Personal Data Protection Bill 2019 (hereinafter referred to as 'PDP Bill') in the Lok Sabha on 11 December 2019. The "Bill" was referred for examination and recommendations to a Joint Committee of both Houses of Parliament (called JPC) on 12 December 2019. JPC received more than 200 representations including that of Dua Associates / Dua Consulting. Around eight members had submitted their written dissent on the said Bill.

The Joint Parliamentary Committee chaired by Member of Parliament, Shri P.P. Chaudhary tabled the report on the Bill along with the amended Bill before both Houses of Parliament on 16th of December 2021. The Committee deliberated for over two years, during which time that Bill underwent substantial changes in scope and nature. A total of 188 amendments have been recommended out of which 91 amendments are of significant nature, while the rest are editing of legal nature in different sections.

Salient features of the "Bill" introduced on 11th December, 2019:

The "PDP Bill 2019" which defines both personal and non-personal data, is a substantive framework which introduces a specialized regulatory approach for the Protection and Privacy of Data in any form (digital or non-digital) in India. The proposed legal framework would be applicable to processing, storage and transfer of any form of personal data across sectors of the economy, academia, industry and the society. The Bill has limited provisions relating to Non Personal Data (NPD).

The framework is on the lines and pattern of General Data Protection Regulations (GDPR) of European Union. Some of the provisions of the "Bill" also reflect the directions followed in the California Privacy Act.

The framework classifies data into 3 broad categories namely:

- Personal Data
- Sensitive Personal Data (SPD)
- Critical Sensitive Personal Data

The nature of sensitive personal data has been defined in the legal terms. The entities across different sectors and individuals will be required to follow its provisions while processing, storing and transmitting data in the domestic territory and in cross-border exchange too. The provisions provide for special conditions to process biometric data.

The consent of the user with respect to collecting, and usage of his/her "data" is the underlying feature of the framework. A framework for consent mechanism is proposed. The Bill also has provisions relating to ground for processing of data without consent.

The Bill provides for the rights of the Data Principal including right of data portability. There are special requirements in the Bill for processing of personal and sensitive data related to children.

The framework would regulate 'data localisation' particularly 'sensitive personal data' and 'critical sensitive data'. Consent of the user and approval of the Regulator would be essential for cross border transfer of Personal Data.

Any breach of sensitive personal data and critical sensitive data will attract heavy fine and compensation to the Data Principal (the owner of such data).

The Data Protection framework proposes to set up an elaborate regulatory mechanism consisting of a Regulatory Authority namely Data Protection Authority (DPA) Adjudication and Appellate Tribunal to regulate process storage and flow of data in the country. All entities would be obligated to appoint a Data Protection Officer who will have responsibility of enforcement and supervision of privacy policy and reporting of data breach to the concerned authorities.

India's Digital Personal Data Protection Act, 2023: Key Provisions[77]

Initially introduced in 2019, the Digital Personal Data Protection Act holds considerable importance as a legislative measure aimed at safeguarding individuals' privacy rights. Its primary focus lies in regulating the collection, storage, processing, and transfer of personal data in the digital landscape. The DPDP Bill underwent 81 amendments after its initial introduction, resulting in a comprehensive overhaul to its present form.

By prioritizing privacy and security, the DPDP Act strives to create a robust framework that addresses the challenges posed by data handling in the digital age. Key provisions of the DPDP Act, 2023 are as follows:

Definitions: Although many concepts in the DPDP Act closely resemble those found in the EU's General Data Protection Regulation (GDPR), framework, there are differences in how terminology is used.

(a) **Data fiduciary**: This refers to the entity that, either independently or in collaboration with others, establishes both the purpose and the methods for processing personal data (similar to a data controller). The government can classify any data fiduciary or a specific group of data fiduciaries as 'significant data fiduciaries' (SDFs). The criteria for this classification as an SDF include he nature of processing activities (such as the volume and sensitivity of personal data involved and the potential impact on data principals' rights) to broader societal and national concerns (such as the potential effects on India's sovereignty and integrity, electoral democracy, state security, and public order). The designation of SDF comes with heightened compliance obligations as explained below.

(b) **Data processor**: This is an entity responsible for processing digital personal data on behalf of a data fiduciary.

(c) **Data principal**: These are individuals whose personal data is gathered and processed (equivalent to a data subject).

(d) **Consent manager**: A person registered with the Data Protection Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw their consent through an accessible, transparent, and interoperable platform.

Applicability: The DPDP Act applies to all data, whether originally online or offline and later digitized, in India. Additionally, the Act applies to the processing of digital personal data beyond India's borders, particularly when it encompasses the provision of goods or services to individuals within the Indian territory.

Age verification mechanisms will be necessary for all companies in India (telcos, banks, e-commerce, etc.) under the new DPDP law, per reporting from The Economic Times. The compliance requirement is not just limited to social media platforms. This is essential to record the verifiable consent of users per legal experts

Personal data breach: This means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity, or availability of personal data.

Individual consent to use data and data principal rights: Under the new legislation, personal data will be

77. Reproduced from Khyati Anand and Melissa Cyrill (September 18, 2023), India's Digital Personal Data Protection Act, 2023: Data Privacy Compliance India Briefing. Available at https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html/

included and processed only with explicit consent from the individual, unless specific circumstances pertaining to national security, law, and order require otherwise. Under data principal rights, individuals also have the right to information, right to correction and erasure, right to grievance redressal, and right to nominate any other person to exercise these rights in the event of the individual's death or incapacity. Currently, there is no specified timeline for the implementation of grievance redressal and data principal rights.

Additional obligations of SDFs: Depending on the quantity and sensitivity of the data they manage—data fiduciaries deemed as SDF are subject to additional obligations under the DPDP Act. Every significant data fiduciary is required to appoint a Data Protection Officer (DPO) responsible for addressing the inquiries and concerns of data principals—those individuals whose data is collected and processed. Regarding international data transfers, the DPDP Act permits data fiduciaries to transfer personal data for processing to any country or territory outside India. However, the central government can impose restrictions through notifications. These restrictions will be determined after assessing relevant factors and establishing necessary terms and conditions to ensure the maintenance of data protection standards during international processing.

Establishment of a Data Protection Board: The Data Protection Board will function as an impartial adjudicatory body responsible for resolving privacy-related grievances and disputes between relevant parties. As an independent regulator, it will possess the authority to ascertain instances of non-compliance with the Act's provisions and impose penalties accordingly. The appointment of the chief executive and board members of the Data Protection Board will be carried out by the central government, ensuring a fair and transparent selection process. To provide an avenue for customers to challenge decisions made by the Data Protection Board, the government will establish an appellate body. This appellate body may be assigned to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), which will be responsible for adjudicating disputes related to data protection and hearing appeals against the decisions made by the Data Protection Board.

Voluntary undertaking: Under this provision, the Data Protection Board has the authority to accept a voluntary commitment related to compliance with the DPDP Act's provisions from any data fiduciary at any stage of complaint proceedings. This voluntary undertaking may entail specific actions to be taken or refrained from by the concerned party. Furthermore, the terms of the voluntary undertaking can be modified by the Board if necessary. The voluntary undertaking serves as a legal barrier to proceedings concerning the subject matter of the commitment, unless the data fiduciary fails to adhere to its terms. In the event of non-compliance, such a breach is considered a violation of the DPDP Act, and the Board is authorized to impose penalties for this infringement. Additionally, the Board has the discretion to require the undertaking to be made public.

Alternate disclosure mechanism: This mechanism will allow two parties to settle their complaints with the help of a mediator.

Offence and penalties: Data fiduciaries can face penalties of up to INR 2.5 billion for failing to comply with the provisions. These include: penalties of up to INR 10,000 for breach of the duty towards data principals; penalty up to INR 2.5 billion for failing to take reasonable security safeguards to prevent breach of personal data; fines up to INR 2 billion for failure to notify the Data Protection Board and affected data principals in case of a personal data breach; penalties of up to INR 2 billion for violation of additional obligations related to children's data; penalty of INR 1.5 billion for failure to comply with additional obligations of significant data fiduciary; penalty of INR 500 million for breach of any other provision of the DPDP Act, 2023 and rules made thereunder.

Conflict with existing laws: The provisions of the DPDP Act will be in addition to and not supersede any other law currently in effect. However, in case of any conflict between a provision of this Act and a provision of any other law currently in effect, the provision of this Act shall take precedence to the extent of such conflict.

Exemptions under the DPDP Act

The exemptions provided in the DPDP Act are as follows:

- For notified agencies, in the interest of security, sovereignty, public order, etc.
- For research, archiving, or statistical purposes.
- For start-ups or other notified categories of data fiduciaries.
- To enforce legal rights and claims.
- To perform judicial or regulatory functions.
- To prevent, detect, investigate, or prosecute offences.
- To process in India personal data of non-residents under foreign contract.
- For approved merger, demerger, etc.
- To locate defaulters and their financial assets etc.

Steps for companies prepare for compliance under the Digital Personal Data Protection Act

By following the below steps, companies can prepare for compliance with India's DPDP Act and protect personal data in line with regulatory guidelines.

Assess and build data privacy:

- Evaluate current compliance status.
- Create a phased action plan covering governance, technology, people, and processes.
- Establish a privacy organization with defined roles, including the DPO, especially if your entity's status is an SDF.

Inventory personal data systems:

- Identify critical data storage and processing systems.

Identify data processors:

- List third parties handling personal data.
- Update agreements and communicate responsibilities.

Draft DPDP Act-compliant documents:

- Create approved data privacy policies and processes.
- Update necessary documents.
- Develop privacy notices, consent forms, and standard contract clauses.

Design consent mechanisms:

- Define consent types.
- Develop user-friendly consent processes.
- Implement efficient consent management tools.

Establish data principal rights handling:

- Set up processes for addressing data principal rights.
- Develop procedures for request handling.

- Use tools for efficient rights management.

Implement data breach response:

- Create breach management processes.
- Integrate with incident management.

Define data retention periods:

- Categorize data and align retention periods with requirements.

Evaluate and implement privacy technologies:

- Choose suitable tech solutions.
- Assess compatibility and scalability.
- Implement chosen solutions.

Conduct communication and awareness programs:

- Develop plans and materials.
- Launch awareness initiatives.
- Provide training to stakeholders.

Monitor government notifications:

- Stay updated on Central Government notifications and any forthcoming rules under the Act.
- Take necessary actions based on government directives.

Global Data Protection Models

European Union (EU) model: The EU's GDPR imposes stringent requirements on organizations to ensure the careful safeguarding of personal data and demands evidence of such protection. The regulation establishes rigorous standards for obtaining consent, empowering customers to exercise control over how their data is handled and protected. Widely acknowledged as a ground-breaking and crucial legislative framework, the GDPR offers valuable guidance to countries in defining the fundamental rights and responsibilities that should be integrated into their own data protection laws. Its primary objective is to effectively respond to the challenges posed by our increasingly digital and interconnected world.

United States (US) model: The US model emphasizes safeguarding an individual's personal privacy from government intrusion. It permits the collection of personal information, provided that the individual is made aware of such data collection and its intended use. Unlike some other countries, the US does not have a singular data protection regulation; instead, it has a combination of laws at both the federal and state levels that are designed to protect the data of its residents.

China model: The Personal Information Protection Law (PIPL) introduces enhanced rights for data principals in China, aiming to curb the improper usage of personal data. The law encompasses key notions, such as personal information, sensitive personal information, and processing. Notably, it explicitly defines its jurisdiction beyond national borders. The PIPL incorporates fundamental elements of data protection, including principles governing the processing of personal information, provisions for consent and non-consent-based grounds for processing, mechanisms for cross-border data transfers, and the rights of data subjects.

EUROPEAN UNION (PROPOSED) AI ACT, 2024[78]

The Artificial Intelligence Act (AI Act) is a proposed European Union regulation on Artificial Intelligence (AI) in the European Union. It aims to establish a common regulatory and legal framework for AI. Proposed by the European Commission on 21 April 2021 and passed in the European Parliament on 13 March 2024, it awaits reading in the EU Council.

Its scope would encompass all types of AI in a broad range of sectors (exceptions include AI systems used solely for military, national security, research, and non-professional purpose). As a piece of product regulation, it would not confer rights on individuals, but would regulate the providers of AI systems, and entities using AI in a professional context.

The AI Act was revised following the rise in popularity of generative AI systems such as ChatGPT, whose general-purpose capabilities present different stakes and did not fit the defined framework. More restrictive regulations are planned for powerful generative AI systems with systemic impact.

Summary of European Union proposed AI Act

The highly anticipated EU Artificial Intelligence Act is finally here! With extra-territorial reach and wide-reaching ramifications for providers, deployers, and users of Artificial Intelligence ("AI"), the Artificial Intelligence Act ("AI Act") was finally approved by the European Parliament ("EP") on March 13, 2024. The text of the approved version is based on the political agreement that the EP reached with the Council of the European Union in December 2023. Members of the EP passed the law with 523 votes in favor, 46 against, and 49 abstentions. The Act aims to safeguard the use of AI systems within the EU as well as prohibiting certain AI outright.

The AI Act applies to:

- providers placing AI systems or models on the market in the EU or putting into service AI systems or placing on the market general-purpose AI models in the EU, irrespective of whether those providers are located within or outside the EU;
- deployers of AI systems that have their place of establishment in or who are located within the EU;
- providers and deployers of AI systems that have their place of establishment or who are located in a third country in situations where the output produced by the AI system is used in the EU;
- importers and distributors of AI systems into or within the EU;
- product manufacturers who place an AI system on the market or put it into service an AI system within the EU together with their product and under their own name or trademark;
- authorized representatives of AI systems where such providers are not established in the EU; and
- affected persons or citizens located in the EU.

The AI Act is subject to a final linguist check by lawyers, which is expected to take place in April 2024. This is essentially a validation of the language in the final text of the AI Act to ensure that language translations do not lose the legal meaning set out in the original text. It will also need to be formally endorsed by the European Council. As such, it is expected to be finally adopted before the end of the EP's legislature in June 2024.

The AI Act will enter into force 20 days after its publication in the Official Journal. It will be fully applicable 24 months after its entry into force. However, certain provisions will come into force and need to be complied with sooner.

78. Reproduced from High-level summary of the AI Act, EU Artificial Intelligence. Available at https://artificialintelligenceact.eu/high-level-summary/

Four (4) Point Summary of European Union Proposed AI

The AI Act classifies AI according to its risk:

- Unacceptable risk is prohibited (e.g. social scoring systems and manipulative AI).
- Most of the text addresses high-risk AI systems, which are regulated.
- A smaller section handles limited risk AI systems, subject to lighter transparency obligations: developers and deployers must ensure that end-users are aware that they are interacting with AI (chatbots and deepfakes).
- Minimal risk is unregulated (including the majority of AI applications currently available on the EU single market, such as AI enabled video games and spam filters – at least in 2021; this is changing with generative AI).

The majority of obligations fall on providers (developers) of high-risk AI systems.

- Those that intend to place on the market or put into service high-risk AI systems in the EU, regardless of whether they are based in the EU or a third country.
- And also third country providers where the high risk AI system's output is used in the EU.

Users are natural or legal persons that deploy an AI system in a professional capacity, not affected end-users.

- Users (deployers) of high-risk AI systems have some obligations, though less than providers (developers).
- This applies to users located in the EU, and third country users where the AI system's output is used in the EU.

General purpose AI (GPAI):

- All GPAI model providers must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training.
- Free and open licence GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk.
- All providers of GPAI models that present a systemic risk – open or closed – must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections.

AI systems:

- deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm.
- exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm.
- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data.
- social scoring, i.e., evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people.
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity.

- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage.
- inferring emotions in workplaces or educational institutions, except for medical or safety reasons.
- 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except when:
- searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited;
- preventing substantial and imminent threat to life, or foreseeable terrorist attack; or
- identifying suspects in serious crimes (e.g., murder, rape, armed robbery, narcotic and illegal weapons trafficking, organised crime, and environmental crime, etc.).

Governance

How will the AI Act be implemented?

- The AI Office will be established, sitting within the Commission, to monitor the effective implementation and compliance of GPAI model providers.
- Downstream providers can lodge a complaint regarding the upstream providers infringement to the AI Office.

The AI Office may conduct evaluations of the GPAI model to:

- Assess compliance where the information gathered under its powers to request information is insufficient.
- Investigate systemic risks, particularly following a qualified report from the scientific panel of independent experts.

Timelines

See this post for an overview of the full implementation timeline.

After entry into force, the AI Act will apply:

- 6 months for prohibited AI systems.
- 12 months for GPAI.
- 24 months for high risk AI systems under Annex III.
- 36 months for high risk AI systems under Annex II.

Codes of practice must be ready 9 months after entry into force.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021[79]

In year 2021, Government notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

Amidst growing concerns around lack of transparency, accountability and rights of users related to digital media and after elaborate consultation with the public and stakeholders, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 has been framed in exercise of powers under section 87 (2) of the Information Technology Act, 2000 and in supersession of the earlier Information Technology (Intermediary Guidelines) Rules 2011.

79. Reproduced from Press Information Bureau of India. Available at https://pib.gov.in/Pressreleaseshare.aspx?PRID=1700749

While finalizing these Rules, both the Ministries of Electronics and Information Technology and Ministry of Information and Broadcasting undertook elaborate consultations among themselves in order to have a harmonious, soft-touch oversight mechanism in relation to social media platform as well as digital media and OTT platforms etc.

Part- II of these Rules shall be administered by Ministry of Electronics and IT, while Part-III relating to Code of Ethics and procedure and safeguards in relation to digital media shall be administered by the Ministry of Information and Broadcasting.

Background:

The Digital India programme has now become a movement which is empowering common Indians with the power of technology. The extensive spread of mobile phones, Internet etc. has also enabled many social media platforms to expand their footprints in India. Common people are also using these platforms in a very significant way. Some portals, which publish analysis about social media platforms and which have not been disputed, have reported the following numbers as user base of major social media platforms in India:

- WhatsApp users: 53 Crore
- YouTube users: 44.8 Crore
- Facebook users: 41 Crore
- Instagram users: 21 Crore
- Twitter users: 1.75 Crore

These social platforms have enabled common Indians to show their creativity, ask questions, be informed and freely share their views, including criticism of the Government and its functionaries. The Government acknowledges and respects the right of every Indian to criticize and disagree as an essential element of democracy. India is the world's largest open Internet society and the Government welcomes social media companies to operate in India, do business and also earn profits. However, they will have to be accountable to the Constitution and laws of India.

Proliferation of social media, on one hand empowers the citizens then on the other hand gives rise to some serious concerns and consequences which have grown manifold in recent years. These concerns have been raised from time to time in various forums including in the Parliament and its committees, judicial orders and in civil society deliberations in different parts of country. Such concerns are also raised all over the world and it is becoming an international issue.

Of late, some very disturbing developments are observed on the social media platforms. Persistent spread of fake news has compelled many media platforms to create fact-check mechanisms. Rampant abuse of social media to share morphed images of women and contents related to revenge porn have often threatened the dignity of women. Misuse of social media for settling corporate rivalries in blatantly unethical manner has become a major concern for businesses. Instances of use of abusive language, defamatory and obscene contents and blatant disrespect to religious sentiments through platforms are growing.

Over the years, the increasing instances of misuse of social media by criminals, anti-national elements have brought new challenges for law enforcement agencies. These include inducement for recruitment of terrorists, circulation of obscene content, spread of disharmony, financial frauds, incitement of violence, public order etc.

It was found that currently there is no robust complaint mechanism wherein the ordinary users of social media and OTT platforms can register their complaint and get it redressed within defined timeline. Lack of transparency and absence of robust grievance redressal mechanism have left the users totally dependent on the whims and fancies of social media platforms. Often it has been seen that a user who has spent his time, energy and money in developing a social media profile is left with no remedies in case that profile is restricted or removed by the platform without giving any opportunity to be heard.

Evolution of Social Media and Other Intermediaries:

If we notice the evolution of social media intermediaries, they are no longer limited to playing the role of pure intermediary and often they become publishers. These Rules are a fine blend of liberal touch with gentle self-regulatory framework. It works on the existing laws and statues of the country which are applicable to content whether online or offline. In respect of news and current affairs publishers are expected to follow the journalistic conduct of Press Council of India and the Programme Code under the Cable Television Network Act, which are already applicable to print and TV. Hence, only a level playing field has been proposed.

Rationale and Justification for New Guidelines:

These Rules substantially empower the ordinary users of digital platforms to seek redressal for their grievances and command accountability in case of infringement of their rights. In this direction, the following developments are noteworthy:

- The Supreme Court in suo-moto writ petition (Prajjawala case) vide order dated 11/12/2018 had observed that the Government of India may frame necessary guidelines to eliminate child pornography, rape and gangrape imageries, videos and sites in content hosting platforms and other applications.
- The Supreme Court vide order dated 24/09/2019 had directed the Ministry of Electronics and Information Technology to apprise the timeline in respect of completing the process of notifying the new rules.
- There was a Calling Attention Motion on the misuse of social media and spread of fake news in the Rajya Sabha and the Minister had conveyed to the house on 26/07/2018, the resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law. He had conveyed this after repeated demands from the Members of the Parliament to take corrective measures.
- The Ad-hoc committee of the Rajya Sabha laid its report on 03/02/2020 after studying the alarming issue of pornography on social media and its effect on children and society as a whole and recommended for enabling identification of the first originator of such contents.

Consultations:

The Ministry of Electronics and Information Technology (MEITY) prepared draft Rules and invited public comments on 24/12/2018. MEITY received 171 comments from individuals, civil society, industry association and organizations. 80 counter comments to these comments were also received. These comments were analyzed in detail and an inter-ministerial meeting was also held and accordingly, these Rules have been finalized.

Salient Features

Guidelines Related to Social Media to Be Administered by Ministry of Electronics and IT:

- ***Due Diligence To Be Followed By Intermediaries:*** The Rules prescribe due diligence that must be followed by intermediaries, including social media intermediaries. In case, due diligence is not followed by the intermediary, safe harbour provisions will not apply to them.
- ***Grievance Redressal Mechanism:*** The Rules seek to empower the users by mandating the intermediaries, including social media intermediaries, to establish a grievance redressal mechanism for receiving resolving complaints from the users or victims. Intermediaries shall appoint a Grievance Officer to deal with such complaints andshare the name and contact details of such officer. Grievance Officer shall acknowledge the complaint within twenty four hours and resolve it within fifteen days from its receipt.
- ***Ensuring Online Safety and Dignity of Users, Specially Women Users:*** Intermediaries shall remove or disable access withing 24 hours of receipt of complaints of contents that exposes the private areas

of individuals, show such individuals in full or partial nudity or in sexual act or is in the nature of impersonation including morphed images etc. Such a complaint can be filed either by the individual or by any other person on his/her behalf.

- ***Two Categories of Social Media Intermediaries:*** To encourage innovations and enable growth of new social media intermediaries without subjecting smaller platforms to significant compliance requirement, the Rules make a distinction between social media intermediaries and significant social media intermediaries. This distinction is based on the number of users on the social media platform. Government is empowered to notify the threshold of user base that will distinguish between social media intermediaries and significant social media intermediaries. The Rules require the significant social media intermediaries to follow certain additional due diligence.

Additional Due Diligence to Be Followed by Significant Social Media Intermediary:

- Appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and Rules. Such a person should be a resident in India.
- Appoint a Nodal Contact Person for 24x7 coordination with law enforcement agencies. Such a person shall be a resident in India.
- Appoint a Resident Grievance Officer who shall perform the functions mentioned under Grievance Redressal Mechanism. Such a person shall be a resident in India.
- Publish a monthly compliance report mentioning the details of complaints received and action taken on the complaints as well as details of contents removed proactively by the significant social media intermediary.
- Significant social media intermediaries providing services primarily in the nature of messaging shall enable identification of the first originator of the information that is required only for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material punishable with imprisonment for a term of not less than five years. Intermediary shall not be required to disclose the contents of any message or any other information to the first originator.
- Significant social media intermediary shall have a physical contact address in India published on its website or mobile app or both.
- Voluntary User Verification Mechanism: Users who wish to verify their accounts voluntarily shall be provided an appropriate mechanism to verify their accounts and provided with demonstrable and visible mark of verification.
- Giving Users An Opportunity to Be Heard: In cases where significant social media intermediaries removes or disables access to any information on their own accord, then a prior intimation for the same shall be communicated to the user who has shared that information with a notice explaining the grounds and reasons for such action. Users must be provided an adequate and reasonable opportunity to dispute the action taken by the intermediary.
- Removal of Unlawful Information: An intermediary upon receiving actual knowledge in the form of an order by a court or being notified by the Appropriate Govt. or its agencies through authorized officer should not host or publish any information which is prohibited under any law in relation to the interest of the sovereignty and integrity of India, public order, friendly relations with foreign countries etc.

- The Rules will come in effect from the date of their publication in the gazette, except for the additional due diligence for significant social media intermediaries, which shall come in effect 3 months after publication of these Rules.

Digital Media Ethics Code Relating to Digital Media and OTT Platforms to Be Administered by Ministry of Information and Broadcasting:

There have been widespread concerns about issues relating to digital contents both on digital media and OTT platforms. Civil Society, film makers, political leaders including Chief Minister, trade organizations and associations have all voiced their concerns and highlighted the imperative need for an appropriate institutional mechanism. The Government also received many complaints from civil society and parents requesting interventions. There were many court proceedings in the Supreme Court and High Courts, where courts also urged the Government to take suitable measures.

Since the matter relates to digital platforms, therefore, a conscious decision was taken that issues relating to digital media and OTT and other creative programmes on Internet shall be administered by the Ministry of Information and Broadcasting but the overall architecture shall be under the Information Technology Act, which governs digital platforms.

Consultations:

Ministry of Information and Broadcasting held consultations in Delhi, Mumbai and Chennai over the last one and half years wherein OTT players have been urged to develop "self-regulatory mechanism". The Government also studied the models in other countries including Singapore, Australia, EU and UK and has gathered that most of them either have an institutional mechanism to regulate digital content or are in the process of setting-up one.

The Rules establish a soft-touch self-regulatory architecture and a Code of Ethics and three tier grievance redressal mechanism for news publishers and OTT Platforms and digital media.

Notified under section 87 of Information Technology Act, these Rules empower the Ministry of Information and Broadcasting to implement Part-III of the Rules which prescribe the following:

- Code of Ethics for online news, OTT platforms and digital media: This Code of Ethics prescribe the guidelines to be followed by OTT platforms and online news and digital media entities.
- Self-Classification of Content: The OTT platforms, called as the publishers of online curated content in the rules, would self-classify the content into five age based categories- U (Universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult). Platforms would be required to implement parental locks for content classified as U/A 13+ or higher, and reliable age verification mechanisms for content classified as "A". The publisher of online curated content shall prominently display the classification rating specific to each content or programme together with a content descriptor informing the user about the nature of the content, and advising on viewer description (if applicable) at the beginning of every programme enabling the user to make an informed decision, prior to watching the programme.
- Publishers of news on digital media would be required to observe Norms of Journalistic Conduct of the Press Council of India and the Programme Code under the Cable Television Networks Regulation Act thereby providing a level playing field between the offline (Print, TV) and digital media.
- A three-level grievance redressal mechanism has been established under the rules with different levels of self-regulation.

  Level-I: Self-regulation by the publishers;

Level-II: Self-regulation by the self-regulating bodies of the publishers;

Level-III: Oversight mechanism.

- Self-regulation by the Publisher: Publisher shall appoint a Grievance Redressal Officer based in India who shall be responsible for the redressal of grievances received by it. The officer shall take decision on every grievance received by it within 15 days.
- Self-Regulatory Body: There may be one or more self-regulatory bodies of publishers. Such a body shall be headed by a retired judge of the Supreme Court, a High Court or independent eminent person and have not more than six members. Such a body will have to register with the Ministry of Information and Broadcasting. This body will oversee the adherence by the publisher to the Code of Ethics and address grievances that have not be been resolved by the publisher within 15 days.
- Oversight Mechanism: Ministry of Information and Broadcasting shall formulate an oversight mechanism. It shall publish a charter for self-regulating bodies, including Codes of Practices. It shall establish an Inter-Departmental Committee for hearing grievances.

Other Statutes on Data Protection

Apart from Information Technology Act, 2000 and Information Technology (Amendment) Act, 2008, there are following statutes as well which affords some indirect protection to data and privacy:

1. Indian Penal Code, 1860[80]
2. Indian Telegraph Act, 1885[81]
3. Indian Contract Act, 1872[82]
4. Indian Copyright Act, 1957[83]
5. The Specific Relief Act, 1963[84]
6. The Public Financial Institution Act, 1983[85]
7. The Consumer Protection Act, 1986[86]
8. The Credit Information Companies (Regulation) Act, 2005[87]

80. The IPC, 1860 does not directly address the breach of data privacy but has been used to bring prosecutions for data theft under Section 405 (criminal breach of trust), 406 (Punishment for criminal breach of trust), 420 (cheating and dishonesty including delivery of property).

81. This Act protects the personal information and privacy of individuals in the telecommunication area.

82. The Indian Contract Act renders data protection and privacy protection in the form of breach of contract and specific performance of contract. The law of contract says that the parties involved in a contract must adhere with the rules and regulations as specified in the agreement. If terms and conditions calling for the protection of information are violated by the disclosure of the information shared between the parties, causing intentional damages to other amounts to breach of contract.

83. This Act provides security to literary, artistic, dramatic and musical work. The copyright act provide right to the original author of above mentioned fields so that no one can misuse their work and maintain the privacy if it is related with some sensitive information and maintain the originality of work. Specifically mention Section 16 and 63B of Indian Copyright Act, 1957.

84. This Act provides for the specific relief to the people, who can claim temporary and permanent injunctions against unauthorized disclosure of confidential information.

85. Kottabomman Transport Corporation Limited vs. State Bank of Travancore and Others, AIR 1992 Ker. 351: Banks are under a duty to secrecy and not to disclose information to third party.

86. This Act provides the provisions through which the consumer can claim protection from exploitation and can save them from deficiency of services by disclosing proprietary information, personal information etc. without adequate authorization.

87. See, Section 19: Information should be accurate and protected against unauthorized use and disclosure.

CASE STUDY

1. On Cyber Threat

User accounts accessed by attackers due to flaw in "view as" feature: In September 2018, the social media company admitted to a serious vulnerability (which was described as a flaw in Facebook's "view as" feature) that allowed hackers to gain access to accounts and even third-party apps that used Facebook for login to gain unauthorized access to millions of accounts, initially it was stated that 50 million accounts were affected. Access tokens for 30 million accounts were stolen by hackers, who accessed contact information (name and email id/ phone number) for 14 million accounts and additional information was accessed for another 15 million accounts including gender, religion, location and device information. Within a month, the company had disclosed that another 40 million user accounts were deemed at risk from the security flaw before steps were taken to protect them. The company said it reset the access tokens of the 50 million accounts affected by the attack and took a "precautionary step" of resetting tokens for the other 40 million accounts. This raises an alarm of cyber threat on the PIIs of the users.

2. On Cyber Crime

- Zee News in their publication on April 29, 2022 reported that the first two months of 2022 reported more cyber-crimes than the entire 2018, according to data by CERT-In (Indian Computer Emergency Response Team). CERT-In is the nodal agency to deal with cyber security threats and operates under the Ministry of Electronic & Information Technology.
- Cyber-crime cases have witnessed a steady spike since 2018. India reported 2,08,456 incidents in 2018; 3,94,499 incidents in 2019; 11,58,208 cases in 2020; 14,02,809 cases in 2021; and 2,12,485 incidents in the first two months of 2022. The above figures show that cyber-crimes increased almost seven times in three years between 2018 and 2021, and more sharply during the pandemic.
- A total of 17,560; 24,768 and 26,121 Indian websites were hacked in 2018, 2019 and 2020 respectively, CERT-In data further says.
- The National Crime Records Bureau (NCRB), however, presents a different set of data. According to NCRB, India reported 50,035 cyber-crimes in 2020; 44,546 cases in 2019 and 27,248 cases in 2018.
- The year 2020 saw 4,047 cases of online banking fraud; 2,160 cases of ATM fraud; 1,194 credit/ debit card fraud and 1,093 OTP frauds. As per NCRB data, there were 972 cases of cyber stalking/bullying of women and children and 578 cases of fake news on social media.
- Committing fraud was found to be the biggest motive and accounted for 30,142 out of the total 50,035 cases (60.02 per cent). This was followed by sexual exploitation (6.6 per cent) and extortion 4.9 per cent.
- Cyber-crime rate was highest in Karnataka (16.2 per cent), followed by Telangana (13.4 per cent) and Assam (10.1 per cent).

LESSON ROUND-UP

- Advent of information technology has not only provided us the assorted means of communicating our information at an inclusive platform but it has also ensured quick communication of information.
- However, it has been righty said that 'with boon goes the bane', so is the sphere of information technology. At one side, this easy medium of transferring data and quicker communication has given birth to numerous recompenses of communication and transaction; on the other side, various dark sides are being observed under IT enables and electronic transactions. The major among them are Cyber Crimes and Cyber Attacks.
- Hence in order to control the mechanism of cyber-crimes and cyber-attacks, cyber law has been evolved gradually which ensures cyber security in cyber sphere.
- Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems.
- A cyber threat (also known as cybersecurity threat) is defined as a malicious act that seeks to steal or damage data or disrupt the digital wellbeing and stability in general.
- Cyber threats may come from a variety of places, people, and contexts.
- Cyberwar (also called cyberwarfare or cyber warfare) is defined as a war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states.
- Cyber-crime is any criminal activity that involves a computer, networked device or a network. In general, most cybercrimes are carried out in order to generate profit for the cybercriminals, yet some of cybercrimes are carried out against computers or devices directly to damage or disable them.
- Cybercrime can have wide-ranging impacts, at the individual, local, state, and national levels.
- The term cyberterrorism was first coined by Banny C. Collin of the Institute for Security and Intelligence (ISI) in the late 1980s. But its usage was better understood during the 9/11 attack.
- A cyber or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.
- Cyber threat hunting is a proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools.
- A cyber threat hunt is composed of steps or processes designed for an efficient, successful hunt.
- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.
- The term digital forensics was first used as a synonym for computer forensics.
- Indeed internet has revolutionized the way we interact; however, it has also bought with it a host of problems such as hate speech, fake news, illegal lobbying and personal data theft. The number of these issues not only make the criminal/offender liable, yet many a times, online platforms are also made liable for the cyber security threat.
- To encounter the challenges of information privacy and to promote legal control over privacy protection in electronic transactions, some legal policies and regulations have already been established at international and national level.

- At international level, some fair information principles like Notice, Choice, Access, Consent, Enforcement etc. are directed to be followed by the e-commerce companies to ensure the information privacy in the conduct of online transactions.
- Though at the industry level, even the e-commerce companies are also taking some steps to protect the information privacy of the individuals by adopting and declaring privacy policy, yet much is left to be governed by the nationally and internationally commended regulations.
- At national level, countries around the world have enacted different laws to protect privacy of individuals.
- With digital transformation at its high in India, March 2023 has witnessed a magnificent move with the official announcement of enacting Digital India Act (DIA) while replacing a 24-year-old Information Technology Act of 2000 (IT Act).
- This proactive move by the Ministry of Electronics and Information Technology (MeitY) aligns with India's ambitious "Digital India" initiative.
- The proposed Digital India Act (DIA) *inter-alia* with an aim to provide a *future ready legislation* opts "*principles and rule-based approach*" for regulating digital transactions including the evolving era of Artificial Intelligence and Machine Learning.
- One shall always remember one of powerful legal maxim "*Ignorantia Juris Non Excusat*", which means ignorance of law is not an excuse.
- Hence, one should stay prepared before the proposed DIA is notified. It is to be noted that separate rules will govern different kinds of industry. Hence ***Industry Specific Compliance Calendars*** will be required.
    - The intention behind the DIA is laudable and this legislation will be revamping India's technology sector regulations.
    - It is for the first time that consultations are taking place during the pre-draft stage of the bill. Policymakers are aware of the challenges that might arise therefore the opinions of important stakeholders are being valued.
    - The need for comprehensive and relevant legislation was much needed for the evolving technology sector in India.
    - The three new criminal laws that were passed by Parliament in 2023 will come into effect from July 1, 2024, according to a notification by the Ministry of Home Affairs
    - For all three new criminal laws, efforts are being made to take these issues forward with the help of technology.
    - This will also help us in increasing the conviction rate. Along with this, efforts are also being made to modernize the entire process.
    - Initially introduced in 2019, the Digital Personal Data Protection Act holds considerable importance as a legislative measure aimed at safeguarding individuals' privacy rights.
    - Its primary focus lies in regulating the collection, storage, processing, and transfer of personal data in the digital landscape. The DPDP Bill underwent 81 amendments after its initial introduction, resulting in a comprehensive overhaul to its present form.
    - By prioritizing privacy and security, the DPDP Act strives to create a robust framework that addresses the challenges posed by data handling in the digital age.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What do you mean by Cyber Threats? Discuss four recent types of Cyber Threats encountered in covid times.
2. What is Cyber Threat Hunting? Describe few techniques of Cyber Hunting.
3. Write a brief note on Digital Intellectual Property along with ways to protect the same.
4. Discuss Artificial Intelligence (AI). Briefly describe the development of AI in India.
5. Write Short Note on any Four of the following:
    a. Cyber Warfare
    b. Cyber Terrorism
    c. Digital Forensics
    d. Safe Harbour Protection
    e. Cyber Security Framework (NCFS)
6. Briefly discuss the need and proposed structure of proposed Digital India Act
7. Write a short note on Digital Personal Data Protection Act, 2023 and also analyze its significance in the perspective of protecting data privacy of personal information.

LIST OF FURTHER READINGS

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

- Chattopaddhyay Sougata (2020) Intellectual Property Rights in Digital Environment, ePrints in Library and Information Science
- Erdal Ozkaya (2022) Practical Cyber Threat Intelligence: Gather, Process, and Analyze Threat Actor Motives, Targets, and Attacks with Cyber Intelligence Practices Paperback – Import, 27 June 2022, BPB Publications
- European Union on Liability of online platform (2021), Study Published by Scientific Foresight Unit (STOA) European Parliamentary Research Service, EU. Available on https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf
- Malik Surendra and Malik Sudeep (2019) Supreme Court on Information Technology Act, Internet and Cyber Laws and Aadhar, Eastern Book Company
- Pokhariyal Purvi, Kashyap Amit and Arun Prasad (2022) Artificial Intelligence: Law and Policy Implications, Eastern Book Company, ISBN: 9789389656954, 9789394364806
- Raman and Sharma (2019) Cyber Terrorism in India: A Physical Reality Or Virtual Myth, Indian Journal of Law and Human Behavior Volume 5 Number 2 (Special Issue), May - August 2019
- Singh and Mara (2021) Intermediary Liability in India – Moving Goalposts, Mondaq
- What is Digital Forensics and Incident Response (DFIR), SentinelOne
- Proposed Digital India Act. Proposal By MEITY. Report available at https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

Cyber Crimes and Investigation Procedures

Lesson 4

KEY CONCEPTS

■ Investigation ■ Cyber Crime ■ Cyber Forensics ■ Digital Evidence ■ Security Audit

Learning Objectives

To understand:

- Status of Cyber Crimes in Indian Scenario
- Government Initiatives to Regulate and Control Cyber Crimes
- Tools and Techniques Used to Commit Cyber Crimes
- Reporting of Cyber Crimes
- Investigation of Cyber Crimes and Process under Indian Laws
- Central Government Initiative on Strengthening Mechanism to Lever Cyber Crimes
- Steps of Conducing Investigation of Cyber Crimes
- Prosecution of Cyber-Crimes
- Computer Forensics
- Digital Evidences
- Security Audit

Lesson Outline

- Introduction
- Overview of Cyber Crimes and Indian Scenario
- Initiatives to Regulate and Control Cyber Crimes: Governmental and Law Enforcement Agencies
- Tools and Techniques Used to Commit Cyber Crimes
- Reporting of Cyber Crimes
- Investigation of Cyber Crimes and Process under Indian Laws
- Computer Forensics and Digital Evidences
- What is Computer Forensics?
- Types of Computer Forensics
- Role of Computer Forensics
- Investigation vide Computer Forensics
- Steps in Digital Forensics
- Branches of Digital Forensics
- Digital Forensics – Chain of Custody
- Security Audit
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

INTRODUCTION

As discussed in the previous chapters that use of Internet and rapid deployment of information and communication technologies in recent years have bought various changes in the world both at individual level as well as organization level. Right from the way we communicate to the way we buy our groceries, each and every activity of human life is revolutionized with the help of information and communication technology. Crime is not an exception to this revolution brought by information and communication technologies. On one hand wherein the pattern of crime has been altered by misusing the tools and techniques of information and communication technology, on the similar hand, historic trends and practices in criminal investigation has also been revolutionized. This has created a tremendous challenge for law enforcement to develop the capacity to confront transnational crimes and follow evidence trails. Among the obstacles were legal, technical and operational challenges, but these are not the total extent of the difficulties faced; rather, they have been recognized as the main issues to be addressed in order that law enforcement agencies are able to meet the emerging challenges of cybercrime. Traditional law enforcement government agencies are now called upon to investigate not only real-world crimes, but also crimes on the Internet. For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible. Due to the Information Technology Act, 2000 ("IT Act"), certain provisions of Criminal Procedure Code, 1973 and the Evidence Act, 1872 have been amended. Along with this, certain new regulations had been enforced by the Indian legal system to meet with the need of cyber-crime investigation. Hence, this chapter aims to provide the understanding on the following:

- Overview of Cyber Crimes and Indian Scenario
- Initiatives to Regulate and Control Cyber Crimes: Governmental and Law Enforcement Agencies
- Tools and Techniques Used to Commit Cyber Crimes
- Reporting of Cyber Crimes
- Investigation of Cyber Crimes and Process under Indian Laws
- Case Study: Steps of Conducing Investigation of Cyber Crimes
- Cyber Forensics
- Digital Evidences
- Security Audit.

OVERVIEW OF CYBER CRIMES[1]

In simplest words, cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.[2] Cybercrime can be carried out by individuals or organizations. As per Britannica Dictionary – "*Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.*" Hence any crime conduced with the use of computer and computer network will fall under the category of cybercrime.

> In any statute, the term cybercrime is not defined. Any unauthorized/ unlawful act, commissioned with the use of a computer or computer network or communication device, to commit or facilitate the crime is called cyber-crime.

1 Students to Note: Cyber Crime and Types of Cyber Crime are discussed in detail in chapter 2 and 3 of this study material.

2 Kaspersky (2021) What is Cybercrime? How to protect yourself from cybercrime.

CYBER CRIME *VIS-À-VIS* INDIAN SCENARIO

As is being seen world over, cyber-crimes are on the rise in India also and so are the arrests made in cyber-crimes cases. India has been a favorite hub for cybercriminals, mostly hackers and other malevolent users who misuse the Internet by committing crimes. Data Security Council of India in their Cyber Crime Investigation Manual[3] in 2011 have quoted *Crime in India 2009 report published by National Crime Reporting Bureau (NCRB)*, and that point in time there has been an increase of over 45% in the number of cyber-crimes reported under The Information Technology Act 2000 (IT Act) in 2009 over the corresponding figures for 2008. In 2021 also cyber-crimes in India saw the rise of 6% in comparison to previous year.[4] As per the data revealed by Statista[5] "*India saw a significant jump in cyber-crimes reported in 2021 from the 2020. That year, over 52 thousand cyber-crime incidents were registered. Karnataka and Uttar Pradesh accounted for the highest share during the measured time period. The northern state of Uttar Pradesh had the highest number of cyber-crimes compared to the rest of the country, with over six thousand cases registered with the authorities in 2018 alone. India's tech state, Karnataka, followed suite that year. A majority of these cases were registered under the IT Act with the motive to defraud, or sexually exploit victims*." As per the report it was estimated that in 2017, consumers in India collectively lost over 18 billion U.S. dollars due to cyber-crimes. However, these were estimates based only on reported numbers. In a country like India, it is highly likely that the actual figures could be under-reported due to a lack of cyber-crime awareness or the mechanisms to classify them. Recent government initiatives such as a dedicated online portal to report cyber-crimes could very well be the main factor behind a sudden spike in online crimes from 2017 onwards. Such an increase in the number of cyber-crimes cases could pose serious economic and national security challenges.

As per 2019 Norton Life Lock Cyber Safety Insights Report, 63% Indians do not know what they will do if their identities are stolen, even though 70% are worried that identities will be stolen. 4 in 10 consumers in India have experienced identity theft.[6] Cyber-crimes know no borders and grow at a pace at par with emerging technologies.

India is the 80th most targeted country worldwide in cybercrime: Report[7]

It is stated in an article of The Hindu, with the rise of AI use and the consistent digital payment adoption here, it has become imperative for organizations to continuously improve their cybersecurity posture to protect their assets and maintain stakeholder trust.

As per the Report published on recording the cyber incidents, India was placed on the 80th position in a report focusing on local threats in the year 2023. The position is based on the malicious programs found directly on users' computers or removable media connected to them (flash drives, camera memory cards, phones, external hard drives) or that initially made their way onto the computer in non-open form, including programs in complex installers or encrypted files.

Additionally, nearly 34% of users in India were targeted by local threats, amounting to some 74,385,324 local incidents being blocked by one of the leading antivirus companies.

India's cybersecurity market reached USD 6.06 billion in 2023. However, according to IDC, a global marketing intelligence firm, the alarming increase in sophisticated external cyber threats and cybersecurity attacks is one of the biggest challenges for the majority of enterprises in establishing organizational trust.

---

3 Data Security Council of India (2011) Cyber Crime Investigation Manual with Knowledge Partner Deloitte

4 https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html

5 Basuroy Tanushree (October 13, 2022) Number of Cyber Crimes reported in India 2012-2021

6 https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019survey/articleshow/75093578.cms#:~:text=Rs%20131.2%20million%20is%20the,the%20global%20average%20being%2067%25

7. Reproduced from The Hindu. Available at https://www.thehindu.com/sci-tech/technology/india-the-80-most-targeted-country-worldwide-in-cybercrime/article67869960.ece

Almost 67% of Indian enterprises are reportedly looking to outsource key areas of security landscape to managed security service providers in the next three years.

The following four major categories of crimes reported in India as per NCRB constitutes nearly 90% of the cyber-crimes:

a. Hacking of Computer System

b. Forgery / counterfeiting using Computers

c. Publication / Transmission of obscene information in electronic form i.e. Pornography

d. Breach of Trust / Frauds.

According to Director CBI, "The use of modern technology has resulted in traditional crime becoming global. This has made the task of investigation more difficult and complex. There are several examples of kidnapping, terrorist attacks, economic crimes, bank frauds and financial scams being committed with the help of computers"[8]. Thus, the task before the law enforcement authorities is going to grow in complexity and, urgent focus is needed to build capacity to tackle this growing menace.

Tools and Techniques used to Commit Cyber Crimes[9]

On one hand where we are witnessing the advancement of information and communication technology; on the similar end, we are seeing the new tools and techniques of committing cybercrimes. In general, cyber criminals make use of various tools and techniques yet the following are the most common tools and techniques used recently to conduct cybercrimes.

It is to be noted that many of these tools (*used for the commission of the cyber-crimes*) are installed on the victim's systems through exploitation of the vulnerabilities in the systems / networks or by surreptitiously gaining access to the victim's systems which may include physical access or by making use of the intermediary systems or by deceiving the victim to allow access to his system or by gathering the victim information.

- **Buffer overflow:** The condition when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.
- **Cracking:** Cracking is breaking into someone else's computer system, often on a network; bypassing passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this either for profit, or maliciously, or for some altruistic purpose or cause.
- **Data Didling:** Involves altering the raw data just before a computer processes it and then changing it back after processing is completed.
- **Malware**: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
- **Phishing:** Using spoof E-mails or directing the people to fake web sites to deceive them into divulging personal financial details so that criminals can access their accounts.
- **Rootkit**: A set of tools that enables continued privileged access to a computer, while actively hiding its

8 http://www.cbi.gov.in/speech/nasscom_20101122_dcbi.php

9 Source: Data Security Council of India (2011) Cyber Crime Investigation Manual with Knowledge Partner Deloitte

presence from the administrator. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

- **Salami Attack:** A programmed attack which is implemented in small (meant to be unnoticeable) increments. This attack involves making alteration so insignificant that it is easily concealed and would go completely unnoticed. Attacks are used for commission of financial crimes.
- **Sniffer**: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate net-work management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.
- **Social Engineering:** A hacker term which involves non-technical intrusion for deceiving or manipulating unwitting people into giving out information about a network or how to access it.
- **Spoofing:** Refers to a situation in which the incoming information from an attacker is masqueraded as one that appears to come from a trusted source to the recipient or to the recipient network. Often the messages from the fraudster appearing to be from a genuine source (like bank), seeks personally identifiable information to perpetrate fraud on the victim.
- **Spyware:** It is a type of malware that is secretly or surreptitiously installed into an information system to gather information on individuals or organisations without their knowledge; a type of malicious code.
- **Steganography**: The art and science of writing hidden messages in such a way that no one, apart from the sender and in-tended recipient, suspects the existence of the message An image file may contain hidden messages between terror groups, which will be known only to the intended recipient and the sender.
- **Trojan:** A malicious program that masquerades as a benign application and can take complete control of the victim's computer system.
- **virus:** A self-replicating program that runs and spreads by modifying other programs or files.
- **Worm**: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.
- **Zombie**: A program that is installed on a system to cause it to attack other systems.

INITIATIVES TO REGULATE AND CONTROL CYBER CRIMES: GOVERNMENTAL AND LAW ENFORCEMENT AGENCIES

The discussion above confirm that India is facing the growing threat of cybercrimes. This has led government of India to channelize the effective ways in enhancing the level of cyber security. This in consolidation has resulted to various initiatives and programs for Cyber Security under the Department of Information Technology along with enactment of the Information Technology Act, 2000. The Act was also amended in the year 2008 retrofitting newer crimes. The Act heralded the legal recognition of electronic documents, digital signatures and transactions done using computers and internet. Further, the Act described the punishment and penalty for criminal offences and contraventions.

Many law enforcement agencies including the Central Bureau of Investigation have created separate units/ cells for handling cybercrimes. The IT capital of India i.e., Bangalore has even led to establish country's first Cyber Crime Police Station. As on date, all the states and almost all the cities have created Cyber Crime Police Stations and, Cyber Crime Cells to handle the menace of growing cybercrimes.

Central Government Initiative on Strengthening Mechanism to Lever Cyber Crimes[10]

The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their Law Enforcement Agencies (LEAs). To strengthen the mechanism to deal with cyber-crimes in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

- The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) to deal with all types of cyber-crime in the country, in a coordinated and comprehensive manner.
- Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber-crime hotspots/ areas having multi-jurisdictional issues by on boarding States/ UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh in 2023.
- National Cyber Forensic Laboratory (Investigation) has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) have provided its services to State LEAs in around 9,000 cyber forensics like mobile forensics, memory forensics, Call Data Record (CDR) Analysis, etc. to help them in investigation of cases pertaining to cyber-crimes.
- The 'National Cyber Crime Reporting Portal' (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber-crimes, with special focus on cybercrimes against women and children. Cyber-crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.
- The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, an amount of more than Rs. 1200 Crore have been saved in more than 4.7 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.
- The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber-crime investigation, forensics, prosecution etc. along with certification. More than 76,000 Police Officers from States/UTs are registered and more than 53,000 Certificates issued through the portal.
- Till date more than 3.2 lakhs SIM cards and 49,000 IMEIs as reported by Police authorities have been blocked by Government of India.
- I4C has imparted cyber hygiene training to 6,000 officials of various Ministries/ Departments of Government of India.
- I4C has imparted cyber hygiene training to more than 23,000 NCC cadets.
- The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 122.24 crores under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. So far, cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs. So far, more than 24,600

10. Reproduced from Increase in Cyber Crime (February 07, 2024), Information was given by Minister of State for Home Minister in a written reply to Rajya Sabha, Press Information Bureau. Available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505

LEA personnel, judicial officers and prosecutors have been provided training on cyber-crime awareness, investigation, forensics etc.

- National Cyber Forensic Laboratory (Evidence) has been set up at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber-crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time.
- To spread awareness on cyber-crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@Cyberdost), Facebook(CyberDostI4C), Instagram (cyberdostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, etc. The States/UTs have also been requested to carry out publicity to create mass awareness.
- CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.
- CERT-In, through RBI, has advised all authorized entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empaneled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.
- CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

CITIZEN FINANCIAL CYBER FRAUD REPORTING AND MANAGEMENT SYSTEM[11]

Recently, as an initiative to provide easy resolution to financial cybercrimes, a new feature "Citizen Financial Cyber Fraud Reporting and Management System" has been activated for prevention of money loss in case of Cyber Financial Fraud. Under this initiative, an immediate reporting the complainant can be made by the victim, which ensures timely action and resolution of the cybercrime.[12]

Reporting of Cyber Crime

The Government of India had launched the online cyber-crime reporting portal, www.cybercrime.gov.in, which is a citizen-centric initiative, to allow the complainants to lodge complaints relating to child pornography/child sexual abuse material or any content which is sexual in nature. The Central Government has launched a scheme for formulating of Indian Cyber Crime Coordination Centre (I4C)[13] to handle the cybercrime incidents in India, in an inclusive & coordinated manner.

The said scheme has following seven components:

- National Cybercrime Threat Analytics Unit (TAU)
- National Cybercrime Forensic Laboratory (NCFL)
- National Cybercrime Training Centre (NCTC)
- Cybercrime Ecosystem Management
- Platform for Joint Cybercrime Investigation Team

11 Source: How is cyber-crime investigation conducted (2020) iPleaders.

12 More details can be accessed from 'Citizen Manual' under "Resources Section" at www.cybercrime.gov.in.

13 https://www.pib.gov.in/PressReleasePage.aspx?PRID=1599067

- National Cybercrime Reporting Portal
- National Cyber Research and Innovation Centre (NCR&IC).

The government is also planning to set up Regional Cyber Crime Coordination Centers at respective States/UTs.

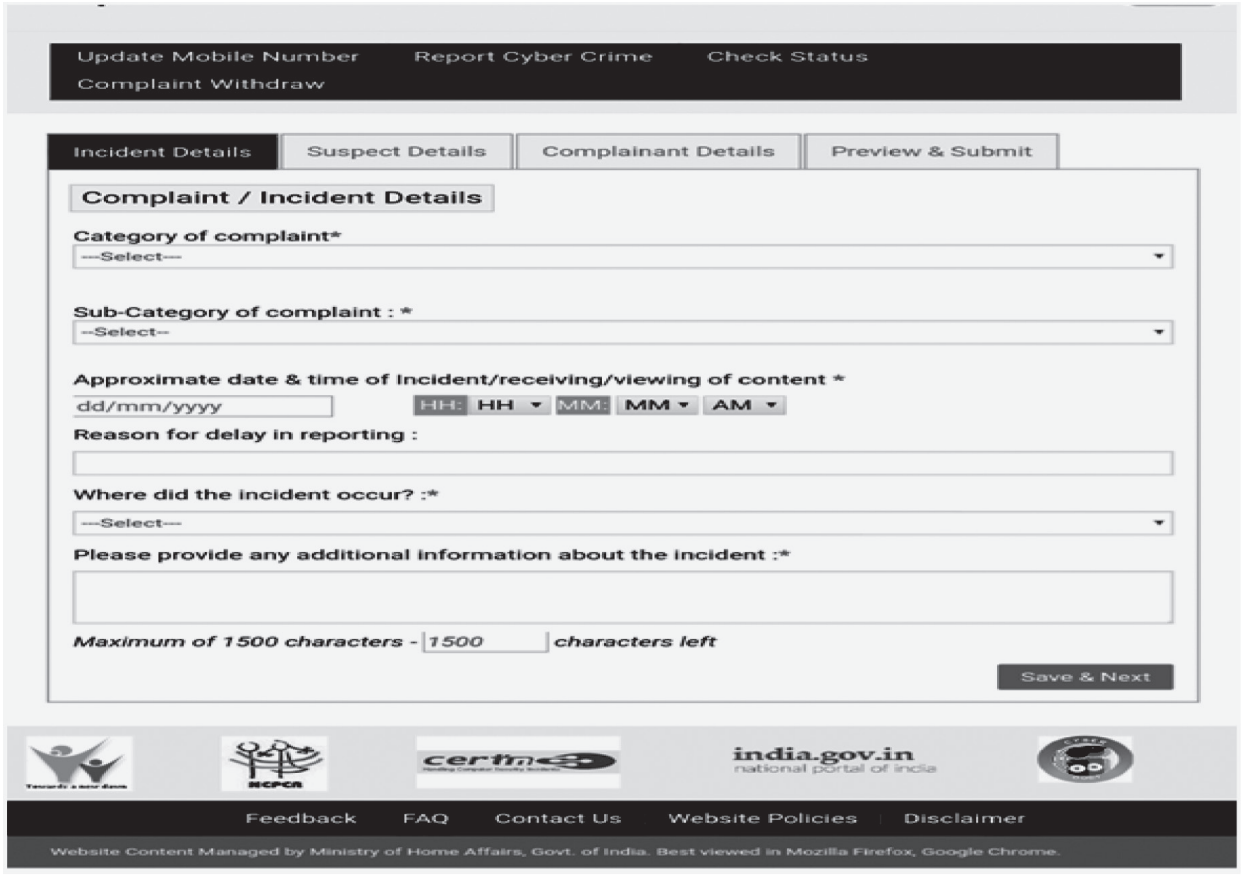
PROCESS OF REPORTING A CYBER CRIME[14]

A Cyber-crime can be reported online as well as offline i.e., in physical form

***A. Online Reporting of Cyber Crime*:** By following below-mentioned steps, one can report a cyber-crime online:

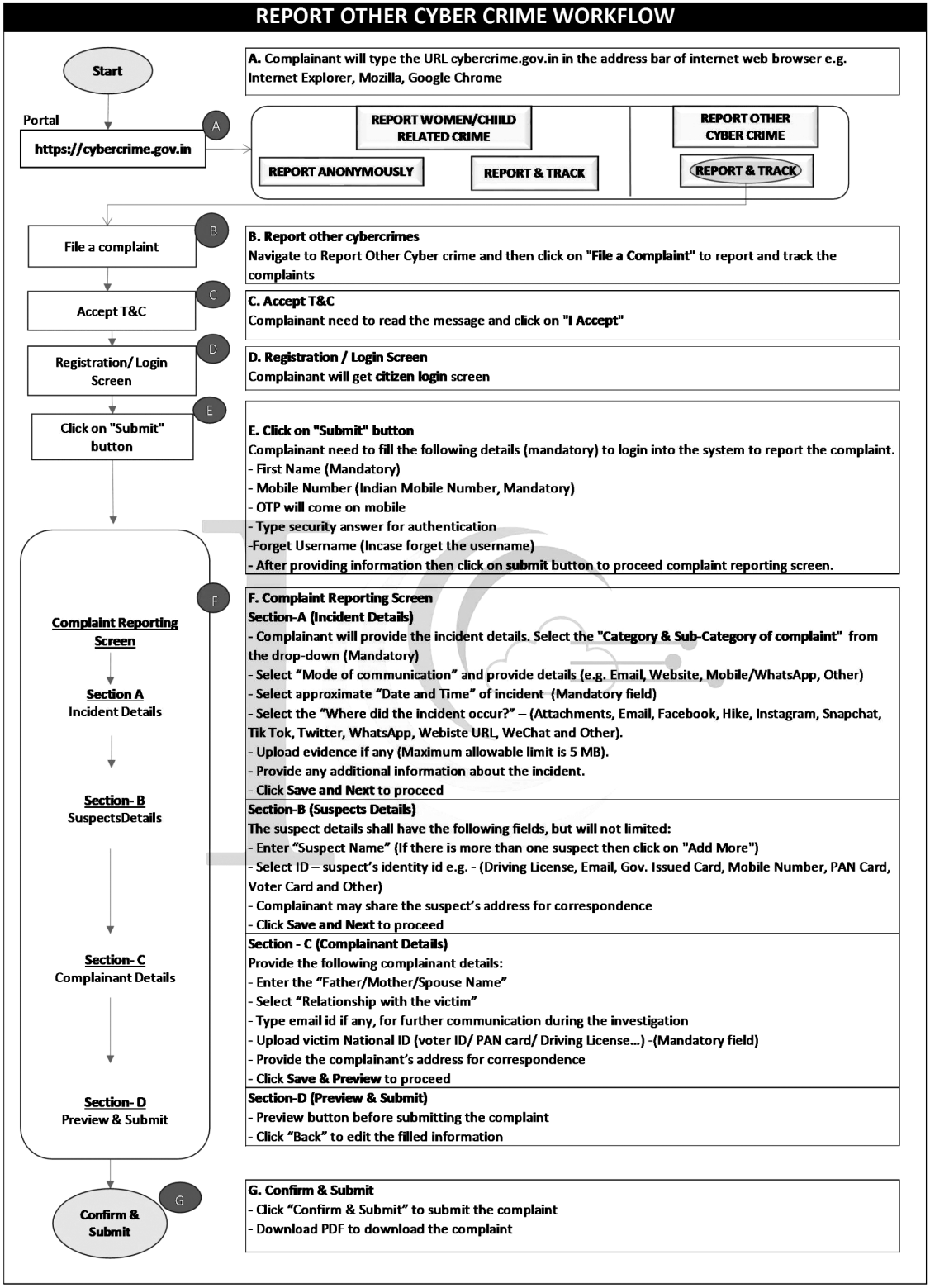
1. Step 1: Go to https://www.cybercrime.gov.in/Accept.aspx.
2. Step 2: Click on 'Report Other Cyber Crimes' on the menu.
3. Step 3: Create 'Citizen login'.
4. Step 4: Click on 'File a Complaint'.
5. Step 4: Read the conditions and accept them.
6. Step 5: Register your mobile number and fill in your name and State.
7. Step 6: Fill in the relevant details about the offence.

It is important to note that one can also report the cyber-crime anonymously.



14 *This portion of the chapter is reproduced from article titled - How is cyber-crime investigation conducted (2020) iPleaders.*

Work Flow for Reporting a Cyber Crime[15]



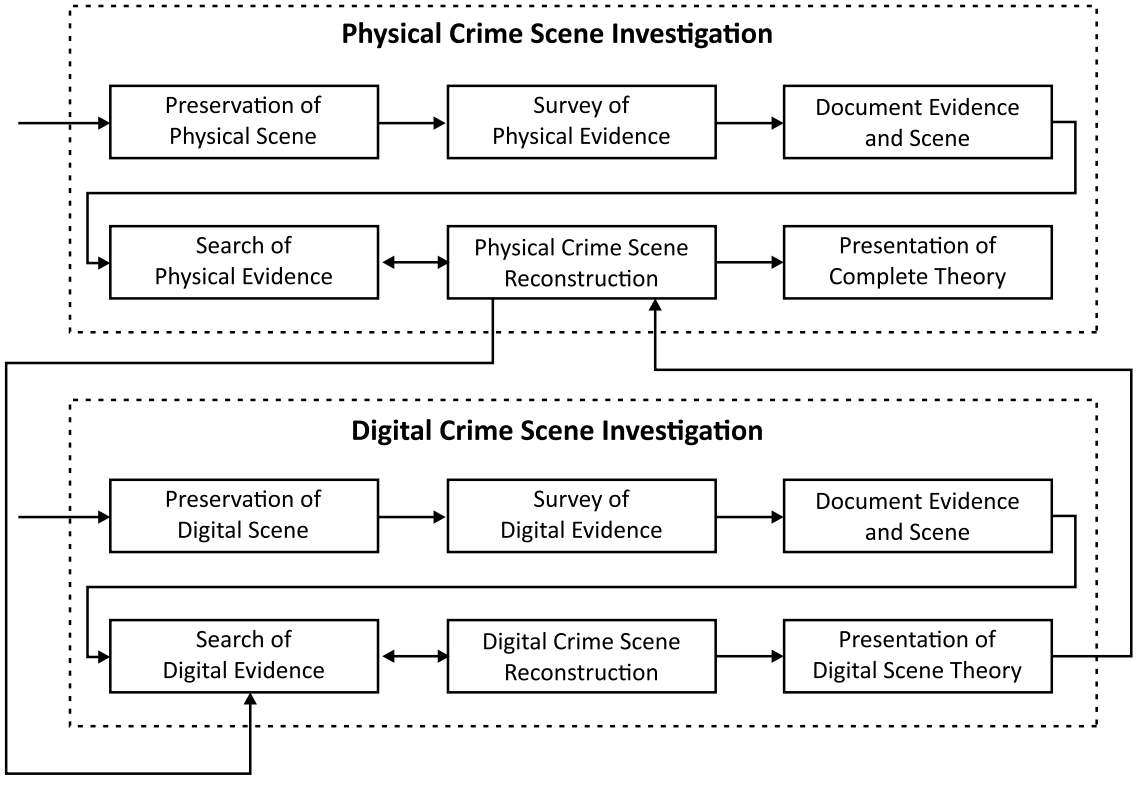
15 Source: https://www.cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf

B. Offline/Physical Reporting of Cyber Crime

One can report a cyber-crime by:

- Filing a written complaint in nearest, any Cyber Cell
- Lodging an F.I.R (First Information Report)
- Filing a complaint at https://www.cybercrime.gov.in/Accept.aspx

After filing of a complaint / F.I.R., the process of investigation, is hereby diagrammatically presented below:



Source: http://www.dynotech.com/articles/images/crimescene.jpg

CASE STUDY

Case Study on Cyber Crime Reporting: SONY.SAMBANDH.COM CASE[14]

India saw its first cybercrime conviction in 2013. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non-Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, according to the cybercrime case study, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested the products to be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency, and the transaction was processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

16. Reproduced from "Important Cyber Law case studies by Cyber Laws and Information Security Advisors".

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint about online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated, and Arif Azim was arrested. Investigations revealed that Arif Azim while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless headphone, in this one of its own kind of cyber fraud case. In this matter, the CBI had evidence to prove their case, and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code - this being the first time that cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court, therefore, released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cybercrimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

State Nodal Officer and Grievance Officer

In case the response has not been appropriate then the complainant can write to State / UT Nodal Officer and Grievance Officer, the details of which can be accessed at https://www.cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx.

INVESTIGATION OF CYBER CRIMES UNDER INDIAN LAWS

For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible. Due to the Information Technology Act, 2000 ("IT Act"), certain provisions of Criminal Procedure Code and the Evidence Act, have been amended. Along with this, certain new regulations had been enforced by the Indian legal system to meet with the need of cyber-crime investigation.

Who can investigate?

The power to investigate the accused in regard to the cyber offences, has been entailed in Section 78 of the IT Act, which says that "notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act". Nevertheless, the IT Act is not sufficient to meet the necessity, therefore the Criminal Procedure Code, 1978 and the Indian Penal Code, 1860, were also amended accordingly to introduce cyber-crime under their ambit. This gives power to the Inspector to register and investigate the cyber-crime as like another crime.

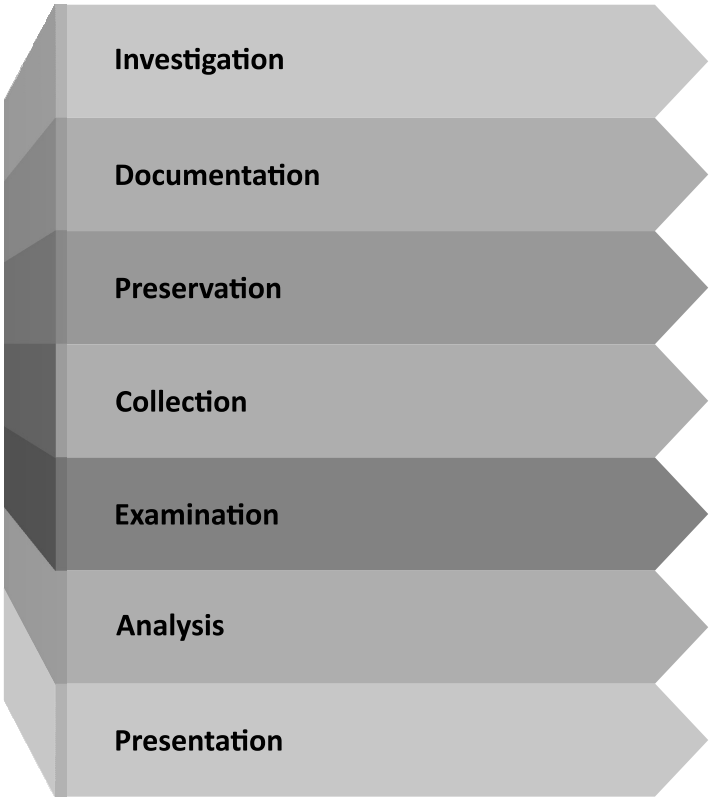
Process of search & arrest

The power of the police office and other officers to enter, search etc. is entailed in Section 80 (1) of the IT Act, which says that, notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of the Inspector or any other officer of the Central Government or State Government authorized by the Central Government in this regard, may enter any public place, search and arrest without warrant any person, who is reasonably suspected of having committed or of committing or about to commit an offence under the IT Act.

Pursuant to Section 80 (2) of the IT Act, any person who is arrested under sub-section (1) by an officer other than a police officer then such officer shall, without any unreasonable delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

Case Study[17]: Steps in Investigation of Cyber-Crime *(Example Data Breach)*

Following are the major steps in conducting the investigation in a cybercrime. Let us understand the same in a cyber-crime of data breach.



Identification: Identify the incident that happened and determine the type of incident, in this case, the incident was a data breach that stolen 500 million identities and got sold in the dark web. The type of the incident could be data breach and data theft. The breach includes personal information like email address, contact information, name etc. The Investigation and/or the forensic examiner should identify the size of the attack (data breach), how the attack happened, method used in stealing the data etc.

The investigation should look for the answers the following questions,

- Check who is involved.
- Find what happened.
- When this happened.
- Where did this incident happen?
- How this incident happens?

By finding the answers to these questions, the investigator can get idea how to proceed with the case. Also, the investigator cannot miss the essential device that might be affected to this investigation. Costs can be estimated

17 See Jayasekara CM (2022) Cyber Crime and Forensic Investigation: Case Study Analysis, Researchgate.

in advance and be prepared for the actual needs. Identify the related evidence such as desktop, smartphones, printers, digital cameras, etc. And try to identify the suspect's characteristics.

There are many factors that may be noticed when identifying,

- Whether there is an administrator that can identify these devices?
- Number of devices that can be involved with this and types of devices.
- If there are any devices that have any remote login capabilities.
- Operating systems that may involve with.
- Power of sources of the suspected devices to operate.

Documentation

Last stage in this identification phase would be documenting every critical thing and revise them if it's necessary. In documentation, we can include, where these devices are found or removed, the information regarding the interview like name ad titles, and the number of devices that are found, where they founded or removed etc.

With this investigator may also continue the investigation process, which may help the business to identify the vulnerabilities and accordingly to adopt modalities to improve their network and security.

Preservation

In this stage, investigator should work in isolation, securing and preserving the physical and digital evidence. This helps to maintain the integrity of the digital evidence and protect the digital evidence from the modifications. Investigator should be responsible and must demonstrate that the evidence should be preserved through all steps in the process like in collection phase, examine phase, analyze phase, etc.

Preservation of the digital and physical evidence should be done by trained and skilled staff members that possess the required techniques and the knowledge of using appropriate tools.

Methods to preserve the Digital Evidence

Following methods need to be considered for preserving the digital evidence by forensic investigator:

- ***Drive Imaging:*** Imaging the drives can help to keep the evidence side and use the images for the analysis. To perform this imagining, professional make a duplicate of the drive with completing the evidence sector by sector.
- ***Making copies of the Evidence:*** Copies of the evidence could also help to retain the evidence. Copies should be encrypted with hash values in the label of the copies so can distinguish from Original. Along with that, critical information like name of the personnel, the date and time and place would be added with. This helps to verify the authenticity and helps to protect the integrity. These hash values could be useful in the court case.
- ***Chain of custody***[18]: When investigator extracts the media from the business and transfer the media if required, then the investigator should document all the transfer on a form called Chain of Custody (CoC).

This stage is crucial because once if the evidence not being preserved properly, this might be invalid in court case. From global perspective, it is to be noted that non-preservation of data and evidences may attract fines under GDPR.

18 Students to Note: Chain of Custody is an important pillar of Digital Evidence and the same is discussed in detail in the later pages of this chapter. See title – Digital Forensics

Collection:

In a cybercrime, there are high probabilities of having certain physical evidences also. Hence along with imaging, duplicating, or copying of the digital evidence, the investigator shall focus on collecting physical evidence also that relates to the crime scene. The investigator shall also collect documents which contain information of the evidence like, name, model, made year etc. Also, the audio recording, photographs, and other visual forms of the crime scenes should be collected and documented. Digital evidence such as desktop, smartphones, printers, digital cameras, etc. should be collected, in addition to the physical evidence. Other relevant evidence may include notes like passwords, suspect's documents, suspect's dairy etc. If the breach initiated within the perimeter, it's required to containment the crime scene, preform the specialized procedures like if the device was ON or OFF when found. If the computer is found OFF, investigator can take the photos of the computer, labelling cables, etc.

For an organized investigation, the investigator should follow some procedures during the collection process such as:

- Separate the electronic evidence from magnetic evidence.
- Keep the evidence in the required temperature.
- Should prepare proper packaging forms like bubble wrap depending on the type of evidence to avoid damages like shock etc.
- Do not store the evidence more than given amount that it should be stored (lifespan of batteries, lifespan of hard disk, etc.).
- Store all acquired evidence in secure manner (e.g.: proper storage)
- Avoid the loss of the dynamic data such as a lists of network connections, personal digital assistants (PDA's), data collected in cell phones, etc.
- During the collection and duplicating the digital evidence, hash values can be used to verify that it is an exact duplicate.

When investigators collecting the digital evidence, they need to care about the volatility and ensure to collect the evidences in, parts in sequence or order of volatility. It's a best exercise to collect the parts from highly volatile to the least volatile.

Order of volatility in a standard document.

- Registers, cache, and peripheral memory (Most Volatile)
- Main physical memory
- Virtual memory
- Network state
- Running processes
- Disk
- Floppies, backup media
- Archival media (CD, USB drives etc.) (Least Volatile)

Examination

This phase would be important for investigator to answer the legal questions and prove the case in court. This involves with in-depth systematic search of evidence that related to the crime scene. The goal of this phase is

to locate, analyze, and extract the digital evidence to refurbish the crime scene, analyze and extract refers, to interpret the data that extracted from the media and placing into the different logical format. Investigation uses lots of techniques while examining and interpret those crucial data into useful formats so that it helps to preserve the integrity and the chain of custody that are required to present in the court. The ways of examination can vary according to the types of devices and the personnel who doing examination must be skilled and trained.

Examination process can be done with two steps:

- Prepare to work on media where evidence files are stored that can be take out and used to prepare documentation for recording all the details of the examination process.
- Preparing a registry can helps to proceed the examination process and track everything by making double check.

Extraction of Data and/or Digital Evidences

Extracting can be done in two different ways such as physical and logical. Physical refers the extraction of the data from the physical level evidence and logical extraction refers the extracting from the file system that present in the drive like active files, etc. After the extraction, they can used to construct the crime scene to get a bigger picture of the incident. Things that might be worth to extract:

- File systems and Applications - using forensic tools, examiner can extract the important metadata like timestamp, directories, authors, etc.
- Registry files – example: in a Windows OS, Windows registry is where contains information like device information, configuration settings, etc.
- Temporary files like cookies, temporary worker/.tamp files, batch files (.bat) etc.
- Unallocated spaces and unused partitions that may expose some important information of deleted files.
- Scanning for the backdoors using tools like THOR and other free open-source forensic tools and monitor the network for data packets seizures.

Analysis:

It is significant to note that all the collected evidences are arranged and analyzed properly, so that specific conclusions can be drawn in solving the cyber-crime. This helps to understand the incident very well by reconstructing the crime scene.

Fundamentally, there are three kinds of ways to reconstruct:

- Temporal Analysis,
- Relational Analysis, and
- Functional Analysis.

Temporal analysis helps to find the factors that are likely to cause this incident and who shall be held responsible for. Relative analysis refers finding the baseline of the crime scene by corresponding the actions of the victim and functional analysis is about finding the actions that caused this.

During this phase, analyst gathering all evidence and present the cruciality of the evidence by using different analysis mechanisms depending on the nature of case.

- *Data hiding analysis*: Recovering the data can be hidden in these digital items could give the examiner a chance to know the significant information that may give the idea about the ownership, etc.

- *Log files analysis*: This analysis uses logs to get the idea of the behavior of system pre crime and find out the possibilities that lead to this crime. Analyzing some important log files like Intrusion Detection system logs and scan the security events are one of examples of log files analysis.
- *Time frame analysis*: The goal of this analysis is to get the idea of when this crime happened with analyzing the events on the digital systems by reviewing the time and data that has embedded into the files as metadata.
- *File analysis*: Analyzing the metadata that embedded in the files and the applications and other information may contain some hints leading to the crime scene like getting idea of the behavior of the user.

Presentation

This is final stage of any investigation which presents the results containing conclusions and summary of the investigation process. The information that provides with this presentation must be clear and precise so the business and victims can understand very well and get better knowledge how to avoid such another destruction in future.

In the presentation, any documents that had taken in each step in the process should be engaged with the audience. Reporting is the significant part of the presentation. A professionally written and clear report can increase the chances to prove the case very well in the court and win the case. In a good report should include the case logs, videos and other media, technical report, non-technical report, Chain of Custody (CoC), etc.

Also more importantly, the report should provide the aims and objectives, detailed steps of every log and technical and non-technical qualifications of the personnel who conducts the process would add more information to presentation.

Last but not the least, investigator and its team should work with the business/victim closely to understand the crime very well and provide the business/victims with all information on how crime committed, their probable loss and how the security system shall be implanted to protect the victim from cyber-crimes. For example, in this case, investigators shall inform the business/victim with the risks involved in the loss/beach of data. With such information the business can take suitable legal step for saving themselves the huge financial loss. However, the business should be aware of the steps that needs to avoid another data breach in the future and protect the customers from further destructions. Also, it is important that business should have tools to briefly address the destructions like data breach to get the depth and scope of the attack. One of the best steps to avoid is to implement more advanced security frameworks involving with the policies and regulations so business can be prepared to avoid attacks in future.

Some of the common cyber-crimes of 2023-2024[19]

- **FedEx Scam**

  How it works: It all starts when someone gets a call from a stranger pretending to be from 'FedEx.' The caller says a package in the person's name, heading to Macau or another country, got seized by Mumbai customs for having illegal stuff. After that, the victim is linked to a "police officer," often from the Mumbai Crime Branch or Anti-Narcotics Unit.

  Protect yourself: Verify the legitimacy of such messages/calls by contacting FedEx directly using official contact information.

- **YouTube Like Scam**

  How it works: Criminals are using WhatsApp and Telegram to approach potential victims with offers for part-time work from home or part-time jobs. In these fraudulent schemes, scammers are enticing users to engage with videos on YouTube by liking and subscribing.

19. Reproduced from Cyber Digest (2024), Indian Cyber Crime Coordination, Ministry of Home Affairs. Available at https://i4c.mha.gov.in/cyber_digest/jan_2024/I4C%20Daily%20Digest-%2029.01.2024%20.pdf

Protect yourself: Avoid clicking on links in suspicious messages. Verify notifications directly on the official YouTube website or app.

- **Online Shopping Scam**

  How it works: Fraudsters make fake websites that seem like real online stores. These sites usually tempt people with attractive discounts on popular products to trick them. When people enter their payment details, the scammers take their money and vanish.

  Protect yourself: Stick to well-known online stores, check reviews, and be wary of deals that appear too good to be true. Opt for secure payment options, and ensure the website has a secure connection before making any purchases.

- **Identity Theft Scam**

  How it works: Identity theft occurs when someone dishonestly obtains another person's important personal and financial information. They then use this information for various fraudulent activities, posing a significant risk to the victim.

  Protect yourself: Create strong and unique passwords, turn on two-factor authentication, be careful about sharing personal details on the internet, and routinely keep an eye on your accounts for any unusual activities.

- **Scholarship and Grant Scam**

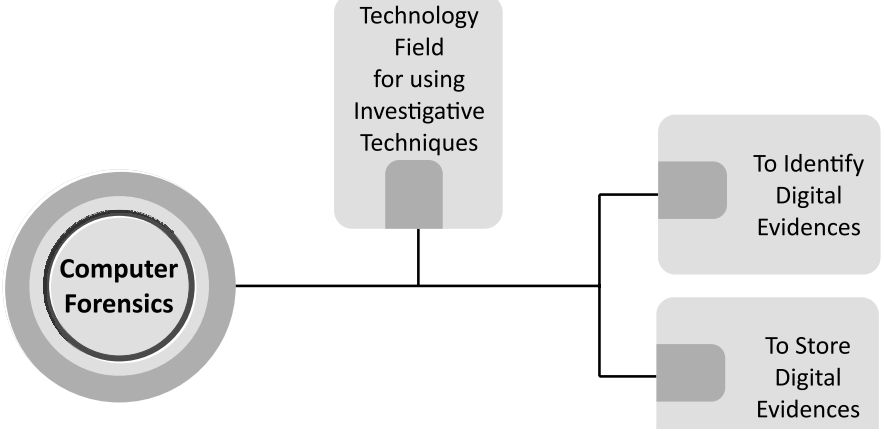
  How it works: Be wary of scammers pretending to be organizations offering scholarships or grants. They might ask for upfront fees or personal information without any intention of actually providing financial assistance.

  Protect yourself: When searching for scholarships, make sure to thoroughly research your options, confirm the legitimacy of organizations, and be cautious if asked for payment or sensitive information. Legitimate scholarships usually don't involve upfront fees.

COMPUTER FORENSICS AND DIGITAL EVIDENCE

What are Computer Forensics?

In general parlance, computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device.

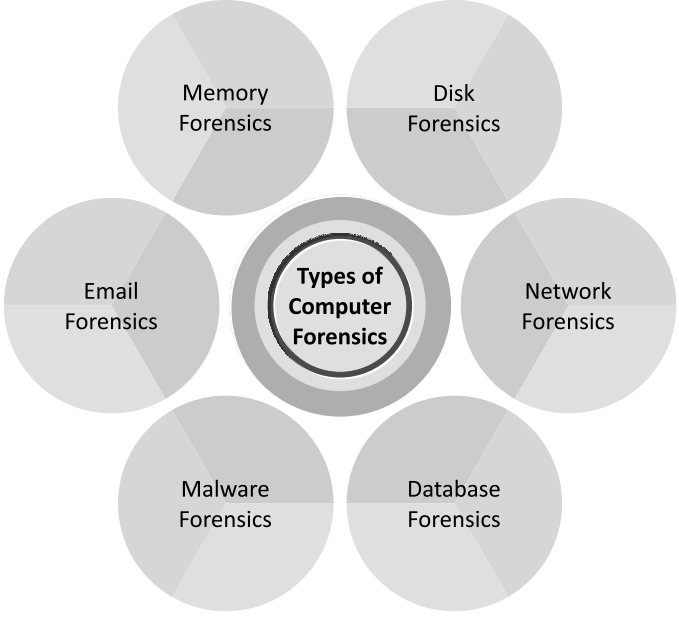


Often, computer forensics is used to uncover evidence that could be used in a court of law. Computer forensics also encompasses areas outside of investigations. Sometimes professionals in this field might be called upon to recover lost data from drives that have failed, servers that have crashed or operating systems that have been reformatted.

Use of Computer Forensics

Computer forensics is primarily used for two separate purposes, investigation and data recovery. To be precise, it can be called that computer forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Types of Computer Forensics[20]



Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.

- ***Network Forensics:*** It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- ***Database Forensics:*** It deals with the study and examination of databases and their related metadata.
- ***Malware Forensics:*** It deals with the identification of suspicious code and studying viruses, worms, etc.
- ***Email Forensics:*** It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- ***Memory Forensics:*** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analysing it for further investigation.
- ***Mobile Phone Forensics:*** It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.

20 Source: Introduction of Computer Forensics (2023) Geeksforgeeks.

Role of Computer Forensics

- ***Identification:*** Identifying what evidence is present, where it is stored, and how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- ***Preservation:*** Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
- ***Analysis:*** Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- ***Documentation:*** A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- ***Presentation:*** All the documented findings are produced in a court of law for further investigations.

COMPUTER FORENSICS VIS-A-VIS CYBER SECURITY

Both computer forensics and cyber security deal with criminals and computers, hence many a times they are considered rather similar. Despite this initial similarity, the function of computer forensics and cyber security greatly differs from each other.

To be precise, cyber security is majorly concerned with providing security/defence against the possible cyber-crime/cyber threat. Cyber security aims to build networks and systems that are secure from potential attackers. Sometimes hacking is also used to test networks, systems or the networks of a client to find areas of weakness and bolster them.

On the other hand, the computer forensics comes into picture when a cyber-crime is already committed and hence cyber forensic focuses largely on data recovery. The data recovered is often used as evidence in criminal trials, but sometimes is recovered for companies after a data loss incident. Additionally, the criminals that computer forensics professionals investigate are not always cybercriminals. Because almost everyone uses a computer, there is often valuable information on their personal device that can contribute to an investigation.

Investigations vide Computer Forensics

Computer forensics can be an essential facet of modern investigations. When a crime is committed and an investigation is started, one of the more common places to look for clues is the computer or cell phone of a suspect. This is where a computer forensics professional enters the picture.

When a suspect has been identified and their personal computer or cell phone taken into evidence, a computer forensics professional goes searching for data that is relevant to the investigation. When searching for information, they need to be careful to follow detailed procedures that allow their findings to be used as evidence. The information they uncover, whether it be documents, browsing information or even metadata, may then be used by prosecution to create a compelling case against the suspect.

- ***Procedure***

  The procedure starts with identifying the devices used and collecting the preliminary evidence on the crime scene. Then the court warrant is obtained for the seizure of the evidence which leads to the seizure of the evidence. The evidence are then transported to the forensics lab for further investigations and the procedure of transportation of the evidence from the crime scene to labs are called chain of custody. The evidence are then copied for analysis and the original evidence is kept safe because analysis are always done on the copied evidence and not the original evidence.

The analysis is then done on the copied evidence for suspicious activities and accordingly, the findings are documented in a nontechnical tone. The documented findings are then presented in a court of law for further investigations.

- ***Data Recovery***

  Aside from working to collect evidence, computer forensics professionals can also work in data recovery. When it comes to data recovery, forensics professionals can take broken hard drives, crashed servers and other compromised devices and retrieve the data that was previously lost. This is valuable for anyone who has lost important data outside of uncovering criminal evidence, such as businesses who have experienced a system crash.

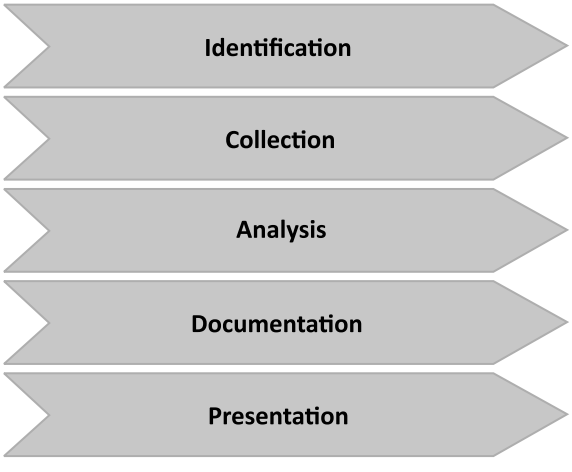
DIGITAL FORENSICS/DIGITAL EVIDENCES[21]

Digital forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation.

In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences. It includes the area of analysis like storage media, hardware, operating system, network and applications.

Steps in Digital Forensics

It consists of following five (s) steps:



21 Reproduced from Geeks for Geeks on Digital Forensics in Information Security, June 16, 2022.

Identification of Evidence: It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.

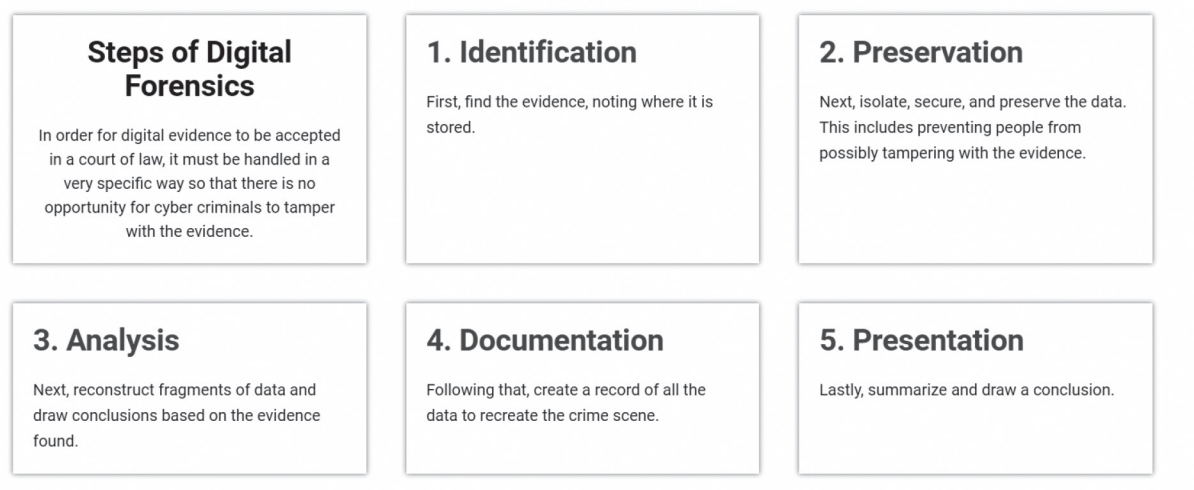
Collection: It includes preserving the digital evidences identified in the first step so that they don't degrade to vanish with time. Preserving the digital evidences is very important and crucial.

Analysis: It includes analysing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.

Documentation: It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.

Presentation: It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

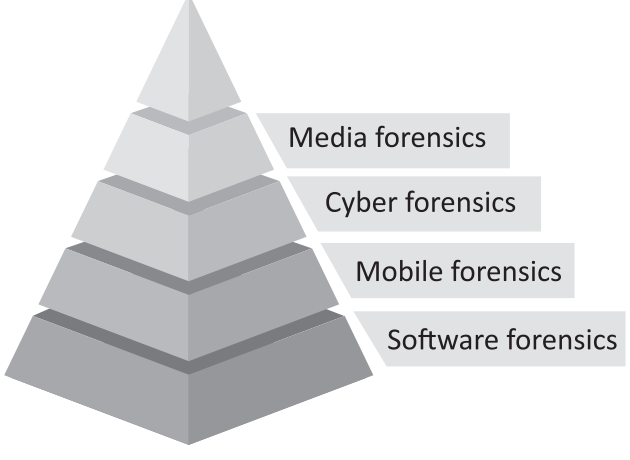
For the purpose of acceptance of Digital Evidence in the court of law, the EC Council has identified following steps of Digital Forensics/Evidence.



Source: https://www.eccouncil.org/what-is-digital-forensics/

Branches of Digital Forensics:

Following are the main branches of digital forensics:



Media forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidences during the investigation process.

Cyber forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a cybercrime.

Mobile forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime committed through a mobile device like mobile phones, GPS device, tablet, laptop.

Software forensics: It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime related to software only.

Steps in Preserving Digital Evidence

(Source: Geeks for Geeks)

Following critical steps that need to be followed to prevent loss of data before bringing to the forensic experts. Time is highly important in preserving digital evidence.

- Do not change the current state of the device: If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Call a forensics expert before doing anything.
- Power down the device: In the case of mobile phones, if it is not charged, do not charge it. In case, the mobile phone is ON power it down to prevent any data wiping or data overwriting due to automatic booting.
- Do not leave the device in an open area or unsecured place: Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
- Do not plug any external storage media in the device: Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
- Do not copy anything to or from the device: Copying anything to or from the device will cause changes in the slack space of the memory.
- Take a picture of the piece of the evidence: Ensure to take the picture of the evidence from all the sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
- Make sure you know the PIN/ Password Pattern of the device: It is very important for you to know the login credentials of the device and share it with the forensic experts, for them to carry their job seamlessly.
- Do not open anything like pictures, applications, or files on the device: Opening any application, file, or picture on the device may cause losing the data or memory being overwritten.
- Do not trust anyone without forensics training: Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.
- Make sure you do not shut down the computer, if required Hibernate it: Since the digital evidence can be extracted from both the disk drives and the volatile memory. Hibernation mode will preserve the contents of the volatile memory until the next system boot.

DIGITAL FORENSICS - CHAIN OF CUSTODY[22]

The digital evidence and digital chain of custody are the backbones of any action taken by digital forensic specialists. Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases. Each step in the chain is essential and in case any step is missed, then the evidence may be rendered inadmissible in the court of law. Thus, we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.

What the Chain of Custody (under the perspective of Digital Cyber Forensics)

The chain of custody in digital cyber forensics is also known as the paper trail or forensic link, or chronological documentation of the evidence.

- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
- It demonstrates trust to the courts and to the client that the evidence has not tampered.

Digital evidence is acquired from the myriad of devices like a vast number of Internet of Things (IoT) devices, audio evidence, video recordings, images, and other data stored on hard drives, flash drives, and other physical media.

Significance of maintaining Chain of Custody

A. Importance to Examiner:

- To preserve the integrity of the evidence.
- To prevent the evidence from contamination, which can alter the state of the evidence.

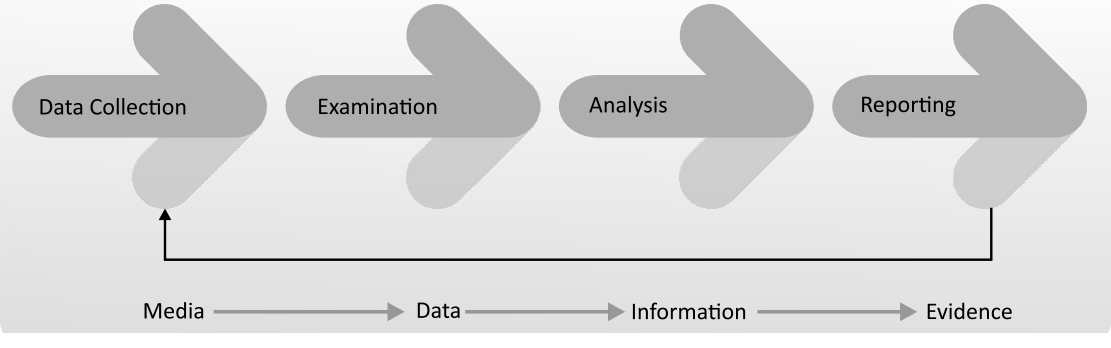
In case you obtained metadata for a piece of evidence but unable to extract any meaningful information from the metadata. In such a case, the chain of custody helps to show where possible evidence might lie, where it came from, who created it, and the type of equipment used. This will help you to generate an exemplar and compare it to the evidence to confirm the evidence properties.

B. Importance to the Court:

If not preserved, the evidence submitted in the court might be challenged and ruled inadmissible.

Process of Chain of Custody:

In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid any probability that the evidence has been compromised in any way.



Source: geeksforgeeks

22 *Reproduced from Article titled – Chain of Custody of Digital Forensics, Geekforgeeks.org*

- *Data Collection:* This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.
- *Examination:* During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
- *Analysis:* This stage is the result of the examination stage. In the analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.
- *Reporting:* This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:
  - Statement regarding Chain of Custody.
  - Explanation of the various tools used.
  - A description of the analysis of various data sources.
  - Issues identified.
  - Vulnerabilities identified.
  - Recommendation for additional forensics measures that can be taken.

The CoC form must be kept up-to-date. This means every time the best evidence is handled off, the chain of custody form needs to be updated.

Procedure to establish the Chain of Custody

In order to assure the authenticity of the chain of custody, a series of steps must be followed. It is important to note that the more information forensic expert obtains concerning the evidence, the more authentic is the created chain of custody. Following procedure is trailed according to the chain of custody for electronic devices:

- Save the original material.
- Take photos of the physical evidence.
- Take screenshots of the digital evidence.
- Document date, time, and any other information on the receipt of the evidence.
- Inject a bit-for-bit clone of digital evidence content into forensic computers.
- Perform a hash test analysis to authenticate the working clone.

Documentation/Authentication of Chain of Custody:

During the process of examination, it is important to document all such information that is beyond the scope of current legal authority and later brought to the attention of the case agent. A comprehensive report must contain following sections:

- Identity of the reporting agency.
- Case identifier.
- Case investigator.
- Identity of the submitter.
- Date of receipt.
- Date of report.

- Descriptive list of items submitted for examination: This includes the serial number, make, and model.
- Identity and signature of the examiner.
- Brief description of steps taken during the examination: For example- string searches, graphics image searches, and recovering erased files.
- Results.

SECURITY AUDIT[23]

In general, security audit is a systematic evaluation of the security of a company's information system by measuring how well it adheres to an established set of criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.

Security audits are often used to determine compliance with regulations such as Information Technology Act, 2000 and other rules and regulations applicable on the IT environment of a particular organization. It majorly specifies how organizations have dealt with the information and data available in the organization.

Meaning of Audit

In order to catch the glimpse of security audit in totality, it also become significant to know and understand the meaning of Audit.

Audit in general refers to the examination or inspection of various books of accounts by an auditor followed by physical checking of inventory to make sure that all departments are following documented system of recording transactions. It is done to ascertain the accuracy of financial statements provided by the organization.[24]

Audit can be done internally by employees or heads of a particular department and externally by an outside firm or an independent auditor. The idea is to check and verify the accounts by an independent authority to ensure that all books of accounts are done in a fair manner and there is no misrepresentation or fraud that is being conducted.

All the public listed firms have to get their accounts audited by an independent auditor before they declare their results for any quarter.

As per *English Oxford Dictionary*, Audit means an official inspection of an organization's accounts, typically by an independent body. It also states a word of cautions that many a times, audits are not expected to detect every fraud.

Cambridge Dictionary refers that Audit is a systematic process to make an official examination of the accounts of a business and produce a report.

English Oxford Dictionary	***Cambridge Dictionary***
Audit means - ● An official inspection of an organization's accounts, ● Typically, by an independent body, ● It also states a word of cautions that many a times, audits are not expected to detect every fraud.	Audit refers as - ● Systematic process, ● To make an official examination of the accounts of a business, and ● To produce a report.

With the analysis of these definitions, it is apt to state that an audit is a systematic and independent examination of books, accounts, statutory records, documents and vouchers of an organization to ascertain how far the financial statements as well as non-financial disclosures present a true and fair view of the concern.

It also attempts to ensure that the books of accounts are properly maintained by the concern as required by law.

23 Students to note: As one of the major purposes of this paper is to understand law and practice related to Cyber Security, hence the Security Audit herein refers to cyber security audit in specific.

24 Definition of Audit, The Economic Times.

Significance of Security Audit

As discussed above that audit is conducted to reflect the true and fair value of certain concern, hence the security audit implies the true and fair value of security of computer, computer network, information and data. To be precise, security audits will help protect critical data, identify security loopholes, create new security policies and track the effectiveness of security strategies. There are several reasons to do a security audit and collectively include these six goals:

- Identify security problems and gaps, as well as system weaknesses.
- Establish a security baseline that future audits can be compared with.
- Comply with internal organization security policies.
- Comply with external regulatory requirements.
- Determine if security training is adequate.
- Identify unnecessary resources.

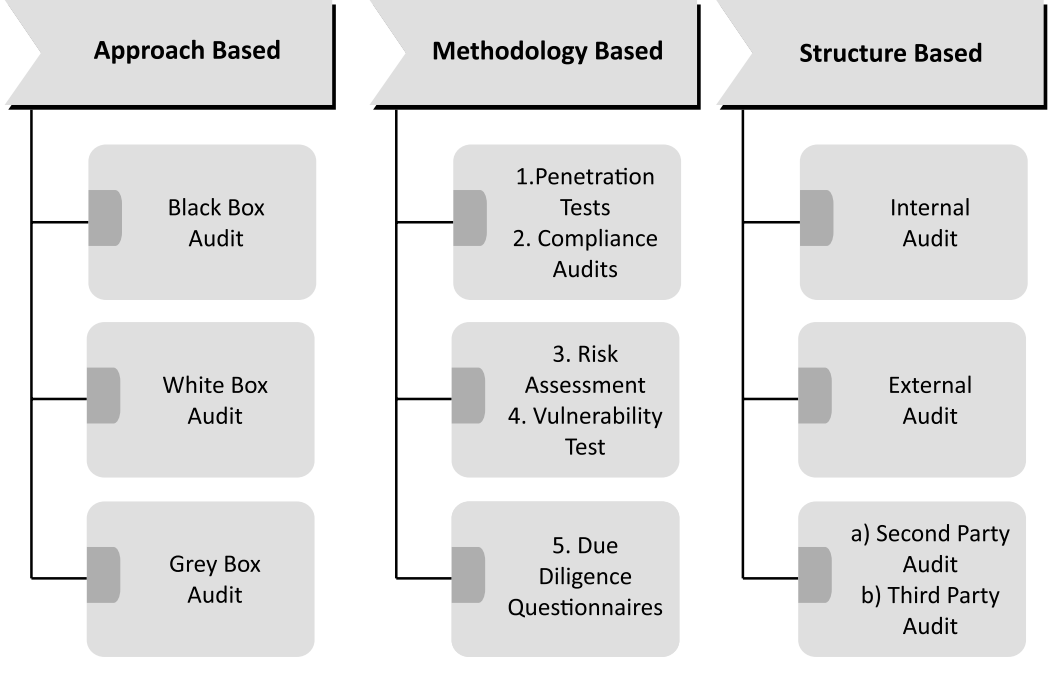
Advantages of Security Audit

As mentioned above, the security audit reveals underlying vulnerabilities and security risks in an organization's information technology assets. The identifying risks through security audit has following advantages:

- Weighs the security structure and protocols of the organization and helps it to define a security standard for organization with the audit results.
- Mitigates hacker-risks by discovering potential hacker entry points and security flaws well in advance.
- Verifies how compliant IT infrastructure is with top regulatory bodies, regulations, laws and rules applicable to certain sector/service. Accordingly helps the organization to stay compliant in accordance.
- Finds lag in organization's security training and awareness and helps you make informed decisions towards its betterment.

Types of Security Audit

Different types of audits based on approach, methodology and structure can be discussed as under.



Approach Based

- **Black Box Audit:** In this type of security audit, the auditor only knows about the info that is publicly available regarding the organization that is to be audited.
- **White Box Audit:** In this type of security audit, the auditor is provided with detailed info (i.e. source code, employee access, etc.) regarding the organization that is to be audited.
- **Grey Box Audit:** In grey box audit, the auditor is provided with some info, to begin with, the auditing process. This info can also be gathered by the auditors themselves but is provided to save time.

Methodology Based

- **Penetration Tests:** The auditor tries to break into the organization's infrastructure.
- **Compliance Audits:** Only certain parameters are checked to see if the organization is complying with security standards.
- **Risk Assessments**: An analysis of critical resources that may be threatened in case of a security breach.
- **Vulnerability Tests*:*** Necessary scans are performed to find possible security risks. Many false positives may be present.
- **Due Diligence Questionnaires:** Used for an analysis of existing security standards in the organization.

Structure Based Audit

Security audits come in two forms, internal and external audits that involve the following procedures:

- **Internal audits:** In these audits, a business uses its own resources and internal audit department. Internal audits are used when an organization wants to validate business systems for policy and procedure compliance.
- **External audits:** With these audits, an outside organization is brought in to conduct an audit. External audits are also conducted when an organization needs to confirm it is conforming to industry standards or government regulations.

There are *two subcategories of external audits: Second and Third Party Audits*. Second Party audits are conducted by a supplier of the organization being audited. Third Party audits are done by an independent, unbiased group, and the auditors involved have no association with the organization under audit.

Steps – On Conducting Security Audit:

Step 1: Preliminary Audit Assessment

This stage is used to assess the current technological maturity level/status of the company and helps to identify the required time, cost and scope of an audit. Firstly, one need to identify the minimum-security requirements, which are as below:

- Security policy and standards
- Organizational and Personal security
- Communication, Operation and Asset management
- Physical and environmental security
- Access control and Compliance
- IT systems development and maintenance

- IT security incident management
- Disaster recovery and business continuity management
- Risk management.

Step 2: Planning & Preparation

The auditor should plan a company's audit based on the information found in previous step. Planning an audit helps the auditor obtain sufficient and appropriate evidence for each company's specific circumstances. It helps predict audit costs at a reasonable level, assign the proper manpower and time line and avoid misunderstandings with clients.

An auditor should be adequately informed about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes. To adequately determine whether the client's goal is being achieved, the auditor should perform the following before conducting the review:

- Meet with IT management to determine possible areas of concern
- Review the current IT organization chart
- Review job descriptions of data center employees
- Research all operating systems, software applications, and data center equipment operating within the data center
- Review the company's IT policies and procedures
- Evaluate the company's IT budget and systems planning documentation
- Review the data center's disaster recovery plan.

Step 3: Establishing Audit Objectives

In the next step, the auditor outlines the objectives of the audit after that conducting a review of a corporate data center takes place. Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks. After thorough testing and analysis, the auditor is able to adequately determine if the data center maintains proper controls and is operating efficiently and effectively.

Following is a list of objectives the auditor should review:

- Personnel procedures and responsibilities, including systems and cross-functional training.
- Change management processes are in place and followed by IT and management personnel.
- Appropriate backup procedures are in place to minimize downtime and prevent loss of important data.
- The data center has adequate physical security controls to prevent unauthorized access to the data center.
- Adequate environmental controls are in place to ensure equipment is protected from fire and flooding.

Step 4: Performing the Review

The next step is collecting evidence to satisfy data center audit objectives. This involves traveling to the data center location and observing processes and within the data center. The following review procedures should be conducted to satisfy the pre-determined audit objectives:

- *Data Center Personnel* – All data center personnel should be authorized to access the data center (key cards, login ID's, secure passwords, etc.). Data center employees are adequately educated about data center equipment and properly perform their jobs. Vendor service personnel are supervised when doing

work on data center equipment. The auditor should observe and interview data center employees to satisfy their objectives.

- *Equipment* – The auditor should verify that all data center equipment is working properly and effectively. Equipment utilization reports, equipment inspection for damage and functionality, system downtime records and equipment performance measurements all help the auditor determine the state of data center equipment. Additionally, the auditor should interview employees to determine if preventative maintenance policies are in place and performed.
- *Policies and Procedures* – All data center policies and procedures should be documented and located at the data center. Important documented procedures include data center personnel job responsibilities, back up policies, security policies, employee termination policies, system operating procedures and an overview of operating systems.
- *Physical security / environmental controls* – The auditor should assess the security of the client's data center. Physical security includes bodyguards, locked cages, man traps, single entrances, bolted-down equipment, and computer monitoring systems. Additionally, environmental controls should be in place to ensure the security of data center equipment. These include Air conditioning units, raised floors, humidifiers and uninterruptible power supply.
- *Backup procedures* – The auditor should verify that the client has backup procedures in place in the case of system failure. Clients may maintain a backup data center at a separate location that allows them to instantaneously continue operations in the instance of system failure.

Step 5: Preparing the Audit Report

After the audit examination is completed, the audit findings and suggestions for corrective actions can be communicated to responsible stakeholders in a formal meeting. This ensures better understanding and support of the audit recommendations. It also gives the audited organization an opportunity to express its views on the issues raised.

Writing a report after such a meeting and describing where agreements have been reached on all audit issues can greatly enhance audit effectiveness. Exit conferences also help finalize recommendations that are practical and feasible.

Step 6: Issuing the Review Report

The audit review report should summarize the auditor's findings and be similar in format to a standard review report. The review report should be dated as per the completion of the auditor's inquiry and procedures. It should state what the review entailed and explain that a review provides only "limited assurance" to third parties.

Typically, a security audit review report consolidates the entirety of the audit. It also offers recommendations surrounding proper implementation of physical safeguards and advises the audited organization on appropriate roles and responsibilities of its personnel. Generally, the audit report include:

- The auditors' procedures and findings.
- The auditors' recommendations.
- Objective, scope, and methodologies.
- Overview/conclusions.

The security audit report may optionally include rankings of the security vulnerabilities identified throughout the performance of the audit and the urgency of the tasks necessary to address them. Rankings like "high", "low", and "medium" can be used to describe the imperativeness of the tasks.

Concluding Remarks

The above discussion confirms the signification of security audit for fortifying the IT infrastructure of a company as well as the minimize the probability of cyber-attacks. A well conducted security audit ensures the following:

- Identify potential threats including the loss of data, equipment or records through natural disasters, malware or unauthorized users.
- Evaluate security and risks. Apart from assessing the risk of each of the identified threats happening, it also guides on how well the organization can defend against them.
- Determine the needed controls by Identifying what security measures must be implemented or improved to minimize risks.
- Helps the organization in ensuring compliance with the applicable laws and regulations related to the IT infrastructure and requirement of the company.

Hence, it will be apt to state that periodic security audit is directly proportionate to the growth of the organization.

Cyber Security Audit: A Snapshot[25]

A cybersecurity audit involves a comprehensive analysis and review of your IT infrastructure. It detects vulnerabilities and threats, displaying weak links and high-risk practices.

Significant benefits of IT security audits are:

- Risk assessment and vulnerability identification
- Strengthened security measures
- Compliance with regulations and standards
- Incident response preparedness
- Safeguarding sensitive data and customer trust
- Proactive threat detection and prevention

Cybersecurity audits ensure a 360-degree in-depth audit of your organization's security posture. They aim to identify vulnerabilities, risks, and threats that may affect the organization. These audits cover various areas, including:

- **Data Security** – involves reviewing network access control, encryption use, data security at rest, and transmissions.
- **Operational Security** – involves a review of security policies, procedures, and controls.
- **Network Security –** a review of network & security controls, anti-virus configurations, security monitoring capabilities, etc.
- **System Security** – This review covers hardening processes, patching processes, privileged account management, role-based access, etc.
- **Physical Security** – a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

Beyond these, a cybersecurity audit can also cover cybersecurity risk management, cyber risk governance, training & awareness, legal, regulatory & contractual requirements, technical security controls, business continuity & incident management, and third-party management.

25. Reproduced from Chinnaswamy Vinugayathri (2023), What Is Cyber Security Audit and How Is It Helpful for Your Business? Indusface. Available at https://www.indusface.com/blog/what-is-cyber-security-audit-and-how-it-is-helpful-for-your-business/#:~:text=A%20cyber security%20audit%20involves%20a,Risk%20assessment%20and%20vulnerability%20identification

Source: https://blueteamresources.in/cyber-security-audit-checklist/

Cyber Attacks in Middle East

With the Middle East Conflict at a very heated moment between bordering countries Pro-Palestinian and Pro-Israel Cyber Groups have been launching an offensive against websites and mail services used by the political sectors the opposing groups show support for. The attacks had been reported by the NIPC (National Infrastructure Protection Centre) in October of 2000 to U.S. Officials. The attacks were a volley of e-mail floods, DoS attacks, and Ping flooding of such sites as the Israel Foreign Ministry, Israeli Defense Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah.[26]

India and Pakistan Conflict

As tensions between the neighbouring regions of India and Pakistan over Kashmir grew over time, Pro-Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Just prior to and after the September 11th attacks, it is believed that the sympathizers of Pakistan began their spread of propaganda and attacks against Indian Internet based communities. Groups such as G-Force and Doctor Nuker have defaced or disrupted service to several major entities in India such as the Zee TV Network, The India Institute of Science and the Bhabha Atomic Research Center which all have political ties. The Group, Pakistani Hackerz Club also went as far as to target the United States Air Force Computing Environment and the Department of Energy's Website.[27]

Retribution by China

In May 1999 the accidental bombing of a Chinese embassy in Yugoslavia by U.S. Bombers, led to a massive website defacement and email bombardment attack on American companies and agencies. Pro Chinese hackers and political groups executed the attacks to gain sympathy for Chinese cause. US Government sites such as the US department of energy and the interior and the National Park Service were all hit and had website defaced along with the White House website. The sites were downed for three days by continual e-mail bombing. Although the attack was rather random and brief and affected a small number of U.S. sites, the effects could have been worse.[28]

Cyber attack by Tamil Tigers

In 1998, with surges of violence committed in Sri Lankan over Several years, attacks in cyber-space were the next area to target. The group known as the Tamil Tigers, a violent guerrilla organization bombarded Sri Lankan embassies with over 800 e-mails a day. This was carried out over a two week period. The attack by the e-mail message conveyed the message, "We are the Internet Black Tigers and we are doing this to disrupt your communications." After the messages created such major disruption the local Intelligence authorities were dispatched to investigate. The authorities declared the attack as the first known attack on the Sri Lankan by the terrorists on any computer system in the nation.[29]

Yugoslavia Conflict

When NATO[30] air strikes hit Former republic of Yugoslavia in Kosovo and Serbia, NATO web servers were

26. "Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection C enter – October 26, 2000 and also at http://www.nipc.gov/warnings/assessments/2000/00-057.htm and https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber- assault-931 (Accessed on 14th February, 2016)

27. "Cyber Attacks during the War on Terrorism" India/Pakistan Conflict, Institute for Security Technology Studies - Dartmouth College Vatis, Michael A - September 22, 2001. also at http://www.ists.dartmouth.edu/docs/cyber_a1.pdf (Accessed on 14th February, 2016)

28. Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001. Also available at https://www.sans.org/reading-room/whitepapers/threats/conventional- terrorismthe-cyber-assault-931 (Accessed on 14th February, 2016)

29. Cyber Terrorism – "Testimony before the Special Oversight Panel oil Terrorism"- Dorothy E Denning - May 23, 2000. also at https://www.sans.org/reading- room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931 (Accessed on 14th February, 2016)

30. The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its

subjected to sustained attacks by hackers employed by the Yugoslav military. All NATO's 100 servers were subjected to "ping saturation", Distributed Denial Of service assaults and bombarded with thousands of e-mails, many containing viruses. The attacks on NATO servers coincided with numerous website defacements of American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of Yugoslavia. These attacks cause serious disruption of NATO communications infrastructures.

Cyber Attack on Estonia

The small Baltic country of Estonia was cyber-attacked from Russia. Ever since the government of the Baltic state decided to remove a war memorial to the Red Army from a square in the capital, Tallinn, Russian outrage has ensued. This took the form of demonstrations and even riots. But then something extraordinary happened: quickly, and wholly without warning, the whole country was subjected to a barrage of cyber-warfare, disabling the websites of government ministries, political parties, banks and newspapers. Techniques normally employed by cybercriminals, such as huge remotely- controlled networks of hijacked computers, were used to cripple vital public services. NATO has sent its top cyber-terrorism experts to Tallinn, with western democracies caught on the hop over the implications of such an attack. The Estonian defence ministry said: "We've been lucky to survive this. If an airport, bank or state infrastructure is attacked by a missile, it's clear war but if the same result is done by computer's, then what do you call It. IS It a state of war? These questions must be addressed." Estonia has blamed Russia, predictably enough; which, if true, would mean this is the first cyber attack by one sovereign state upon another. The Estonian attacks were more likely to be the work of angry young Russian hackers working alone than any sort of organised blitz by the Kremlin. But either way, the implications are serious.[31]

Sony PlayStation Network, Microsoft's Xbox Live network case

In this case the confidential data of the employees and their families has been leaked in 2014. The company has faced loss in revenue due to movies being leaked, sensitive employee information was disclosed including their salaries and social security numbers, and executive emails were publicized. The attack was hatched by the Lizard Squad, an organization that refers to itself as a cyber-terrorist. Then they launched a massive Distributed denial of service attack against Sony's PlayStation Network and Microsoft's Xbox Live networks. They followed up these disruptions with an attack against the Tor Project, a network of virtual tunnels that allow people and groups to improve their privacy and security on the Internet and after that North Korea attacked the network infrastructure and network has gone down for almost Ten hours due to the attack affecting the lives of millions. Due to that many think that it is an act by the US government. However it is not but they manage to create doubts regarding purchasing the product among the consumer and people regarding the multinational companies. The Motive behind these cyber terrorist attacks is collateral damage involved and the obvious ties to geo-political situations that we see in so many attacks. The Current President Barack Obama of United States has said that "cyber- terrorism is perhaps one of the greatest threats against the U.S. today. Unfortunately, the attacks are not only here to stay, but given the utter reliance on the Internet today, they are likely to grow in a very serious manner".[32]

Indian Law & Cyber Terrorism

It is the easiest way in modern scenario is attack a country is through cyber network. India is in developing stage and the impact of cyber attack on Indian infrastructure and communication is going to be immense, because India now heavily depends on computers and information Technology.

---

member states agree to mutual defense in response to an attack by any external party. (Source Wikipedia accessed on 16th February, 2016)

31. See "Attack of the cyber terrorists" by MICHAEL HANLON Available at: http://www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html (Accessed on 16th February, 2016)

32. See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/ (Accessed on 16th February, 2016)

There is need of series of innovative laws and global standards on dealing with cyber crimes. The Computer/ Internet is changing the process of knowledge creation and dissemination of information as well as deeper transmission is taking place towards redefining the communication process. Thus a fine balance can be achieved between terrorism and Law enforcement with due care and consideration. Thus we have enacted Information Technology Act, 2000 to punish the cyber criminals.

Earlier there was no specific provision in the IT Act, 2000 which deals specifically with Cyber terrorism due to this, a new section 66F has been inserted by Information Technology (Amendment) Act, 2008. It is a welcome change brought by the IT Amendment Act, 2008 in view of increasing terrorist activities in India and neighbouring nations.

Punishment for cyber terrorism[33] - (1) whoever, -

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or destruction of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life.

For the prevention of cyber terrorism we can use the method of “Counter strike through aggressive Defence”. The concept of counter strike through aggressive defence presupposes the adoption and use of information technology to produce legitimate and legalized disabling and reasonably destructive effects. Some adopted measures completely destroys the functioning of the offending computer while others simply disable the computer for the time being by either shutting it down or making it temporarily non-functional. The technology adopted must not only be safe and effective, but it must also be “legal and law-abiding”. A counter-measure, which is not very accurate, and law abiding would be a remedy worst than the malady and hence it should be avoided. For instance, if a virus has been launched by using a public server, then by disabling that server the genuine and legitimate users will be unnecessarily harassed and they would be denied the services which they are otherwise entitled to. Thus, the countermeasure measure adopted must be job specific and not disproportionate to the injury sought to be remedied.[34]

33. Information Technology Act, 2000, s., 66F

34. Article by Praveen Dalal, Cybercrime and cyber terrorism: Preventive defence for cyberspace violations, Computer Crime Research Center, March 10, 2006.

In March 2013, suspected Chinese hackers breached the computers of India's top military organisation, the Defence Research and Development Organisation (DRDO), in what was touted to be amongst the biggest such security breaches in the Indian history. India has seen many such attacks on its critical installations and the misuse of social media and Internet has brought home the threat of cyber-terrorism, the country is vulnerable to such cyber- terrorism attacks with some countries and vested interest groups bent on espionage and destruction.[35]

According to Pavan Duggal the threat of cyber attacks remains "imminent", the country lacks an institutionalised mechanism of a cyber army to deal with the threat. Further stated that "the recent DRDO breach was a classical case of cyber war attack rather than mere hacking. It was an attack on India's critical information infrastructure. Cyber warfare as a phenomenon is not covered under the Indian cyber law. Clearly, India's cyber security is not in sync with the requirements of the times"[36]

Over the past few years, India has witnessed a growing number of cyber terrorist attacks, with government departments, particularly defence establishments, coming under attack. There are following cases of cyber terrorism in India.

1. In 2012, hacker group 'Anonymous' carried out a series of Distributed Denial of Service (DDoS) attacks against a number of government websites, in retaliation against the alleged Internet censorship.
2. Also in 2012, Hackers from Algeria carried out an attack on websites run by the DRDO, the Prime Minister's Office and various other government departments.
3. Hackers from Pakistan and terrorist organization are increasing their attacks on Indian Websites to provide a new dimension to the ongoing conflict over Jammu and Kashmir. 'GForce' a group of anonymous hackers whose members write slogans critical of India and its claim over Kashmir, have owned up to several instances of hacking of Indian sites run by the Indian government like breaking into the high security computer network of Bhabha Atomic Research Center.
4. Indian Parliament attack is one of the deadliest attacks on Indian Democracy. It is a case of cyber terrorism where accused committed cyber forgery and made passes, downloaded official logo and layout map of the parliament has been downloaded through the Pakistan service provider. They controlled the e-mail and identity system of Indian Army.
5. In March, 2016 the Indian Infrastructure was attacked by the Terror outfit with the name of Al Qaeda who, allegedly hacked a micro site of the Rail net page of the Indian Railways to show its sinister reach for the first time. The hacked page of Bhusawal division of Personnel Department of the Central Railway and part of a large intranet created for the department's administrative needs was replaced by a message of Maulana Aasim Umar, Al Qaeda chief in south Asia, for all Indian Muslims to participate in Jihad.[37]

Information Technology becomes an easy tool in hands of terrorist. They use computers and networks to communicate with their operatives all around the world in codes without detected by the enforcement agencies. Cases like Ayodhya incident, attack in Mumbai in 2006, defacement of Indian Military sites in India by hackers in July 2005, attack on American Center at Kolkata and Pathankot Terrorist Attack etc., are the major cyber terrorist attacks in India.

As per the cyber law and cyber security expert Prashant Mali "The threat landscape remains very threatening, India is awakening to the global threat of cyber warfare now. Our cyber security is still ineffective as mass awakening towards it is missing or inadequate. Even though NTRO and DRDO are mandated with cyber offensive work, only time will show effectiveness of these organisations."

---

35. http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274 (Accessed on 16th February, 2016)

36. Ibid

37. http://www.ndtv.com/india-news/al-qaeda-hacks-into-indian-railways-website-leaves-message-to-join-jihad-1283023 (Accessed on 21 March, 2016)

With cyber security impacting the country's security, Shiv Shankar Menon, the national security adviser, announced that the government is putting in place national cyber security architecture to prevent sabotage, espionage and other forms of cyber threats.

Shantanu Ghosh, vice president at India Product Operations-Symantec Corporation, which developed Norton Antivirus has said that "The past few years have witnessed a dramatic shift in the threat landscape. The motivation of attackers has moved from fame to financial gain and malware has become a successful criminal business model with billions of dollars in play. We have now entered a third significant shift in the threat landscape, one of cyber- espionage and cyber-sabotage."

Rikshit Tandon, advisor to the Cyber Crime Unit of the Uttar Pradesh Police, said: "Cyber terrorism is a grave threat not only to India but to the world. It can come to any country and, yes, a proactive measure by government and consortium of countries needs to be taken as a collective effort and policy since internet has no geographical boundaries".[38]

Hacking

Hacking is labelled as amongst the most serious of all cyber crimes. It is said that hacking erodes the faith of people in information technology and the Internet. Hacking a computer system has been projected as a menace requiring harsh laws to act as deterrents. Such a general projection is somewhat misconceived.

Hacking a computer simply implies getting into another's computer without permission. Gaining unlawful access to another's computer is hacking. Unauthorized entry into a computer belonging to another is hacking. It is equivalent to phone-tapping. Hackers see the weakness in the target computer programme and then find ways to enter and access therein. Anti- hacking tools such as the 'Firewall' technology and intrusion detection systems are preventive measures that can be taken to protect a computer from being hacked. Firewall, like a wall of fire, prevents hacking. Intrusion detection systems will in addition also try to detect the source of hacking.

Hacking perse, in simple terms, is criminal trespass into a computer that is a private property. Criminal trespass under the Indian Penal Code, 1860 is simply defined as entering into property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, by unlawfully remaining there with intent thereby to intimidate, insult or annoy any such person or with intent to commit an offence.[39] Criminal trespass entails a punishment of imprisonment upto three months or fine upto rupees five hundred, or with both[40] Criminal trespass perse is thus a minor offence.

Here is a short list of great hackers of the world.

The most famous hacker in the history is Kevin Mitnick. At the tender age of 17 in 1981, he hacked into a phone exchange that allowed him to redirect subscriber calls in any way he wanted. In 1983, he accessed a Pentagon computer. In 1990s, he cracked/hacked/broke into the computer systems of the world's top technology and telecommunications companies like Nokia, Fujitsu, Motorola and Sun Microsystems. He was arrested by the FBI in 1995 and later released on parole in 2000.[41]

Gary McKinnon, an Englishman, was arrested in November 2002 on the accusation that he had hacked into more than 90 US military computer systems in the U.K.

Vladmir Levin, a Russian computer 'expert' is said to be the first to hack a bank to steal money. In early 1995,

38. Ibid

39. Indian Penal Code, 1860., s. 441

40. Indian Penal Code, 1860., s. 447

41. http://www.funonthenet.in/forums/index.php?topic=1260.0;wap2 (Accessed on 20th February, 2016)

he hacked into Citibank and robbed US$ 10 million. He was arrested by Interpol in the U.K. in 1995, after he had transferred money to his accounts in the US, Finland, Holland, Germany and Israel.

A Los Angeles radio station announced a contest that would reward the 102nd caller with a 'Porsche 944S2'. Kevin Poulsen took control of the entire city's telephone network and ensured he was the winner being the 102nd caller. He also hacked into 'Arpanet' that was the precursor to the Internet. Arpanet was a global network of computers.

US based hacker Timothy Lloyd planted a malicious software code in the computer network of Omega Engineering which was a prime supplier of components to NASA and the US Navy. Omega lost US$10 million due to the attack by which its manufacturing operations were impaired.[42]

Species of criminal trespass have been treated with more deterrent punishments. For instance, punishment for house-trespass is punishable with imprisonment upto one year.[43] House-trespass in order to commit an offence punishable with death (i.e. murder etc.) is punishable with imprisonment for life or rigorous imprisonment upto ten years.[44] House-trespass in order to commit an offence punishable with imprisonment for life is punishable with imprisonment upto ten years.[45] House-trespass, other than the above, entails punishment with imprisonment extending to two years and if the offence intended to be committed is theft, the term of the imprisonment may extend to seven years.[46] For house-trespass committed after preparation to cause hurt, assault or wrongful restraint or putting any person in such fear, the punishment prescribed is imprisonment extending to seven years.[47] Lurking house- trespass or housebreaking is punishable with imprisonment extending to two years.[48] Lurking house-trespass or housebreaking in order to commit an offence punishable with imprisonment, is liable for imprisonment upto three years and if such intended offence is theft, the term of imprisonment has been extended to ten years.[49] The punishment for lurking house-trespass or housebreaking by night is punishable with imprisonment extending to three years.[50] Grievous hurt caused whilst committing lurking house-trespass or housebreaking, is punishable with imprisonment for life, or imprisonment extending to ten years.[51] All persons jointly concerned in lurking house- trespass or housebreaking by night, are liable to be punished with imprisonment for life or extending to ten years, where death or grievous hurt is caused or attempted to be caused by any one or more of them.[52]

Another instance of an offence that has numerous species is "mischief". Every species of mischief is separately laid down in the I.P.C. with differing punishments, depending upon the magnitude thereof.[53] Many of the offences in the I.P.C. such as robbery, criminal breaches of trust, cheating etc., have their respective species that are treated differently from one another.

The legal approach towards hacking should be the same as that of criminal trespass, mischief and the innumerable other offences in the I.P.C. All forms of hacking cannot be treated alike. It needs to be understood that hacking too has numerous dimensions and species like other offences.

A person who enjoys exploring computer systems is also a hacker. Many teenagers obsessed with the Internet and computers hack for fun and excitement. Excitement to make an impact, show of capability and knowledge

42. Ibid
43. Indian Penal Code, 1860., s. 448
44. Indian Penal Code, 1860., s. 449
45. Indian Penal Code, 1860., s. 450
46. Indian Penal Code, 1860., s. 451
47. Indian Penal Code, 1860., s. 452
48. Indian Penal Code, 1860., s. 453
49. Indian Penal Code, 1860., s. 454
50. Indian Penal Code, 1860., s. 456
51. Indian Penal Code, 1860., s. 459
52. Indian Penal Code, 1860., s. 460
53. Indian Penal Code, 1860., s. 425-440

of computers, fun and publicity, and the desire to explore are some of the motives of these teenagers to hack into computer systems.

Another form of hacking is by Internet security companies, to test the computer systems of their clients and potential clients, to impress them and get business assignments of setting up security systems for the clients.

Hacking is also committed to damage the business of competitors and enemies. Disruption of a computer and denial of access to a person authorized to access any computer, are some of the damages that may be caused by hacking. Hacking is also done to spy into others computer systems and for stealing information/data residing therein. Hacking is also used as a Weapon to commit other crimes such as cheating and misappropriation of funds electronically from the bank account of another.

Hacking is done at the country level too. Frequently, Pakistani hackers are accused of hacking Indian web-sites. For instance, the web-site of SEBI (Stock Exchange Board of India) was hacked whereby a link to a pornographic web-site was inserted.

Hacktivists are protestors against governments or institutions / organizations, who protest through hacking. For instance, anti-globalization protests have been made through hacking the web-site of WTO.

There are therefore numerous species of hacking, though in essence, it is the offence of criminal trespass. All forms of hacking cannot thus be treated alike. It is the intent, purpose and consequences of hacking that determine its gravity. A twelve year old, who, for excitement and playing a prank enters restricted web-sites, should not be treated as a national enemy. A terrorist organization hacking into a protected system such as the defence computer systems to steal nuclear secrets, or a criminal syndicate hacking to misappropriate huge amounts, cannot be treated on par with a teenager prying into the computer system of his best friend's girlfriend or even the CBI (Central Bureau of Investigation) for fun and excitement. The nature of the hacking determines the gravity and all forms of hacking should not be projected or legally treated in the same manner. Hacking has so many species. Hacking is a skill that can be used positively as well as negatively. A man opening locks to help people who have lost the key is a locksmith. However, a person who opens locks to steal is a thief.

The seriousness of hacking depends upon the nature, purpose, intent and the extent of loss and injury that are caused to the victim. For instance, in a reported incident in the U.S., the owner of a hobby web-site for children received an e-mail informing her that a group of hackers had gained control over her web-site. They demanded a ransom of one million dollars. The threat was overlooked as a mere scare tactic. A few days late, she discovered that the hackers had 'web-jacked' her web-site. 'Web-jacking' has been equated with hijacking an aeroplane, as forcibly assuming control of a web-site, for diverse motives. The hackers had altered a part of the web-site which said "How to have fun with goldfish". The word "goldfish" was replaced with "piranhas". Piranhas are tiny but extremely dangerous flesh eating fish. Many children visiting the web-site, purchased 'piranhas' from pet shops and tried playing with them, thereby hurting themselves badly.[54]

Hacking in various forms is already part of several offences, either as the means to their commission or as a consequence. For instance, hacking could be a tool and means to commit cheating, misappropriation, criminal breach of trust, theft, copyright violations, spying into official secrets, or as part of the conspiracy to wage war against the State, that are all well defined offences. Some of the species of hacking have been defined as contraventions as well as criminal offences in the LT. Act, 2000 as amended by the I.T. (Amendment) Act, 2008. In the original version of the I.T. Act, 2000, section 66 defined and punished hacking in the following terms:

"Hacking with Computer System - (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects is injuriously by any means, commits hacking.

54. "Hack Attack" by Shuchi Nagpal, Asian School of Cyber Laws in Indian Express Vigil, March 2002. also available at http://www.asianlaws.org/press/hack_attack.htm (Accessed on 20th February, 2016)

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both".[55]

The title of the aforesaid section 66 was a misnomer, which created confusion. It was widely believed as if section 66 was the only legal provision that dealt with the offence of hacking a computer system. This confusion has been done away with, by certain amendments made by the I.T. (Amendment) Act, 2008. The words "Hacking with Computer System" have been deleted from section 66, the scope of which has been substantially widened:

"If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both".

The various species of the offence of hacking that are provided (even though not called 'hacking' specifically) for or may have elements of hacking, in the amended version of the I.T. Act, 2000 are:

- Access to a computer.
- Downloading, copying or extraction of data from a computer.
- Introducing computer virus and contaminants.
- Causing damage to a computer.
- Causing disruption of a computer.
- Causing denial of access to a computer.
- Affecting critical information infrastructure.
- Cyber terrorism.

LESSON ROUND-UP

- As discussed in the previous chapters that use of Internet and rapid deployment of information and communication technologies in recent years have bought various changes in the world both at individual level as well as organization level.
- Right from the way we communicate to the way we buy our groceries, each and every activity of human life is revolutionized with the help of information and communication technology. Crime is not an exception to this revolution brought by information and communication technologies.
- On one hand wherein the pattern of crime has been altered by misusing the tools and techniques of information and communication technology, on the similar hand, historic trends and practices in criminal investigation has also been revolutionized.
- This has created a tremendous challenge for law enforcement to develop the capacity to confront transnational crimes and follow evidence trails.
- India has been a favorite hub for cybercriminals, mostly hackers and other malevolent users who misuse the Internet by committing crimes.
- On one hand where we are witnessing the advancement of information and communication technology; on the similar end, we are seeing the new tools and techniques of committing cybercrimes.
- In general, cyber criminals make use of various tools and techniques yet the following are the most common tools and techniques used recently to conduct cybercrimes.
- The discussion above confirm that India is facing the growing threat of cybercrimes.

55. Information Technology Act, 2000., s. 66

- As per the Report published on recording the cyber incidents, India was placed on the 80th position in a report focusing on local threats in the year 2023.
- India's cybersecurity market reached USD 6.06 billion in 2023.
- However, according to IDC, a global marketing intelligence firm, the alarming increase in sophisticated external cyber threats and cybersecurity attacks is one of the biggest challenges for the majority of enterprises in establishing organizational trust.
- This has led government of India to channelize the effective ways in enhancing the level of cyber security.
- The Government of India had launched the online cyber-crime reporting portal, www.cybercrime.gov.in, which is a citizen-centric initiative, to allow the complainants to lodge complaints relating to child pornography/child sexual abuse material or any content which is sexual in nature.
- The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their Law Enforcement Agencies (LEAs).
- To strengthen the mechanism to deal with cyber-crimes in a comprehensive and coordinated manner, the Central Government has taken various steps including the establishment of 'Indian Cyber Crime Coordination Centre'
- For conducting cyber-crime investigation, certain special skills and scientific tools are required without which the investigation is not possible.
- Due to the Information Technology Act, 2000 ("IT Act"), certain provisions of Criminal Procedure Code and the Evidence Act, have been amended.
- Along with this, certain new regulations had been enforced by the Indian legal system to meet with the need of cyber-crime investigation.
- In general parlance, computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device.
- Computer forensics is primarily used for two separate purposes, investigation and data recovery.
- Both computer forensics and cyber security deal with criminals and computers, hence many a times they are considered rather similar.
- Despite this initial similarity, the function of computer forensics and cyber security greatly differs from each other.
- Computer forensics can be an essential facet of modern investigations.
- When a crime is committed and an investigation is started, one of the more common places to look for clues is the computer or cell phone of a suspect. This is where a computer forensics professional enters the picture.
- Digital forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation.
- The digital evidence and digital chain of custody are the backbones of any action taken by digital forensic specialists. Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases.

- Each step in the chain is essential and in case any step is missed, then the evidence may be rendered inadmissible in the court of law. Thus, we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.
- In general, security audit is a systematic evaluation of the security of a company's information system by measuring how well it adheres to an established set of criteria.
- A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.
- Security audits are often used to determine compliance with regulations such as Information Technology Act, 2000 and other rules and regulations applicable on the IT environment of a particular organization.
- It majorly specifies how organizations have dealt with the information and data available in the organization.
- The above discussion confirms the signification of security audit for fortifying the IT infrastructure of a company as well as the minimize the probability of cyber-attacks.
- Identify potential threats including the loss of data, equipment or records through natural disasters, malware or unauthorized users.
- Evaluate security and risks. Apart from assessing the risk of each of the identified threats happening, it also guides on how well the organization can defend against them.
- Determine the needed controls by Identifying what security measures must be implemented or improved to minimize risks.
- Helps the organization in ensuring compliance with the applicable laws and regulations related to the IT infrastructure and requirement of the company.
- Hence, it will be apt to state that periodic security audit is directly proportionate to the growth of the organization.
- A cybersecurity audit involves a comprehensive analysis and review of your IT infrastructure. It detects vulnerabilities and threats, displaying weak links and high-risk practices.
- Cybersecurity audits ensure a 360-degree in-depth audit of your organization's security posture. They aim to identify vulnerabilities, risks, and threats that may affect the organization.
- Beyond these, a cybersecurity audit can also cover cybersecurity risk management, cyber risk governance, training & awareness, legal, regulatory & contractual requirements, technical security controls, business continuity & incident management, and third-party management.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation.)

1. Write a brief note on process of Online Reporting of Cyber Crimes in India.
2. Write a short note on the steps on conducting investigations of cyber-crimes.
3. Discuss 5 latest initiatives of Government of India in strengthening the mechanism to control cyber crime.

4. What is Computer Forensics? Mention the significance of Computer Forensics in Cyber Crime.
5. What do you mean Digital Forensics? Describe the branches of Digital Forensics.
6. Write short note on any of the following:
    - Security Audit
    - Advantages of Security Audit
    - Types of Security Audit
    - Investigation vide Computer Forensics.
6. What are the components of Checklist of Cyber Security Audit? Describe

LIST OF FURTHER READINGS

- Banoth Rajkumar et al (2023) A Comprehensive Guide to Information Security Management and Audit, ISBN 9781032344430 Published September 30, 2022 by CRC Press
- Important Cyber Law Case Studies, Cyber Laws and Information Security Advisors. Available at https://www.cyberralegalservices.com/detail-casestudies.php
- Katz Eric, Cyber Forensics: The Fascinating World of Digital Evidences, Purdue Cyber Forensic Labs
- Graeme Edwards (2020) Cybercrime Investigators Handbook, (Audio Book), Audible by Amazon
- Nelson, Phillips and Steuart (2019) Guide to Computer Forensics and Investigations 6TH edition, CENGAGE INDIA
- Sharma Nishesh (2017) Cyber Forensics in India: A Legal Perspective, Universal Law Publishing, India.

LIST OF OTHER REFERENCES

- Buckbee Michael (2020) What is an IT Security Audit? The Basics, Varonis
- Data Security Council of India (2011) Cyber Crime Investigation Manual with Knowledge Partner Deloitte
- Effective Governance Risk Management, ISACA Journal. ISACA. Retrieved 2022-04-21
- Information Systems Security Audit, ISACA Journal. ISACA. Retrieved 2022-04-21
- Irwin Luke (2022) What is a Cyber Security and Why is it Important? IT Governance Blog
- Legislative Audit Division - State of Montana (2006, June). “Data Center Review” Helena, MT
- Privacy Technical Assistance Center, “Responding to IT Security Audits: Improving Data Security Practices”. PDF
- Varghese Jinson (2023) IT Security Audit: Importance, Types and Methodology, Astra.

Regulatory Framework on AI, Cyber Security and Cyberspace

Lesson 5

KEY CONCEPTS

■ E-Governance ■ RBI Regulations ■ Artificial Intelligence ■ Cyber Security ■ Cyberspace ■ SEBI Regulations ■ International Principles

Learning Objectives

To understand:

- How to focus on major themes pertaining to artificial intelligence and cybersecurity-crime and its inter-relationship
- The responsibility and function of regulatory authority like SEBI and RBI governing the issues related to Artificial Intelligence and cyberspace
- To study international legal regime related to development of modern technology tools like AI to improve the existing position of digital security

Lesson Outline

- E-Governance in India
- RBI Regulations governing AI, Cyber Security and Cyberspace
- SEBI Regulations governing AI, Cyber Security and Cyberspace
- International Principles governing AI, Cyber Security and Cyberspace
- Other Applicable Regulatory Framework
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

E-GOVERNANCE IN INDIA

Meaning of e-Governance

E-Governance as the name suggest is made up of two words. "E" and "Governance". Hence to understand the concept of e-Governance, we shall first understand the meaning of Governance. Governance is the process of making and enforcing decisions within an organization or society.[1] It is the process of interactions through the laws, social norms, power (social and political) or language as structured in communication of an organized society over a social system (family, social group, formal or informal organization, a territory under a jurisdiction or across territories). It is usually done by the government of a state. Conceptually, governance can be defined as the rule of the rulers, typically within a given set of rules. One might conclude that governance is the process – by which authority is conferred on rulers, by which they make the rules, and by which those rules are enforced and modified. Hence with "e" in e-Governance which stands for 'electronic' - is basically associated with carrying out the functions and achieving the results of governance through the utilization of ICT (Information and Communications Technology).

However, this would require the government to change itself – its processes, its outlook, laws, rules and regulations and also its way of interacting with the citizens. It would also require capacity building within the government and creation of general awareness about e-Governance among the citizens.

The Council of Europe referred to e-Governance as:

- the use of electronic technologies in three areas of public action;
- relations between the public authorities and civil society the functioning of the public authorities at all stages of the democratic process (electronic democracy);
- the provision of public services (electronic public services).

In a broader sense, 'e-governance' is all about reform in governance facilitated with the inventive and resourceful use of ICT.

Evolution of E-Governance

Electronic Governance, popularly known as e-governance. E-Governance originated in India during the 1970s with a focus on in-house government applications in the areas of defence, economic monitoring, planning and deployment of ICT to manage data intensive functions related to elections, census, tax administration etc. It is a distinct dimension of New Public Management (NPM) which has gained considerable momentum since the early 1990s. The term 'e-Governance' is often used to describe the networking paradigm and its decentralizing and communicatory implications. E-governance as competing paradigms is the process of enabling governance experts using Information and Communication Technology (ICT) to make governance effective for citizens in terms of efficiency, transparency, and cost-effectiveness.

- The establishment of the Department of Electronics in 1970 was the first major step towards e-governance in India as it brought 'information' and its communication to focus.
- National Informatics Centre (NIC) established in 1977, launched the District Information System program to computerize all district offices in the country
- The main thrust for e-governance was provided by the launching of NICNET in 1987 – the national satellite-based computer network.

Demands of transparency, ethics, rightfulness, access to justice, eradication of corruption and other related issues along with welfare driven political leadership, other associated governments, capacity building needs

1. Compare: Bevir, Mark (2012). Governance: A very short introduction. Oxford, UK: Oxford University Press. ISBN 9780191646294

and perceived citizen expectations and all has contributed to adoption of e-government methods for good governance.

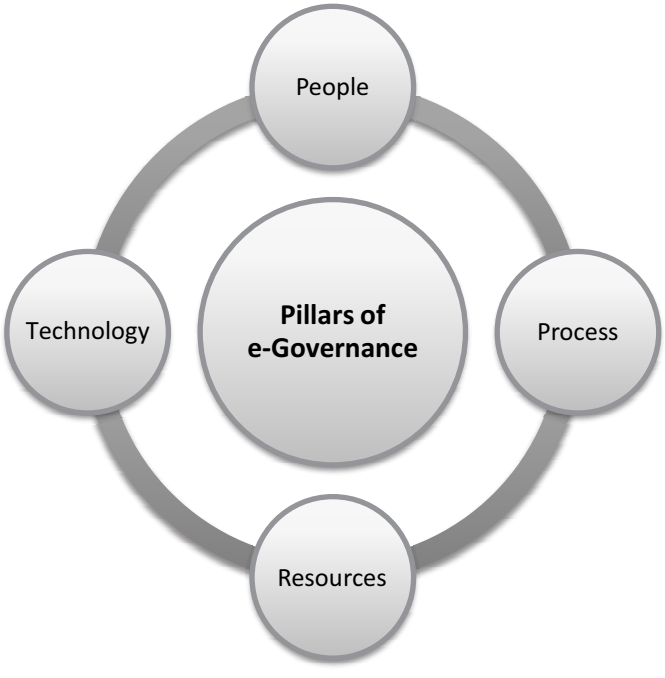
At a broader level, apart from delivering government services, e-governance includes integration of several stand-alone systems and services between ***Government-to-Citizens (G2C), Government-to-Business (G2B), and Government-to-Government (G2G)*** as well as back-office processes and interactions within entire government framework.

The overall objective of such e-governance is to enable the administration to provide services with affordable cost and optimum time to the end user (citizen).

Objectives

- Better service delivery to citizens.
- Ushering in transparency and accountability.
- Empowering people through information.
- Improve efficiency within Government i.e. between center-state or inter-states.
- Improve interface with business and industry.

Pillars of e-Governance



Types of Interaction in e-Governance

- G2G: Government to Government
- G2C: Government to Citizen
- G2B: Government to Business
- G2E: Government to Employee

Electronic governance or e-governance is adopted by countries across the world. In a fast-growing and demanding economy like India, e-governance has become essential. The rapid growth of digitalisation has led to many governments across the globe to introduce and incorporate technology into governmental processes. Electronic governance or e-governance can be defined as the usage of Information and Communication Technology (ICT) by the government to provide and facilitate government services, exchange of information, communication transactions and integration of various standalone systems and services.

In other words, it is the use of technology to perform government activities and achieve the objectives of governance. Through e-governance, government services are made available to citizens and businesses in a convenient, efficient and transparent manner. Examples of e-governance include Digital India initiative, National Portal of India, Prime Minister of India portal, Aadhaar, filing and payment of taxes online, digital land management systems, Common Entrance Test etc.

Types of interactions in e-Governance

e-Governance can take place in four major types of interactions, apart from the processes and interactions in the back-office, within the government framework:

Government to Government (G2G)

Information is exchanged within the government i.e., either, between the central government, state government and local governments or between different branches of the same government.

Government to Citizen (G2C)

The citizens have a platform through which they can interact with the government and get access to the variety of public services offered by the Government.

Government to Businesses (G2B)

The businesses are able to interact with the government seamlessly with respect to the services of the government offered to businesses.

Government to Employees (G2E)

The interaction between the government and its employees occurs in an efficient and speedy manner.

National E-governance Plan[2]

The National e-Governance Plan (NeGP) has been formulated by the Department of Electronics and Information Technology (DEITY) and Department of Administrative Reforms and Public Grievances (DARPG) in 2006.

The NeGP aims at improving delivery of Government services to citizens and businesses with the following vision: "Make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realise the basic needs of the common man." The National e-Governance Plan (NeGP), takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision, a shared cause. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is evolving, and large-scale digitization of records is taking place to enable easy, reliable access over the internet. The ultimate objective is to bring public services closer home to citizens, as articulated in the Vision Statement of NeGP.

2. Reproduced from E-governance in India: Concept, Initiatives and Issues, Insignts on India, 2018

The Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects and 8 components, on May 18, 2006. In the year 2011, 4 projects - Health, Education, PDS and Posts were introduced to make the list of 27 MMPs to 31Mission Mode Projects (MMPs). The Government has accorded approval to the vision, approach, strategy, key components, implementation methodology, and management structure for NeGP. However, the approval of NeGP does not constitute financial approval(s) for all the Mission Mode Projects (MMPs) and components under it. The existing or ongoing projects in the MMP category, being implemented by various Central Ministries, States, and State Departments would be suitably augmented and enhanced to align with the objectives of NeGP.

In order to promote e-Governance in a holistic manner, various policy initiatives and projects have been undertaken to develop core and support infrastructure. The major core infrastructure components are State Data Centres (SDCs), State Wide Area Networks (S.W.A.N), Common Services Centres (CSCs) and middleware gateways i.e National e-Governance Service Delivery Gateway (NSDG), State e-Governance Service Delivery Gateway (SSDG), and Mobile e-Governance Service Delivery Gateway (MSDG). The important support components include Core policies and guidelines on Security, HR, Citizen Engagement, Social Media as well as Standards related to Metadata, Interoperability, Enterprise Architecture, Information Security etc. New initiatives include a framework for authentication, viz.

e-Pramaan and G-I cloud, an initiative which will ensure benefits of cloud computing for e-Governance projects.

Central government initiatives as mission mode projects (MMP)

- ***e-office***

  The Government of India has recognized the need to modernize the Central Government offices through the introduction of Information and Communications Technology. e-Office is aimed at increasing the usage of work flow and rule-based file routing, quick search and retrieval of files and office orders, digital signatures for authentication, forms and reporting components.

- ***Immigration, Visa and Foreigner's Registration & Tracking (IVFRT)***

  India has emerged as a key tourist destination, besides being a major business and service hub. Immigration Check Post is the first point of contact that generates public and popular perception about the country, thus necessitating a state of the art system for prompt and user-friendly services.

- ***Unique Identification Number (UID)***

  The unique identification project was conceived as an initiative that would provide identification for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the government.

- ***Pensions***

  The pensions MMP is primarily aimed at making the pension/ retirement related information, services and grievances handling mechanism accessible online to the needy pensioners, through a combination of interactive and non-interactive components, and thus, help bridge the gap between the pensioners and the government.

- ***Banking***

  The Banking MMP is yet another step towards improving operational efficiency and reducing the delays and efforts involved in handling and settling transactions. The MMP which is being implemented by the banking industry aims at streamlining various e-services initiatives undertaken by individual banks. Implementation is being done by the banks concerned, with the banking Department providing a broad framework and guidance.

- ***Posts***

  Modernization of Postal Services has been undertaken by the Department of Posts through computerization and networking of all post offices using a central server-based system, and setting up of computerized registration centers (CRCs).

State Mission Mode Projects

- ***e-Governance in Municipalities***

  It is a unique initiative of the Government of India conceptualized under the umbrella of the overall National e-Governance Plan (NeGP) and the Jawaharlal Nehru National Urban Renewal Mission (Jnnurm) aimed at improving operational efficiencies within Urban Local Bodies (ULBs).

- ***Crime and Criminal Tracking Network & Systems***

  Crime and Criminal Tracking Network & Systems (CCTNS) MMP aims at creating a comprehensive and integrated system for enhancing the efficiency and effective policing at all levels and especially at the Police Station level through adoption of principles of e-Governance, and creation of a nationwide networked infrastructure for evolution of IT-enabled state-of-the-art tracking system.

- ***Public Distribution System***

  Computerization of the PDS is envisaged as an end-to-end project covering key functional areas such as supply chain management including allocation and utilization reporting, storage and movement of food grains, grievance redressal and transparency portal, digitization of beneficiary database, Fair Price Shop automation, etc.

- ***Health***

  ICT for programme management has been undertaken by the Ministry of Health & Family Welfare in the Mother and Child Tracking System (MCTS) programme and the Ministry envisages a more comprehensive use of ICT including for Hospital Information Systems, supply chain management for drugs and vaccines, providing ICT tools to ASHA and ANM workers, programme management of National Rural Health Mission (NRHM), etc. through this MMP.

- **e-panchayat**

  The Panchayati Raj Institutions (PRIs) are saddled with the problems of inadequate physical and financial resources, technical capabilities and extremely limited computerization. As a result, the potential of PRIs as the preferred delivery channel for the schemes of State and Centre as well as for citizen services has not been fully realized. While some computerization efforts for PRIs have been made by NIC over the years, the e-Governance revolution sweeping the country has not touched the PRIs yet in significant measure. The Ministry of Panchayati Raj, Government of India has therefore decided to take up the computerization of PRIs on a mission mode basis.

- **e-District**

  e-District is one of the 31 Mission Mode Projects under National e Governance Plan (NeGP) with the DIT, GoI being the nodal ministry. This project aims at providing support to the basic administrative unit i.e. District Administration by undertaking backend computerization to enable electronic delivery of high volume citizen centric government services which would optimally leverage and utilize the three infrastructure pillars of State Wide Area Networks (SWAN), State Data Centers (SDC) and Common Service Centers (CSCs) to deliver services to the citizen at his doorsteps.

- **National Land Records Modernization Programme (NLRMP)**

  A Project for Computerization of Land Records (CLR) was launched in 1988-89 with the intention to remove the inherent flaws in the manual system of maintenance and updation of Land Records. In 1997-98, the scheme was extended to tehsils to start distribution of Records of Rights to landowners on demand. The focus of the entire operation has always been to employ state of the art information technology (IT) to galvanize and transform the existing land records system of the country.

Integrated Mission Mode Projects

- ***e-procurement***

  Ministry of Commerce & Industry (Department of Commerce) has been nominated as the Nodal Ministry for implementation of e-Government Procurement (e-GP) Mission Mode Projects (MMP). The vision of the e-Procurement MMP is "To create a national initiative to implement procurement reforms, through the use of electronic Government procurement, so as to make public procurement in all sectors more transparent and efficient".

- ***e-Courts***

  The e-Court Mission Mode Project (MMP) was conceptualized with a vision to transform the Indian judiciary by making use of technology. The project had been developed, following the report submitted by the e-Committee under Supreme Court on national policy & action plan on implementation of information communication tools in Indian judiciary. A clear objective – to re-engineer processes and enhance judicial productivity both qualitatively and quantitatively to make the justice delivery system affordable, accessible, cost effective, transparent and accountable.

- **e-Biz**

  The e-Biz Mission Mode Project, being executed by Department of Industrial Policy and Promotion (DIPP), Ministry of Commerce and Industry, Government of India, was conceptualized with the vision. Its vision is "To transform the business environment in the country by providing efficient, convenient, transparent and integrated electronic services to investors, industries and business throughout the business life cycle".

- **Common Services Centers**

  The CSCs would provide high quality and cost-effective video, voice and data content and services, in the areas of e-governance, education, health, telemedicine, entertainment as well as other private services. A highlight of the CSCs is that it will offer web-enabled e-governance services in rural areas, including application forms, certificates, and utility payments such as electricity, telephone and water bills.

Recent Initiatives

Some of the major recent initiatives under e-Governance includes the follows:

- Direct Cash Transfer
- Aadhar Enabled Payment System
- MyGov Citizen Portal
- E-Kranti Scheme
- Digital Cloud for every Indian
- Digital India Program.

Direct Cash Transfer

To facilitate disbursements of Government entitlements like NREGA, Social Security pension, Handicapped Old Age Pension etc. of any Central or State Government bodies, using Aadhaar and authentication thereof as supported by UIDAI.

Aadhar Enabled Payment System (AEPS)

AEPS is a bank led model which allows online interoperable financial inclusion transaction through the Business correspondent of any bank using the Aadhaar authentication. This has helped in financial inclusion. The four Aadhaar enabled basic types of banking transactions are as follows:-

- Balance Enquiry
- Cash Withdrawal
- Cash Deposit
- Aadhaar to Aadhaar Funds Transfer.

MyGov Citizen Portal

Prime Minister launched an online platform mygov.nic.in to engage citizens in the task of "good governance" (surajya) on 26th July 2014. MyGov is a technology-driven platform that would provide people with the opportunity to contribute towards good governance.

E-Kranti Scheme

This is project for linking the internet with remote villages in the country. This scheme will broaden the reach of internet services to the rural areas in the country. The fundamental features of this scheme will be making the records handy to the government with ease. It also includes Expansion of internet and commencement of IT-based jobs in rural areas. It will also boost the use of mobile phones and computers in rural areas. It will also expand the use of IT in agriculture and retail trade too.

Digital Cloud for every Indian

Certificates issued by the government - education, residential, medical records, birth certificates, etc. - are to be stored in individual 'digital lockers and a communication protocol established for government departments to access them without physically having to see the hard copy. The purpose of government is that copies of certificates issued by the government itself not to be carried around by people to government offices for various services.

Digital India Program

The advent of Information and Communication Technology (ICT) and related advances IT services have been one of the ground-breaking changes in the all-encompassing development of the world at large. India is not an exception to the progressive effect of ICT. This serves enormous benefits by way of building capacities and competencies of elevating developing economies like India. It creates a swift in connecting people, upgrades the technology base, eases out the realization of government schemes and design and also helps in effective institution of governance in the nation.

Digital Technologies along with the promotion of Cloud Computing and Mobile Applications have emerged as catalysts for rapid economic growth and citizen empowerment across the globe. Global statistics reveal that the number of users who access the internet on mobile devices has surpassed the users who access it on PCs. Digital technologies under the tagline of Smart Applications are intended to build smartly progressive and constructive existence for citizens. These technologies are increasingly used by the society in day-to-day life from personal communications, buying goods at retail stores, availing services at doorstep to availing the governance through government offices.

Seeing the potential of digitalization and its constructive impact supporting inclusive development of our country, Government of India has launched the "Digital India" campaign. The Digital India drive envisions transforming our nation and creating opportunities for all citizens by harnessing digital technologies.

One notable aspect of the Digital India program is that it is aimed at catching the imagination of the people and this is the reason that Digital India has attracted the attention of almost everyone, both within the country and abroad. This is potentially one of the schemes which can bring about transformational benefits and fundamentally alter almost every aspect of our national life including the way citizens interact with not just the government but with each other.

The vision of Digital India program is to empower every citizen with access to digital services, knowledge and information. It can be summarized that this is intending to develop a digitally empowered society and to digitally integrate the government departments and the citizens of India. It aims at ensuring that the government services are made available to people of India electronically. Digital India is a Programme to prepare India for a knowledge future.

Digital India- Meaning and Concepts

Digital India is an initiative undertaken by the Government of India to integrate the government departments and the people of India. It aims at ensuring that the government services are made available to citizens electronically by reducing paperwork, increasing transparency, and also to encourage transparency in the system for government services and facilities. The initiative also plans to connect rural areas with high-speed internet networks.

One of the major objectives of Digital India includes in providing high speed internet connectivity to 250,000 Gram Panchayats, improve inter-operability, and promote digital literacy.

Digital India is a campaign run by the government of India to make this country a digitally empowered country. The aim of launching this campaign is to provide Indian citizens electronic government services by reducing the paperwork. It is very effective and efficient technique which will save time and man power to a great extent. This initiative was started to connect people of rural areas with the high-speed internet networks to access any information needed.

Digital India movement is majorly emplacing on promoting e-governance and to transform India into digitally empowered society and knowledge economy. As per the expert views, Digital India movement is channelized in preparing India for the knowledge-based transformation and delivering good governance to citizens by synchronized and co-ordinated engagement with both Central Government and State Governments.

Aims and Objectives:

Digital India campaign has been implemented by the Government of India to ensure following aims and objectives:

- To ensure the broadband highways;
- To ensure the universal access to mobile phones;
- To facilitate people with high-speed internet;
- To bring e-Governance by reforming government through digitization;
- To bring e-Kranti through electronic delivery of services;
- To make available online information for all;
- To ensure more jobs under the IT specialization.

Key Areas:

With a view to enlarge the reach of government services to the remotest areas of our country, Digital India programme is objectifying on three key vision areas which includes 'Digital Empowerment; Development of Digital Infrastructure and Ease of accessibility of e-governance and digital services.'

1. **Digital Empowerment:** To avail the maximum gain of Digital India drive, it is must that the citizens of our nation should be aware about the facilities and the means to avail them to their fullest. Therefore, to ensure directed empowerment towards digitalization, government has introduced various schemes to achieve following aims like universal digital literacy, universally accessible digital resources, availability of digital resources and services in maximum Indian languages. Further, collaborative digital platforms are also established for participative governance wherein the citizens are not required to physically submit documents or certificates to the government and it can be done digitally.
2. **Digital Infrastructure:** No facility can be availed without a proper infrastructure, so it is with digital services. To set up an excellent Digital Infrastructure is one the major priority of the government to ensure reach of the utility to every citizen. To build the requisite digital infrastructure, government is initiating the following activities:
    - High speed internet shall be made available in all gram panchayats;
    - Cradle to grave digital identity;
    - Mobile and Bank account would enable participation in digital and financial space at individual level;
    - Easy access to common service centre within their locality;
    - Shareable private space on a public cloud; and
    - Safe and secure cyber space in the country.
3. **E-Governance & e-Services:** With a view to extend the reaping of e-governance and to ensure the availability of e-services on demand, effortlessly integrated services are established across departments or jurisdictions. The services of digital era are made available in real time from online & mobile platforms.

Apart from this, all citizens are receiving entitlements to be portable and available on the cloud. Digitally transformed services are provided for improving ease of doing business. Along with this, citizens are also encouraged in making financial transactions electronic & cashless. Best among all is the institution of Leveraging Geospatial Information Systems (GIS) for decision support systems & development.

Initiatives under Digital India

To emplace the key drivers of Digital India movement, the government has launched several initiatives like digital locker under the name "Digi Locker" which aims to minimize the usage of physical documents and enable sharing of e-documents across agencies. Another is 'MyGov.in' which is as an innovative platform to build a partnership between citizen and government. Swachh Bharat Mission (SBM) Mobile app has also been introduced and used by people and Government organizations for achieving the goals of Swachh Bharat Mission. Along with this, eSign framework is there which would allow citizens to digitally sign a document online using Aadhaar authentication.

E-Governance/Digital India: Snap Shot of Recent Government Initiatives[3]

The Ministry of Electronics and Information Technology (MeitY), Government of India launched the 'Digital India' programme with the vision to transform India into a digitally empowered society and knowledge-based economy by ensuring digital access, digital inclusion, digital empowerment and bridging the digital divide. In summary, our mission is to ensure that the digital technologies improve the life of every citizen; expand India's digital economy, create investment & employment opportunities and global digital technological capabilities in the country.

Digital India has dramatically reduced distance between Government and citizens significantly. Further, Digital India has also helped in delivery of substantial services directly to the beneficiary in a transparent and corruption free manner. India has become one of the pre-eminent nations of the world to use technology to transform the lives of citizens. Digital India is an umbrella programme that covers multiple projects of various Central Ministries/Departments and States/UTs. Some of the major initiatives related to public service delivery are as follows:

- **Common Services Centres** – CSCs are offering government and business services in digital mode in rural areas through Village Level Entrepreneurs (VLEs). Over 400 digital services are being offered by these CSCs. So far, 5.31 Lakh CSCs are functional (including urban & rural areas) across the country, out of which, 4.20 Lakh CSCs are functional at Gram Panchayat level.
- **Unified Mobile Application for New-age Governance (UMANG)** – for providing government services to citizen through mobile. More than 1,570 government services and over 22,000 bill payment services are made available at UMANG.
- **e-District Mission Mode Project (MMP)** – e-District project has been implemented at district and sub-district levels of all States/UTs, benefitting all citizens by delivering various e-Services such as Certificates (Birth, Caste, Death, Income and Local Resident), Pension (Old Age, Disability and Widow), Electoral, Consumer Court, Revenue Court, Land Record and services of various departments such as Commercial Tax, Agriculture, Labour, Employment Training & Skill Development etc. Presently 4,671 e-services have been launched in 709 districts across India.
- **DigiLocker** – It is facilitating paperless availability of public documents. Digital Locker has more than 11.7 crore users and more than 532 crore documents are made available through DigiLocker from 2,167 issuer organisations.
- Unified Payment Interface (UPI) is the leading digital payment platform. It is integrated with 330 banks and facilitated over 586 crore monthly transactions worth over Rs 10 lakh crore has been facilitated for the month of June, 2022.
- **CO-WIN** – It is an open platform for management of registration, appointment scheduling & managing vaccination certificates for Covid-19. More than 203 crore vaccination doses and 110 crore registrations have been facilitated by co-win.
- **MyGov** – It is a citizen engagement platform that is developed to facilitate participatory governance. More than 2.48 crore users are actively using MyGov.
- **MeriPehchaan** – National Single Sign-on platform called MeriPehchaan has been launched in July 2022 to facilitate / provide citizens ease of access to government portals.
- **MyScheme** – This platform has been launched in July 2022 to facilitate citizens to avail eligibility-based services.

3. This information was given by the Minister of State for Electronics & Information Technology, in a written reply to a question in Lok Sabha on August 03, 2022. Source – E-Governance, Press Information Bureau, Government of India.

- **Direct Benefit Transfers –** 315 Schemes across 53 Ministries are offering Aadhaar enabled direct benefit transfer to citizens. So far, Rs. 24.3 lakh crore has been disbursed through DBT platform.
- **Diksha** – Diksha is a national level educational platform that helps students and teachers to participate, contribute and leverage a common platform to achieve learning goals at scale for the country. As on 27th July 2022, 7,633 courses were available and more than 15 crore enrolments have been done.

Some of the major digital initiatives taken by the Government for welfare of farmers are as follows:

- **National Agriculture Market (e-NAM)** – Government of India has launched National Agriculture Market (e-NAM) Scheme with the objective of creating online transparent competitive bidding system to facilitate farmers with remunerative prices for their produce. More than 1.73 crore farmers & 2.26 lakh traders have been registered on e-NAM platform. Also, 1000 mandis of 18 States and 3 UTs have been integrated with e-NAM platform.
- **M-KISAN** – mKisan Portal (www.mkisan.gov.in) for sending advisories on various crop related matters to the registered farmers through SMSs. In mkisan more than 5.13 crore farmers are registered for receiving crop advisories through SMS. More than 2,462 crore mobile based advisories have been sent to farmers to assist them in their farming activities.
- **One Stop Window** – Farmers Portal (www.farmer.gov.in) for dissemination of information on various agricultural related matter including, seeds variety, Storage Godown, Pests and plant diseases, Best Agricultural Practices, Watershed, Mandi details etc.
- **Soil Health Card** – It provides soil related information to facilitate farmers in farming activities. More than 22 crore soil health cards have been printed and dispatched to farmers.
- Mobile based advisory system for agriculture & Horticulture (M4AGRI) – It is mobile based advisory system for agriculture and horticulture. It has been implemented in the North-East States namely Tripura, Mizoram, Manipur, Meghalaya, Sikkim, and Arunachal Pradesh.

The Government has taken following steps in direction of data governance for socio-economic development in the country. The brief details are as follows:

- **Open Government Data** – To facilitate data sharing and promote innovation over non-personal data, Open Government Data platform has been developed. More than 5.65 lakh datasets across 12,800+ catalogues are published. The platform has facilitated 93.5 lakh downloads.
- **API Setu** – To facilitate data exchange among the system, API Setu has been developed as a platform. The platform has more than 2100 APIs, and 1000+ user organisations.
- MeitY has prepared the draft National Data Governance Framework Policy which aims to realize the full potential of India's digital government vision, maximize the efficiency of data-led governance & public service delivery and to catalyze data-based research and innovation. Currently the draft policy is under finalization. MeitY released the Draft National Data Governance Framework Policy on 26th May 2022 for public consultation.

The Government has already taken necessary measures to tackle challenges with regard to data privacy and data security through administering the Information Technology (IT) Act, 2000 which has necessary provisions for data privacy and data security.

RBI REGULATIONS GOVERNING AI, CYBER SECURITY AND CYBERSPACE

The advent of information and communication technology has revolutionized all the sectors across the globe. Indian banking and financial sector are not an exception to the transformation that has happened with the advent of information technology. Of all the IT domains that are impacting this industry, Artificial Intelligence (AI) and Data Analytics are the most influential contenders. In the present banking scenario, these stand out to

be the solution to a plethora of problems – increasing competition, fraud and cyber security threats, regulatory compliances, improving efficiency of the revenue stream, etc. According to PwC's report titled 'Industry 4.0: Building the Digital Enterprise report'[4], nearly 39% of companies in India planned to invest 8% of their annual revenues in digital programmes by 2021. As the Indian government pushes for India to become a USD 5 trillion economy by 2024, it also wants India's digital economy to become USD 1 trillion by 2025.[5] With all these set-goals in digital India, the banking industry is playing vital role and preparing itself with major digital alterations in recent years. Most conventional banks are using modern technologies to streamline their operations.

Under this backdrop, regulators are taking lead in regulating the use of modern technologies including AI in the domain of banking industry.

RBI and Artificial Intelligence: Evolving Governance[6]

Machine Learning (ML) and Artificial Intelligence (AI) are already being used in supervisory procedures by RBI. It now intends to make sure that the Department of Supervision at the central bank may reap the rewards of advanced analytics. Additionally, they have plans to bring in outside consultants for this work. For supervisory tests, the department has been creating and utilizing linear and a few ML models. Urban Cooperative Banks (UCBs), Non-Bank Financial Businesses (NBFCs), payment banks, small financing banks, neighborhood banks, credit information firms, and a few more Indian financial organizations are all subject to the RBI's regulatory authority. Artificial Intelligence (AI) and Machine Learning (ML) driven tools for data analysis and information creation will be integral part of Reserve Bank's Medium-term Strategy Framework 'Utkarsh 2.0' for the period 2023-2025. The first strategy framework (Utkarsh 2022) covering the period 2019-2022 was launched in July 2019. It became a medium-term strategy document guiding the Bank's progress towards realisation of the identified milestones. Against the backdrop of a challenging global and domestic environment, Utkarsh 2.0 commences from 2023, when India assumes the G-20 Presidency, With India's G-20 presidency during the period of Utkarsh 2.0, it confers a unique opportunity to showcase our accomplishments in the realm of digital payments and strive towards broad basing of acceptance of the Indian Rupee in bilateral and multilateral trade. The Vision in Utkarsh 2.0 that will guide the Reserve Bank of India over the period 2023-25 include, 'Excellence in performance of its functions'; Strengthened trust of citizens and Institutions in the RBI; and Enhanced relevance and significance in national and global roles. In this age of data, the Bank plays the dual role of data collection as well as information dissemination. With this comes the responsibility of reliability of data collected to create meaningful and accurate information. Therefore, adoption of AI and ML driven tool for data analysis and information creation will be an integral part of Utkarsh 2.0. The RBI is looking to extensively use advanced analytics, artificial intelligence and machine learning to analyse its huge database and improve regulatory supervision over banks and NBFCs.

RBI Jurisdiction

- Banks, urban cooperative banks, Non-Bank Financial Businesses (NBFCs), payment banks, small financing banks, local area banks, credit information firms, and a few other Indian financial organizations are all subject to the RBI's regulatory authority.
- To safeguard the interests of depositors and maintain financial stability, it conducts supervision of these companies intending to evaluate their soundness, solvency, asset quality, governance structure, liquidity, and operational viability.

4. Available at https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

5. Available https://meity.gov.in/ writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

6. Reproduced from Cheguri Preethi (2022) India seeks to expand AI Regulatory Prospects – RBI comes to Rescue, Analytics India.

RBI intents to use AI and ML rigorously:

AI and ML technologies are utilized for real-time data reporting, efficient data management, and data distribution on the data gathering side. Monitoring supervised firm-specific risks, including liquidity risks, market risks, credit exposure and concentration risks, misconduct analysis, and product misspelling, is done through data analytics. RBI inter-alia is looking to investigate and profile data with a supervisory focus. Hence, RBI is adopting an active regulatory mechanism to improve the Reserve Bank's data-driven surveillance capabilities.

RBI Governing Cyber Security and Cyberspace:

The Reserve Bank of India (RBI), being the regulatory body of the Indian Banking System, circulates guidelines on various aspects. For the last few years, banks and other financial sectors have become the soft targets for cybercriminals. Attacks such as Ransomware, malware insertion, phishing emails, DDos thriving exponentially. Financial institutions are amongst the most highly targeted organizations for cyber security attacks. To address this, the Reserve Bank of India (RBI) has outlined a list of controls, known as the RBI Guidelines for Cyber Security Framework[7], for banks to achieve a minimum recommended baseline of cyber-attack resilience.

The "Cyber Security Framework in Banks" circular from RBI sets the guidelines for Banks in India for developing and implementing next-generation cyber defence capabilities. The framework would direct the execution of progressively more robust security measures based on the nature, scale and variety of bank digital product offering.

Source: https://valuementor.com/en-in/rbi-cyber-security-framework/

The RBI cyber security framework addresses three core areas:

a. Establish Cyber Security Baseline and Resilience;

b. Operate Cyber Security Operations Centre (C-SOC);

c. Cyber Security Incident Reporting (CSIR).

7. Available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0

RBI Cyber Security Circular: Brief

Need for a Board approved Cyber-Security Policy

Banks were directed immediately put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board. It may be ensured that the strategy deals with the following broad aspects:

1. **Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank**

   In order to address the need for the entire bank to contribute to a cyber-safe environment, the Cyber Security Policy should be distinct and separate from the broader IT policy / IS Security policy so that it can highlight the risks from cyber threats and the measures to address / mitigate these risks.

   The size, systems, technological complexity, digital products, stakeholders and threat perception vary from bank to bank and hence it is important to identify the inherent risks and the controls in place to adopt appropriate cyber-security framework. While identifying and assessing the inherent risks, banks are required to reckon the technologies adopted, alignment with business and regulatory requirements, connections established, delivery channels, online / mobile products, technology services, organizational culture and internal & external threats. Depending on the level of inherent risks, the banks are required to identify their riskiness as low, moderate, high and very high or adopt any other similar categorisation. Riskiness of the business component also may be factored into while assessing the inherent risks. While evaluating the controls, Board oversight, policies, processes, cyber risk management architecture including experienced and qualified resources, training and culture, threat intelligence gathering arrangements, monitoring and analysing the threat intelligence received vis-à-vis the situation obtaining in banks, information sharing arrangements (among peer banks, with IDRBT/RBI/CERT-In), preventive, detective and corrective cyber security controls, vendor management and incident management & response are to be outlined.

2. **Arrangement for continuous surveillance**

   Testing for vulnerabilities at reasonable intervals of time is very important. The nature of cyber-attacks is such that they can occur at any time and in a manner that may not have been anticipated. Hence, it is mandated that a SOC (Security Operations Centre) be set up at the earliest, if not yet been done. It is also essential that this Centre ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

3. **IT architecture should be conducive to security**

   The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times. The same needs to be reviewed by the IT Sub Committee of the Board and upgraded, if required, as per their risk assessment in a phased manner. The risk cost/ potential cost trade off decisions which a bank may take should be recorded in writing to enable an appropriate supervisory assessment subsequently.

   An indicative, but not exhaustive, minimum baseline cyber security and resilience framework to be implemented by the banks (as given in Annex 1[8] of the circular).

   Banks should proactively initiate the process of setting up of and operationalizing a Security Operations Centre (SOC) to monitor and manage cyber risks in real time. (An indicative configuration of the SOC is given in Annex 2[9] the circular).

8. Available at https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN1.pdf

9. https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN2.pdf

4. Comprehensively address network and database security

Recent incidents have highlighted the need to thoroughly review network security in every bank. In addition, it has been observed that many times connections to networks/databases are allowed for a specified period of time to facilitate some business or operational requirement. However, the same do not get closed due to oversight making the network/database vulnerable to cyber-attacks. It is essential that unauthorized access to networks and databases is not allowed and wherever permitted, these are through well-defined processes which are invariably followed. Responsibility over such networks and databases should be clearly elucidated and should invariably rest with the officials of the bank.

5. Ensuring Protection of customer information

Banks depend on technology very heavily not only in their smooth functioning but also in providing cutting-edge digital products to their consumers and in the process collect various personal and sensitive information. Banks, as owners of such data, should take appropriate steps in preserving the Confidentiality, Integrity and Availability of the same, irrespective of whether the data is stored/in transit within themselves or with customers or with the third-party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by banks.

6. Cyber Crisis Management Plan

A Cyber Crisis Management Plan (CCMP) should be immediately evolved and should be a part of the overall Board approved strategy. Considering the fact that cyber-risk is different from many other risks, the traditional BCP/DR arrangements may not be adequate and hence needs to be revisited keeping in view the nuances of the cyber-risk. As you may be aware, in India, CERT-IN (Computer Emergency Response Team – India, a Government entity) has been taking important initiatives in strengthening cyber-security by providing proactive & reactive services as well as guidelines, threat intelligence and assessment of preparedness of various agencies across the sectors, including the financial sector. CERT-IN also have come out with National Cyber Crisis Management Plan and Cyber Security Assessment Framework. CERT-In/NCIIPC/RBI/IDRBT guidance may be referred to while formulating the CCMP.

CCMP should address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment. Banks need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fall out. Banks are expected to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. Among other things, banks should take necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of Service, Distributed Denial of Services (DDoS), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

7. Cyber security preparedness indicators

The adequacy of and adherence to cyber resilience framework should be assessed and measured through development of indicators to assess the level of risk/preparedness. These indicators should be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals. The awareness among the stakeholders including employees may also form a part of this assessment.

8. Sharing of information on cyber-security incidents with RBI

It is observed that banks are hesitant to share cyber-incidents faced by them. However, the experience gained globally indicates that collaboration among entities in sharing the cyber-incidents and the best

practices would facilitate timely measures in containing cyber-risks. It is reiterated that banks need to report all unusual cyber-security incidents (whether they were successful or were attempts which did not fructify) to the Reserve Bank. Banks are also encouraged to actively participate in the activities of their CISOs' Forum coordinated by IDRBT and promptly report the incidents to Indian Banks – Center for Analysis of Risks and Threats (IB-CART) set up by IDRBT. Such collaborative efforts will help the banks in obtaining collective threat intelligence, timely alerts and adopting proactive cyber security measures.

9. Supervisory Reporting framework

It has been decided to collect both summary level information as well as details on information security incidents including cyber-incidents. Banks are required to report promptly the incidents, in the format given in Annex-3.[10]

10. Organizational arrangements

Banks should review the organisational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.

11. Cyber-security awareness among stakeholders / Top Management / Board

It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. Banks should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of the bank's cyber resilience objectives, and require and ensure appropriate action to support their synchronized implementation and testing. It is well recognized that stakeholders' (including customers, employees, partners and vendors) awareness about the potential impact of cyber-attacks helps in cyber-security preparedness of banks. Banks are required to take suitable steps in building this awareness. Concurrently, there is an urgent need to bring the Board of Directors and Top Management in banks up to speed on cyber-security related aspects, where necessary, and hence banks are advised to take immediate steps in this direction.

IMPLICATIONS OF RBI REQUIREMENTS

Security policy and procedures requirements:

1. Define and adopt a comprehensive Cyber Security Framework that includes: –
   - (i) The risks posed by cyber threats, as well as the actions to manage or reduce these risks, must be highlighted in a cyber-security strategy.
   - (ii) Banks must implement a cyber-security policy outlining a plan for combating cyber threats in light of the business's complexity and acceptable levels of risk.
   - (iii) The risk assessment approach may be used to identify major gaps in controls early on, and suitable corrective action can be recommended under the active supervision and monitoring of the IT Committee.
   - (iv) Put in place the measures specified in the Cyber Security Framework requirements.

10. Available at https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN3.pdf

2. Monitoring and surveillance of the Infrastructure:
   (i) Establish a cyber-security testing/assessment procedure on a regular basis to uncover vulnerabilities/security issues in the bank's infrastructure/applications.
   (ii) Establish a Cyber Security Operations Centre (C-SOC) for proactive monitoring with advanced technologies for detection, fast reaction, and data analytics.
   (iii) Ensure that C-SOC covers requirements defined in the guidelines.
3. Testing of the IT infrastructure and architecture audit:
   (i) Establish a cyber security testing/assessment program to identify vulnerabilities/ security flaws in Bank's infrastructure/applications on a periodic basis.
   (ii) Establish Cyber Security Operations Centre (C-SOC) for proactive monitoring using sophisticated tools for detection, quick response and backed by tools for data analytics.
   (iii) Ensure that C-SOC covers requirements defined in guidelines.
4. Setup network and database security:
   (i) Conduct a thorough evaluation of network (firewall rules, port opening/closing, etc.) and database (direct database access, back-end updates, etc.) security.
   (ii) Define and document processes for appropriate business or operational requirements to get access to networks and databases.
5. Securing Customer Information:
   (i) Bank is the owner of customer's personal and sensitive information collected by the Bank.
   (ii) Bank is responsible for securing customer information even when it is with the customer or with third party vendor.
6. Setting up Cyber Crisis Management Plan:
   (i) Create a Cyber Crisis Management Plan (CCMP) that addresses the following needs during a breach: Detection, Response, Recovery, and Containment.
   (ii) Examine the existing BCP/DR (Business Continuity Plan/Disaster Recovery) programme and ensure it is updated to satisfy the needs of modern cybersecurity.
   (iii) Establishing preventive, detective, and corrective measures to safeguard the bank against cyber-threats and to identify, respond to, contain, and recover from any cyber-intrusions as soon as possible.
7. Testing and assessment of the cyber security plan:
   (i) Define indicators to assess and measure adequacy of and adherence to cyber security/resilience framework.
   (ii) Use indicators for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals.
8. Incident monitoring and management processes:
   (i) Improve incident monitoring and management systems for information security incidents and cyber security efforts.
   (ii) Process to be defined to report any abnormal cyber security incidents (whether successful or failed) to the Reserve Bank of India using the methodology outlined in the guidelines.

(iii) Update incident management policies and processes to cleanse and share cyber security issues

9. Setting up an Information Security team:

   Examine the information security organization structure, as well as the duties and responsibilities of the CISO, to verify that cyber security problems are effectively addressed inside the Bank.

10. Training and awareness:

    Hold cyber security awareness and training workshops for all important stakeholders, including the Board of Directors, top management, third-party vendors, customers, and employees.

Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices[11]

The RBI came out with Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on November 7, 2023 with an objective to tighten the governance framework for technology within banking segment. Earlier, the RBI had released the Master Direction on Outsourcing of IT Services released on June 23, 2022 to strengthen control framework for better management of outsourcing of technology services.

Who all will be impacted with these Regulations:

- Banks;
- Small Financial Banks and CICs
- NBFCs
- Service Provider, Fintech and Technology Enabler

The master direction will apply to all RBI regulated entities except local area banks and NBFC-core investment companies. It prescribes procedures and framework for strategic alignment, risk management, resource management, performance management and business continuity/ disaster recovery management. It also provides for periodic reviews of risks, IT and information security risk management framework, information security policy and cyber security policy.

The framework provides for the constitution of three major committees by the regulated entities — IT strategy committee of the board, IT steering committee and information security committee. The regulated entities are also required to designate a senior level executive having no direct reporting relationship with the head of IT Function as 'chief information security officer'. Further, the regulated entities have been recommended to conduct disaster recovery drills at least on a half-yearly basis for critical information and back up data in a secured manner as a business continuity measure.

These guidelines integrate consolidated and updated earlier instructions on IT Governance, Risk, Controls, Assurance Practices, and Business Continuity/Disaster Recovery Management separately released for Banks and NBFCs. **Newly released Master Direction shall come into effect from April 1, 2024**[12]

These guidelines are applicable to the following Regulated Entities (REs), unless explicitly exempted:

- Scheduled Commercial Banks (excluding Regional Rural Banks)
- Small Finance Banks
- Payments Banks

11. Reproduced from Charting the Course: Decoding RBI's Master Direction on IT Governance, Risk, Controls & Assurance Practices. The Digital Fifth. Available at https://thedigitalfifth.com/decoding-rbis-master-direction-on-it-governance/

12. Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices. Available at https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12562

- All Non-Banking Financial Companies (NBFCs) in Top, Upper, and Middle Layers as per Scale-Based Regulation (SBR)
- All India Financial Institutions (NHB, NABARD, EXIM Bank SIDBI, and NaBFID)
- Credit Information Companies

Companies excluded from the scope are:

- Local Area Banks
- NBFC – Core Investment Companies

Regulated Entities are required to establish a robust IT Governance Framework, including governance structure and processes essential to achieve the entity's business/strategic objectives. This framework should define the roles (including authority) and responsibilities of the Board of Directors (Board), Board level Committee, Local Management Committee (in the case of foreign banks operating as branches in India), and Senior Management. It must encompass adequate oversight mechanisms to ensure accountability and mitigate business risks.

RBI's Updated Master Direction: Navigating the Digital Landscape Safely

In response to the dynamic shifts in the financial sector, the Reserve Bank of India (RBI) has recently launched an updated Master Direction, reflecting the profound changes brought about by digital technologies. This article delves into the key drivers behind this strategic move and explores the thematic objectives set by the RBI to strengthen IT governance, risk management, and resilience in the banking sector.

- **Technology becoming central to Banking & Lending services:** Banks rely heavily on technology for daily operations, utilizing core banking systems, online platforms, and mobile applications. This technological dependence extends to risk management and automated decision-making, enhancing overall operational efficiency.
- **Shift in Operating Models of Banks:** The last decade has witnessed a monumental transformation in the financial sector, propelled by the advent of digital technologies. The surge in online services, coupled with competitive pressures and the need for operational efficiency, has paved the way for innovations in Mobility, AIML, APIs, and Cloud Computing. These technological integrations aim to enhance service delivery, elevate customer engagement, and fortify risk management strategies.
- **Rise of Banks-FinTech's Partnership:** Collaborations between traditional financial institutions and FinTech firms have become increasingly prevalent, ushering in a new era of opportunities and challenges. While these partnerships offer benefits, they also introduce complexities in managing IT systems, encompassing aspects such as data security, system integrations, interdependencies, regulatory compliance, vendor management, and shared responsibilities.
- **Increasing impetus on Digital Transformation:** The digital transformation wave underscores the importance of agile technologies, scalability, adaptability, and resilience across the financial spectrum. The ability to navigate these facets effectively is crucial for staying competitive and meeting evolving customer expectations.
- **Continued Cyber Threats:** With increased reliance on digital technologies comes an expanded attack surface for cyber threats. This has led to a surge in cybercrimes, including DDoS attacks, phishing attempts, data breaches, and ransomware attacks. Safeguarding against these threats is imperative for maintaining the integrity of financial systems.
- **Regulatory Monitoring:** The introduction of stringent regulations, such as the Digital Personal Data Protection Act, has heightened the need for financial institutions to ensure the security and compliance of their IT systems. This regulatory scrutiny has prompted the RBI to release updated guidelines, reinforcing the importance of robust IT governance and risk management.

Thematic Objectives of the New RBI Master Directions:

- **Elevating the Role of the Board and Top Management:** The RBI emphasizes the establishment of a Board-level IT strategy committee and an IT steering committee, underscoring the pivotal role of top management in mitigating IT risks.
- **Improving Delivery Capabilities and Excellence:** Encouraging best practices in software development, project management, and IT service management to enhance speed, efficiency, and quality in IT service delivery.
- **Sustaining the Technology Landscape:** Prioritizing regular technology updates, ongoing maintenance, and robust disaster recovery plans to ensure operational efficiency, system security, and business resilience.
- **Fortifying Risk Management:** Mandating regular IT risk reviews and comprehensive risk management frameworks, addressing infrastructure, security, cyber threats, and third party risks.
- **Boosting Security and Resilience:** Enforcing strict security controls, data encryption, regular cyber drills, and enhanced disaster recovery arrangements to fortify the overall security and resilience of IT systems.
- **Enhancing Monitoring & Supervision:** Calling for continuous auditing, regular vulnerability assessments, enhanced reporting on critical systems, and meticulous vendor risk management to bolster monitoring and supervision.

SEBI REGULATIONS GOVERNING AI, CYBER SECURITY AND CYBERSPACE

Established in 1988, the SEBI (Securities and Exchange Board of India) is the regulatory body for securities and commodity markets in India under the Ministry of Finance. It acts as an executive government entity with statutory powers thanks to the SEBI Act of January 1992. SEBI ensures that the needs of market intermediaries, investors, and issuers of securities are met, including safeguarding their data, customer data, and transactions.

As of April 2022, SEBI has six committee members that are required to oversee guidance for cybersecurity initiatives for the Indian market and advise SEBI to develop and maintain cybersecurity requirements following global industry standards. Amid increasing cybersecurity threats to the securities market, SEBI in year 2022 issued an advisory for stock exchanges, depositories and other regulated entities asking them to define roles and responsibilities of chief information security officer and other senior personnel. Also, it asked them to clearly specify the reporting and compliance requirements in the security policy. SEBI Regulated Entities (REs) have been advised to implement these cybersecurity practices as recommended by Financial Computer Security Incident Response Team (CSIRT-Fin). The REs have been asked to proactively monitor the cyberspace to identify phishing websites and report the same to CSIRT-Fin.Additionally, SEBI also communicates with other agencies like NCSC (National Cyber Coordination Center), DoT (Department of Telecommunications), and The Ministry of Electronics and Information Technology (MeitY).

Accordingly, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in e-mail, can establish an important pillar of defense. Given the sophistication and persistence of the threat with a high level of coordination among threat actors, it is important to recognise that many traditional approaches to risk management and governance that worked in the past may not be comprehensive or agile enough to address the rapid changes in the threat environment and the pace of technological change that is redefining public and private enterprise. SEBI implemented guidelines that apply to organizations within its scope — stock brokers, stock exchanges, AMCs (asset management companies), mutual funds, and depository participants, among others. The operating systems and applications should be updated with the latest patches on a regular basis. It further said that security audit or Vulnerability Assessment and Penetration Testing (VAPT) of the application should be conducted at regular basis. Penalties for SEBI non-

compliance, for example, violating disclosure regulations, are mandated with a fine of ₹ 20,000 per day until companies reach compliance.

Indian markets today generate over 550 crore daily order and trade messages in the equity and equity derivative segments. In order to keep pace with the demands and challenges of markets, the Securities and Exchange Board of India (SEBI) is investing in technology to improve its own productivity and speed of response to the market.

With advent of technologies such as machine learning and artificial intelligence, it is essential for a regulator like SEBI to leverage sophisticated algorithms, artificial intelligence and machine learning to address critical challenges for data analytics arising when processing vast amount of data, either structured or unstructured. Further, it is also imperative for it to have resilient infrastructure such as data centres and cloud facilities to safely and effectively manage this ever-increasing data. The regulator has developed a system based on Artificial Intelligence (AI) that scans various stock market shows and builds a database of recommendations made. This database will be a part of the big-data network SEBI is employing to conduct comprehensive surveillance for securities market offences, such as insider trading and front running.

The Securities and Exchange Board of India (SEBI) has asked all mutual funds companies in India to report Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered to investors (individuals and institutions) or used internally by it to facilitate investing and trading or for any other purpose. The move is aimed at conducting a survey for creating an inventory of the AI / ML landscape in the Indian financial markets to gain an in-depth understanding of the adoption of such technologies in the markets and to ensure preparedness for any AI / ML policies that may arise in the future.

As most AI / ML systems are black boxes and their behaviour cannot be easily quantified, it is imperative to ensure that any advertised financial benefit owing to these technologies in investor facing financial products offered by intermediaries should not constitute to misrepresentation.

The SEBI adopted the following key initiatives in recognition of the power of emerging technologies in the recent times in the interest of corporate governance:

- **Adoption of AI for surveillance**: The future of surveillance will entail sophisticated deployment of technology to detect more complex and evolving manipulation techniques by fraudsters. It is proposed that the use of AI for data analytics and pattern recognition will aid SEBI in better identifying abnormal or fraudulent behaviour in the market including front running and insider trading. Technology will be used to simulate human intelligence to further refine its alerts system.
- **Implementation of data lake at SEBI**: This is expected to be achieved through a data lake solution which can support open source analytical tools such as R, Python, etc. with interoperable features. During the year, SEBI completed its tendering process for implementation of the proposed Data Lake. The proposed Data Lake will have characteristics such as visualization, time series/machine learning analytical capabilities, ability to seek and search both structured/unstructured/semistructured data, self-serviced business intelligence capabilities, in memory processing of data etc. The implementation of Data Lake is now underway.
- **Setting up a new and modern data centre**: SEBI had implemented a large scale tier 3+ data center. The new data center is currently hosting SEBI's Private Cloud Infrastructure (SPCI). It is envisaged to consolidate infrastructure from other data centers in Mumbai to the new Data Center. The consolidation of all hardware will increase manageability of server side hardware and result in better turn-around times for service requests.
- **Setting up private cloud infrastructure to facilitate rapid scaling of all systems**: In 2020-21, SEBI implemented its private cloud infrastructure also known as 'SPCI'. It is proposed that new and upcoming projects will utilize the SPCI and in most cases no separate hardware procurements will be required.

Usage of commodity hardware will be encouraged where practicable. The SPCI is already hosting many applications such as Resource Person Portal, File Tracking System (IONS) and Data Lake.

- **Academic programmes**: The National Institute of Securities Markets (NISM) is involved in designing and offering academic programmes that focus on creating a cadre of professionals in securities markets. During the academic year 2020-21, NISM has conducted training programmes on various topics including artificial intelligence, cyber security, blockchain etc. A Post Graduate Certificate in Management (Data Science in Financial Markets) was also organised.
- **Policy initiatives**: With a view to analyse complex bank statements, call data records, internal protocol detail records, hash functions to ensure the sanctity of data, handling of IT digital devices and adoption of data analytics to identify the pattern of relationships for unearthing sophisticated connections while investigating complex cases, a new cell namely 'Connection Research and Analysis Cell' (CRAC) under Integrated Surveillance Department was created in December 2020. Further multiple subcommittees were formed for various projects such as Data Lake, Data Analytics, Private Cloud, Network Revamp, etc.

With a growing reliance on technology, the market infrastructure institutions (MIIs) have fully automated their operations and functions, from order entry to order matching to transaction confirmation, all the way to clearing and settlement of trades. However, according to SEBI, there have been instances of technical problems resulting in business disruption or service unavailability.

SEBI Cyber Security Guidelines, 2023 – Cyber Security and Cyber Resilience framework for Portfolio Managers[13]

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity, and Availability (CIA) of the computer systems, networks, and databases (Confidentiality refers to limiting access of systems and information to authorized users, Integrity is the assurance that the information is reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users). The cyber security framework includes measures, tools, and processes that are intended to prevent cyber-attacks and improve cyber resilience. Cyber Resilience is an organization's ability to prepare and respond to a cyber-attack and to continue operations during, and recover from, a cyber-attack.

With rapid technological advancement in the securities market, there is a greater need for maintaining robust cyber security and to have a cyber resilience framework to protect the integrity of data and guard against breaches of privacy.

As part of the operational risk management, the Portfolio Managers need to have robust cyber security and cyber resilience framework in order to provide essential facilities and services and perform critical functions in the securities market as Portfolio Manager.

Based on feedback received from stakeholders, it has been decided that the guidelines annexed with this circular shall be effective from October 01, 2023.

In this context, Association of Portfolio Managers in India (APMI) shall also furnish activity wise implementation timelines and progress in implementation of provisions of this circular to SEBI on bi-monthly basis.

Portfolio Managers and APMI shall take necessary steps for implementing the circular, including putting the required processes and systems in place to ensure compliance with the provisions of this circular.

Accordingly, all Portfolio Managers with asset under management of INR 3000 crore or more, under discretionary

13. Reproduced from SEBI Circular on Cyber Security and Cyber Resilience framework for Portfolio Managers, March 29, 2023. Available at https://www.sebi.gov.in/legal/circulars/mar-2023/cyber-security-and-cyber-resilience-framework-for-portfolio-managers_69521.html

and non-discretionary portfolio management service taken together, as on the last date of the previous calendar month shall comply with the provisions of Cyber Security and Cyber Resilience as placed at below.

Governance

- As part of the operational risk management framework to manage risk to systems, networks, and databases from cyber-attacks and threats, Portfolio Managers should formulate comprehensive cyber security and cyber resilience policy document encompassing the framework mentioned hereunder. The policy document should be approved by the Board or equivalent body of the Portfolio Manager, and in case of deviations from the suggested framework, reasons for such deviations should also be provided in the policy document.
- The policy document should be reviewed by the Board or equivalent body of the Portfolio Manager at least once annually with the view to strengthen and improve its cyber security and cyber resilience framework.
- The cyber security and cyber resilience policy should include the following process to identify, assess, and manage cyber security risks associated with processes, information, networks, and systems;
  - (a) 'Identify' critical IT assets and risks associated with such assets,
  - (b) 'Protect' assets by deploying suitable controls, tools, and measures,
  - (c) 'Detect' incidents, anomalies, and attacks through appropriate monitoring tools/processes,
  - (d) 'Respond' by taking immediate steps after identification of the incident, anomaly, or attack,
  - (e) 'Recover' from incident through incident management, disaster recovery, and business continuity framework.
- The Cyber security policy should encompass the principles prescribed by the National Critical Information Infrastructure Protection Centre (NCIIPC) of the National Technical Research Organization (NTRO), Government of India, in the report titled 'Guidelines for Protection of National Critical Information Infrastructure' and subsequent revisions, if any, from time to time.
- Portfolio Managers should also incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc., or their subsequent revisions, if any, from time to time.
- Portfolio Managers should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board or equivalent body of Portfolio Manager.
- The Board or equivalent body of the Portfolio Manager shall constitute a Technology Committee comprising experts proficient in technology. This Technology Committee should on a half yearly basis review the implementation of the cyber security and cyber resilience policy approved by their Board or equivalent body, and such review should include a review of their current IT and cyber security and cyber resilience capabilities, set goals for a target level of cyber resilience, and establish a plan to improve and strengthen cyber security and cyber resilience. The review shall be placed before the Board or equivalent body of the Portfolio Manager for appropriate action.
- The Portfolio Managers should establish a reporting procedure to facilitate communication of unusual activities and events to CISO or to the senior management in a timely manner.
- The aforementioned committee and the senior management of the Portfolio Manager, including the CISO, should periodically review instances of cyberattacks, if any, domestically and globally, and take steps to strengthen cyber security and cyber resilience framework.

- Portfolio Managers should define the responsibilities of its employees, outsourced staff, and employees of vendors and other entities, who may have access to or use systems/networks of the Portfolio Managers, towards ensuring the goal of cyber security.

Identify

- Portfolio Manager shall identify and classify critical assets based on their sensitivity and criticality for business operations, services, and data management. The critical assets shall include business-critical systems, internet-facing applications/ systems, systems that contain sensitive data, sensitive personal data, sensitive financial data, Personally Identifiable Information (PII) data, etc. All the ancillary systems used for accessing/ communicating with critical systems either for operations or maintenance shall also be classified as critical assets. The Board or equivalent body of the Portfolio Manager shall approve the list of critical assets.
- To this end, Portfolio Manager shall maintain an up-to-date inventory of its hardware and systems, software and information assets (internal and external), details of its network resources, connections to its network and data flows.
- Portfolio Managers should accordingly identify cyber risks (threats and vulnerabilities) that it may face, along with the likelihood of such threats and impact on the business and thereby, deploy controls commensurate to the criticality.
- Portfolio Managers should also encourage its third-party service providers, if any, such as Custodians, Brokers, Distributors, etc. to have similar standards of Information Security.

Protection

Access Controls

- No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.
- Any access to Portfolio Manager's systems, applications, networks, databases, etc., should be for a defined purpose and for a defined period. Portfolio Manager should grant access to IT systems, applications, databases, and networks on a need-to-use basis and based on the principle of least privilege.
- Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
- Portfolio Manager should implement strong password controls for users' access to systems, applications, networks and databases. Password controls should include a change of password upon first log-on, minimum password length and history, password complexity as well as maximum validity period. The user credential data should be stored using strong and latest hashing algorithms.
- Portfolio Managers should ensure that records of user access are uniquely identified and logged for audit and review purposes. Such logs should be maintained and stored in encrypted form for a time period not less than two (2) years.
- Portfolio Managers should deploy additional controls and security measures to supervise staff with elevated system access entitlements (such as admin or privileged users). Such controls and measures should inter-alia include restricting the number of privileged users, periodic review of privileged users' activities, disallowing privileged users from accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.

- Account access lock policies after failure attempts should be implemented for all accounts.
- Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the Portfolio Manager's critical systems, networks, and other computer resources, should be subject to stringent supervision, monitoring, and access restrictions.
- Two-factor authentication at log-in should be implemented for all users that connect using online/ internet facility.
- Portfolio Managers should formulate an Internet access policy to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc.
- Proper 'end of life' mechanism should be adopted to deactivate access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

Physical Security

- Physical access to the critical systems should be restricted to minimum. Physical access of outsourced staff or visitors should be properly supervised by ensuring at the minimum that outsourced staff or visitors are accompanied at all times by authorized employees.
- Physical access to the critical systems should be revoked immediately if the same is no longer required.
- Portfolio Managers should ensure that the perimeter of the critical equipment rooms is physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.

Network Security Management

- Portfolio Managers should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices, and enterprise mobile devices within the IT environment. The Portfolio Manager should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly. The checks should be done at least once in a year.
- Portfolio Managers should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect their IT infrastructure from security exposures originating from internal and external sources.
- Anti-virus software should be installed on servers and other computer systems. Updation of anti-virus definition files and automatic anti-virus scanning should be done on a regular basis.

Security of Data

- Data-in motion and Data-at-rest should be in encrypted form by using strong encryption methods such as Advanced Encryption Standard (AES), RSA, SHA2, etc.
- Portfolio Managers should implement measures to prevent unauthorized access or copying or transmission of data / information held in contractual or fiduciary capacity. It should be ensured that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- The information security policy should also cover use of devices such as mobile phone, faxes, photocopiers, scanners, etc. that can be used for capturing and transmission of data.
- Portfolio Managers should allow only authorized data storage devices through appropriate validation processes.

Hardening of Hardware and Software

- Only a hardened and vetted hardware / software should be deployed by the Portfolio Managers. During the hardening process, Portfolio Managers should inter-alia ensure that default passwords are replaced with strong passwords and all unnecessary services are removed or disabled in equipments/ software.
- All open ports which are not in use or can potentially be used for exploitation of data should be blocked. Other open ports should be monitored and appropriate measures should be taken to secure the ports.

Application Security and Testing

- Portfolio Managers should ensure that regression testing is undertaken before new or modified system is implemented. The scope of tests should cover business logic, security controls and system performance under various stressload scenarios and recovery conditions.
- Patch Management
- Portfolio Managers should establish and ensure that the patch management procedures include the identification, categorization and prioritization of security patches. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.
- Portfolio Managers should perform rigorous testing of security patches before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
- Disposal of systems and storage devices
- Portfolio Managers should frame suitable policy for disposals of the storage media and systems. The data / information on such devices and systems should be removed by using methods viz. wiping / cleaning / overwrite, degauss and physical destruction, as applicable.

Vulnerability Assessment and Penetration Testing (VAPT)

- Portfolio Managers shall carry out periodic VAPT, inter-alia, including critical assets and infrastructure components like servers, networking systems, security devices, load balancers, other IT systems pertaining to the activities done as Portfolio Manager, etc., in order to detect security vulnerabilities in the IT environment and in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks.
- Portfolio Managers shall conduct VAPT at least once in a financial year. However, for the Portfolio Managers, whose systems have been identified as “protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) under the Information Technology (IT) Act, 2000, VAPT shall be conducted at least twice in a financial year.
- Further, all Portfolio Managers shall engage only Indian Computer Emergency Response Team (CERT-In) empanelled organizations for conducting VAPT.
- The final report on said VAPT shall be submitted to SEBI after approval from Technology Committee of respective Portfolio Manager, within 1 month of completion of VAPT activity.
- Any gaps or vulnerabilities detected shall be remedied on immediate basis and compliance of closure of findings identified during VAPT shall be submitted to SEBI within 3 months post the submission of final VAPT report.
- In addition, Portfolio Managers shall perform vulnerability scanning and conduct penetration testing

prior to the commissioning of a new system which is a critical system or part of an existing critical system.

Monitoring and Detection

- Portfolio Managers should establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices should also be monitored for anomalies.
- Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks, Portfolio Managers should implement suitable mechanism to monitor capacity utilization of its critical systems and networks.
- Suitable alerts should be generated in the event of detection of unauthorized or abnormal system activities, transmission errors or unusual online transactions.

Response and Recovery

- Alerts generated from monitoring and detection systems should be suitably investigated, including impact and forensic analysis of such alerts, in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.
- The response and recovery plan of the Portfolio Manager should aim at the timely restoration of systems affected by incidents of cyber-attacks or breaches. Portfolio Managers should have Recovery Time Objective (RTO) and Recovery Point Objective (RPO) not more than 4 hours and 30 minutes, respectively
- The response plan should define responsibilities and actions to be performed by its employees and support or outsourced staff in the event of cyber-attacks or breach of cyber security mechanism.
- Any incident of loss or destruction of data or systems should be thoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.
- Portfolio Managers should also conduct suitable periodic drills to test the adequacy and effectiveness of response and recovery plan.

Sharing of information

- All cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Managers shall be reported to SEBI within 6 hours of noticing/ detecting such incidents or being brought to their notice about such incidents. The incident shall also be reported to CERT-In in accordance with the guidelines/ directions issued by CERT-In from time to time. Additionally, the Portfolio Manager, whose systems have been identified as “protected system” by NCIIPC, shall also report the incident to NCIIPC. The quarterly reports containing information on cyber-attacks, threats, cyber-incidents, and breaches experienced by Portfolio Manager and measures taken to mitigate vulnerabilities, threats and attacks including information on bugs/ vulnerabilities/ threats that may be useful for other Portfolio Managers shall be submitted to SEBI within 15 days from the quarter ended June, September, December and March of every year. The above information/ reports shall be shared through the dedicated e-mail ids: vapt_reports@sebi.gov.in and cybersecurity_pms@sebi.gov.in

- Such details as are felt useful for sharing with other Portfolio Managers in masked and anonymous manner shall be shared using mechanism to be specified by SEBI from time to time.

Training

Portfolio Managers should conduct periodic training programs to enhance awareness level among the employees and outsourced staff, vendors, etc. on IT / Cyber security policy and standards. Special focus should be given to build awareness levels and skills of staff from non-technical disciplines.

The training program should be reviewed and updated to ensure that the contents of the program remain current and relevant.

Periodic Audit

Portfolio Managers shall arrange to have its systems audited on an annual basis by an independent CISA / CISM qualified or CERT-IN empanelled auditor to check compliance with the above areas and shall submit the report to SEBI along with the comments of the Board or equivalent body of Portfolio Manager within three months of the end of the financial year.

Vendors or Service Providers

Portfolio Managers have outsourced many of their critical activities to different agencies / vendors / service providers. The responsibility, accountability and ownership of those outsourced activities lies primarily with Portfolio Manager.

Therefore, Portfolio Manager have to come out with appropriate monitoring mechanism through clearly defined framework to ensure that all the requirements as specified in this circular is complied with. The periodic report submitted to SEBI should highlight the critical activities handled by the agencies and to certify the above requirement is complied.

1. MeitY Unveils India AI Governance Guidelines under IndiaAI Mission to Ensure Safe, Inclusive, and Responsible Adoption of Artificial Intelligence across Sectors

The Ministry of Electronics and Information Technology (MeitY), under the India AI Mission, unveiled the India AI Governance Guidelines, a comprehensive framework to ensure safe, inclusive, and responsible AI adoption across sectors. The guidelines propose a robust governance framework to foster cuttingedge innovation, and safely develop and deploy AI for all while mitigating risks to individuals and society. The framework comprises four key components:

- Seven guiding principles (Sutras) for ethical and responsible AI.
- Key recommendations across six pillars of AI governance.
- An action plan mapped to short, medium, and long-term timelines.
- Practical guidelines for industry, developers, and regulators to ensure transparent and accountable AI deployment.

INTERNATIONAL PRINCIPLES GOVERNING AI, CYBER SECURITY AND CYBERSPACE: AN OVERVIEW[14]

With few exceptions (most notably, the Budapest Convention on Cybercrime and the not-yet-in-force African Union Convention on Cyber Security and Personal Data Protection), international law does not have tailor-made rules for regulating cyberspace. Moreover, the technology is both novel and dynamic. Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations, including -

- UN General Assembly's First Committee on Disarmament and International Security,
- G20,
- European Union,
- ASEAN, and
- Organization of American States (OAS).

Have affirmed that existing international law applies to the use of Information and Communication Technologies (ICTs) by states. As such, the current discourse centers not on whether international law applies, but rather how it does so.

Major Issues:

Issues surrounding international law's application to cyberspace may be broken into five discrete categories: (i) silence; (ii) existential disagreements; (iii) interpretative challenges; (iv) attribution; and (v) accountability.

OECD AI Principles: Overview[15]

Artificial intelligence (AI) is transforming every aspect of our lives. It influences how we work and play. It promises to help solve global challenges like climate change and access to quality medical care. Yet AI also brings real challenges for governments and citizens alike. As it permeates economies and societies, what sort of policy and institutional frameworks should guide AI design and use, and how can we ensure that it benefits society as a whole? The OECD supports governments by measuring and analysing the economic and social impacts of AI technologies and applications, and engaging with all stakeholders to identify good practices for public policy. The OECD AI Policy Observatory (OECD.AI) combines resources from across the OECD and its partners from all stakeholder groups. It facilitates dialogue and provides multidisciplinary, evidence-based policy analysis and data on AI's areas of impact. It is a unique source of real-time information, analysis and dialogue designed to shape and share AI policies across the globe.

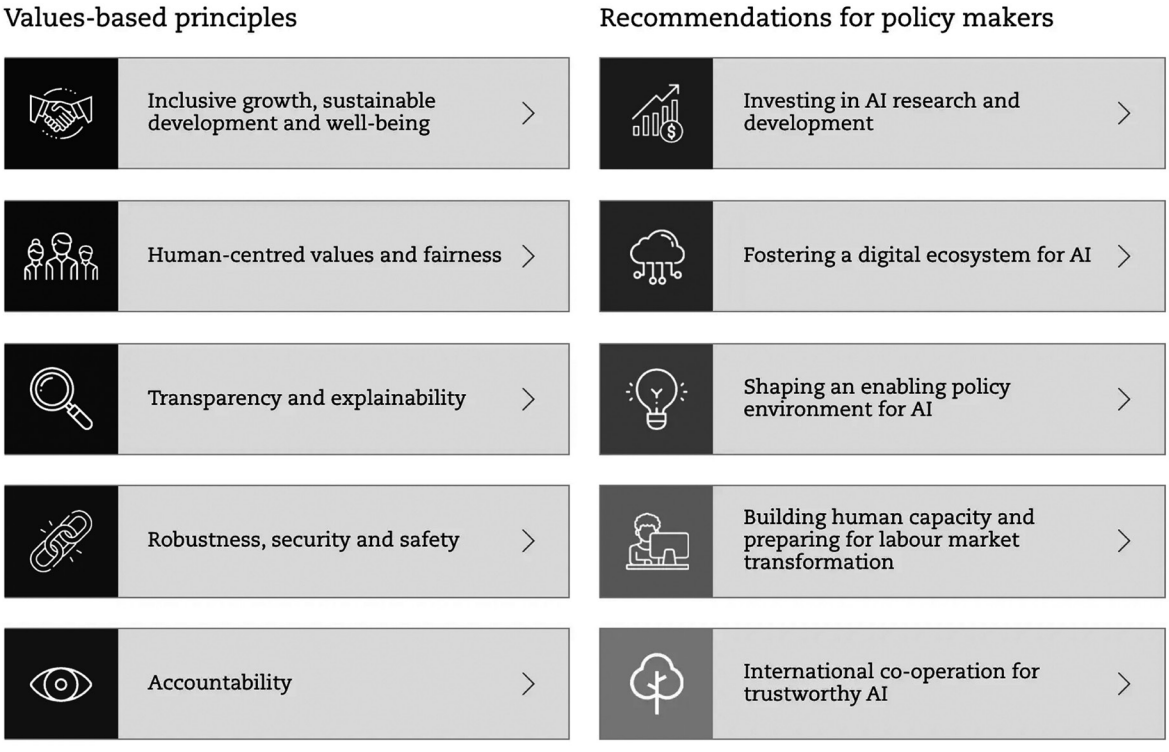
Its country dashboards allow you to browse and compare hundreds of AI policy initiatives in over 60 countries and territories. The Observatory also hosts the AI Wonk blog, a space where the OECD Network of Experts on AI and guest contributors share their experiences and research.

The OECD Principles on Artificial Intelligence promote AI that is innovative and trustworthy and that respects human rights and democratic values. They were adopted in May 2019 by OECD member countries when they approved the OECD Council Recommendation on Artificial Intelligence.

The OECD AI Principles are the first such principles signed up to by Governments. They include concrete recommendations for public policy and strategy, and their general scope ensures they can be applied to AI developments around the world.

14 . Students to note that arena of international principals governing AI, Cyber Security and Cyberspace is quite wide. Hence in this chapter, we are highlighting major bodies guiding the unfirm practice and principles governing/guiding AI, Cyber Security and Cyberspace

15. https://oecd.ai/en/ai-principles



Source: https://oecd.ai/en/ai-principles

Other Applicable Regulatory Framework[16]

In addition to RBI and SEBI which regulates the banking and securities aspects of Indian economy, there are other regulatory bodies also – which aims to enforce cybersecurity regulations in other sectors of Indian economy. These are the main regulating bodies that ensure laws and standards are upheld by all Indian organizations.

1. **Computer Emergency Response Team (CERT-In)**

   Made official in 2004, the Computer Emergency Response Team (CERT-In) is the national nodal agency for collecting, analyzing, forecasting, and disseminating non-critical cybersecurity incidents.

   In addition to cybersecurity incident reporting and notifying, the CERT-In cybersecurity directive helps with issuing guidelines for Indian organizations guidelines as well, offering the best information security practices for managing and preventing cybersecurity incidents.

   The Jurisdiction of Information Technology Rules, 2013 is responsible for mandating all Indian data centers, service providers, and their intermediates. All intermediaries are required to report any cybersecurity incidents to CERT-In.

   CERT-In acts as the primary task force that:

   - Analyzes cyber threats, vulnerabilities, and warning information;
   - Responds to cybersecurity incidents and data breaches;
   - Coordinates suitable incident response to cyber-attacks and conducts forensics for incident handling;

16. Reproduced from Kyle Chin (2023) Top Cyber Security Regulations in India, UpGuard. Available at https://www.upguard.com

- Identify, define, and take suitable measures to mitigate cyber risks;
- Recommend best practices, guidelines, and precautions to organizations for cyber incident management so that they can respond effectively.

CERT-In roles and functions were later clarified in an additional amendment under Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules (IT Rules, 2013).

CERT-In Newest 6-Hour Data Breach Reporting Deadline

The newest regulations by CERT-In address cybersecurity reporting, mandating all Indian companies, service providers, intermediaries, data centers, and businesses to report identified cybersecurity incidents and data breaches within a 6-hour deadline.

However, many Indian organizations disapproved of the impossible requirement, stating that the short reporting window is insufficient to respond to cybersecurity incidents with a detailed report.

Despite the backlash, affected organizations that fail to follow these regulations face up to one-year imprisonment, significant penalties, and non-compliance fines if they fail to report cybersecurity incidents to CERT-In.

2. National Critical Information Infrastructure Protection Center (NCIIPC)

The National Critical Information Infrastructure Protection Center (NCIIPC) was established on January 16, 2014, by the Indian government, under Section 70A of the IT Act, 2000 (amended 2008).

Based in New Delhi, the NCIIPC was appointed as the national nodal agency in terms of Critical Information Infrastructure Protection. Additionally, the NCIIPC is regarded as a unit of the National Technical Research Organization (NTRO) and therefore comes under the Prime Minister's Office (PMO).

The Indian Parliament divides cybersecurity into two segments: "Non-Critical Infrastructure (NCI)," which CERT-In is responsible for, and "Critical Information Infrastructure (CII)," which NCIIPIC is responsible for. CII is defined by the Indian Parliament as "facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation."

NCIIPC is required to monitor and report national-level threats to critical information infrastructure. The critical sectors include:

- Power and energy
- Banking, financial services, and insurance
- Telecommunication and information
- Transportation
- Government
- Strategic and public enterprises

NCIIPC successfully implemented several guidelines for policy guidance, knowledge sharing, and cybersecurity awareness for organizations to conduct preemptive measures of these important sectors, especially in power and energy. The guidelines represent the first means for regulating such sectors and requiring "mandatory compliance by all responsible entities."

Additionally, the Indian government approved the Revamped Distribution Sector Scheme in August 2021. The main goal of this regulation is to improve the operations of DISCOMs (distribution companies) by enhancing the cyber infrastructure with AI-based solutions. This will ultimately aid organizations and companies in meeting the framework's goals.

3. Cyber Regulations Appellate Tribunal (CRAT)

Under the IT Act, 2000, Section 62, the Central Government of India created the Cyber Regulations Appellate Tribunal (CRAT) as a chief governing body and authority for fact-finding, receiving cyber evidence, and examining witnesses.

While CRAT doesn't have as much jurisdiction for cybersecurity notification as CERT-In, the government also serves to respond to and act on related cybersecurity incidents and breaches.

According to the Civil Court and Code of Civil Procedure, 1908, CRAT has the power to:

- Receive evidence on affidavits;
- Ensure that all electronic and cyber evidence and records are presented for court;
- Enforce, summon, and issue regular commissions for examining witnesses, documents, and people under oath;
- Review final decisions of the court to resolve incidents and cases;
- Approve, dismiss, or declare the defaulter's applications as ex-parte.

4. Insurance Regulatory and Development Authority (IRDAI)

The insurance sector of India is regulated by IRDAI, which issues information security guidelines for insurers and addresses the importance of maintaining data integrity and confidentiality.

With this new Information and Cyber Security for Insurers Guidelines, the IRDAI:

- Mandates insurance companies to have a CISO (chief information security officer);
- Puts together an information security committee;
- Creates plans for managing cyber crises;
- Creates and implements cybersecurity assurance programs;
- Implements proper methods for protecting data;
- Maintains risk identification and risk mitigation processes.

The insurance sector of India mainly focuses on areas of higher risk, including ransomware attacks, transaction frauds, data leaks, and risks of violating intellectual property rights. According to a report by Sophos, 68% of Indian organizations were affected by ransomware and resorted to paying ransom to recover their data.

On October 9, 2022, IRDAI introduced an improved cybersecurity framework focused on the insurers' main security concerns. It aims to encourage insurance firms to establish and maintain a robust risk assessment plan, improve mitigation methods of internal and external threats, prevent ransomware attacks and other types of fraud, and implement a strong and robust business continuity.

Depending on the seriousness of the violation, insurers and businesses may be penalized upward of ₹1 lakh (₹100,000). If insurers fail to protect data they may be fined up to ₹5 crores per affected person. The IRDAI Guidelines for Information and Cyber Security for Insurers apply to all insurers regulated by Insurance Regulatory.

5. Telecom Regulatory Authority of India (TRAI) & Department of Telecommunications (DoT)

The Telecom Regulatory Authority of India, along with the DoT (Department of Telecommunication), have tightened regulations for user data privacy and how it's used.

TRAI is a regulatory body, and DoT is a separate executive department of the Ministry of Communications

in India. Although TRAI has been granted more regulatory powers, both works together to govern and regulate telephone operators and service providers.

On June 16, 2018, TRAI released recommendations for telecom providers on "Privacy, Security and Ownership of the Data in the Telecom Sector." In the newest guidelines, TRAI addresses newer responsibilities governing consumer data because most digital transactions in India are done via cell phones.

TRAI addresses data protection with the following objectives:

- Define and understand the scope of "Personal data, Ownership, and Control of Data," namely, the data of users of the telecom service providers;
- Understand and identify the "Rights and Responsibilities of Data Controllers";
- Assess and identify the efficiency of how data is protected and which data protection measures are currently in place in the telecommunications sector;
- Identify and address critical issues regarding data protection;
- Collect and control user data of TISP (traffic information service providers) services.

The DoT has collaborated with the Indian IT ministry to impose layered data consent rules that safeguard personal data processing. This gives users the freedom to decide whether or not they will consent to the usage of their personal data and the right to withdraw consent at any time.

The new rules state that organizations and companies will only have to collect the necessary user details and that the data may be retained only for as long as required. Additionally, Indian telecommunications service providers comply with common standards like ISO 27000, 3GPP and 3GPP2, and ISO/IEC 15408.

LESSON ROUND-UP

- E-Governance as the name suggest is made up of two words. "E" and "Governance".
- Demands of transparency, ethics, rightfulness, access to justice, eradication of corruption and other related issues along with welfare driven political leadership, other associated governments, capacity building needs and perceived citizen expectations and all has contributed to adoption of e-government methods for good governance.
- The National e-Governance Plan (NeGP) has been formulated by the Department of Electronics and Information Technology (DEITY) and Department of Administrative Reforms and Public Grievances (DARPG) in 2006.
- These technologies are increasingly used by the society in day-to-day life from personal communications, buying goods at retail stores, availing services at doorstep to availing the governance through government offices.
- Seeing the potential of digitalization and its constructive impact supporting inclusive development of our country, Government of India has launched the "Digital India" campaign. The Digital India drive envisions transforming our nation and creating opportunities for all citizens by harnessing digital technologies.
- The advent of information and communication technology has revolutionized all the sectors across the globe. Indian banking and financial sector are not an exception to the transformation that has happened with the advent of information technology.

- Of all the IT domains that are impacting this industry, Artificial Intelligence (AI) and Data Analytics are the most influential contenders.
- Machine Learning (ML) and Artificial Intelligence (AI) are already being used in supervisory procedures by RBI. It now intends to make sure that the Department of Supervision at the central bank may reap the rewards of advanced analytics.
- Additionally, they have plans to bring in outside consultants for this work. For supervisory tests, the department has been creating and utilizing linear and a few ML models. Urban cooperative banks (UCBs), non-bank financial businesses (NBFCs), payment banks, small financing banks, neighborhood banks, credit information firms, and a few more Indian financial organizations are all subject to the RBI's regulatory authority.
- The RBI came out with Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices on November 7, 2023 with an objective to tighten the governance framework for technology within banking segment.
- Earlier, the RBI had released the Master Direction on Outsourcing of IT Services released on June 23, 2022 to strengthen control framework for better management of outsourcing of technology services.
- These guidelines integrate consolidated and updated earlier instructions on IT Governance, Risk, Controls, Assurance Practices, and Business Continuity/Disaster Recovery Management separately released for Banks and NBFCs.
- Newly released Master Direction shall come into effect from April 1, 2024
- Governance structure and processes essential to achieve the entity's business/strategic objectives.
- This framework should define the roles (including authority) and responsibilities of the Board of Directors (Board), Board level Committee, Local Management Committee (in the case of foreign banks operating as branches in India), and Senior Management. It must encompass adequate oversight mechanisms to ensure accountability and mitigate business risks.
- As of April 2022, SEBI has six committee members that are required to oversee guidance for cybersecurity initiatives for the Indian market and advise SEBI to develop and maintain cybersecurity requirements following global industry standards.
- Additionally, SEBI also communicates with other agencies like CERT-In, NCSC (National Cyber Coordination Center), DoT (Department of Telecommunications), and The Ministry of Electronics and Information Technology (MeitY).
- SEBI implemented guidelines that apply to organizations within its scope — stock brokers, stock exchanges, AMCs (asset management companies), mutual funds, and depository participants, among others.
- With rapid technological advancement in the securities market, there is a greater need for maintaining robust cyber security and to have a cyber resilience framework to protect the integrity of data and guard against breaches of privacy.
- As part of the operational risk management, the Portfolio Managers need to have robust cyber security and cyber resilience framework in order to provide essential facilities and services and perform critical functions in the securities market as Portfolio Manager.
- Accordingly, all Portfolio Managers with asset under management of INR 3000 crore or more, under discretionary and non-discretionary portfolio management service taken together, as on the last date of the previous calendar month shall comply with the provisions of Cyber Security and Cyber Resilience, which has been put to effect from October 01, 2023.

- Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations governs AI, cyber security and cyberspace.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation.)

1. Briefly explain the concept of e-governance and types of e-governance.
2. Write a short note on RBI Circular on Cyber Security and its present-day impact on Banking Industry.
3. Write a brief note on compliance required to be followed as per SEBI Cyber Security Guidelines, 2023 – Cyber Security and Cyber Resilience framework for Portfolio Managers.
4. Write short note on any two of the following:
    - Vulnerability Assessment and Penetration Testing (VAPT)
    - Data Incident Reporting
    - RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (November 7, 2023).

LIST OF FURTHER READINGS

- Nisha Dewani and Others (2022) Handbook of Research on Cyber Law, Data Protection and Privacy
- RBI Guidelines for Cyber Security, Deloitte Report, July 2016
- RBI Cyber Security Framework in India, Value Mentor, 2020
- RBI Circular on Cyber Security, PwC
- Walters and Novak (2021) Cyber Security, Artificial Intelligence, Data Protection and Law, Spinger.

LIST OF OTHER REFERENCES

- CSC 2.0 – Aims to cover 2.5 Lakhs of Gram Panchayats for Maximising delivery of e-Services to the citizens, The Digital India Campaign, Ministry of Electronics and Information Technology, Government of India;
- Digital India – Power to Empower, Ministry of Electronics and Information Technology, Government of India;
- Digital India – Unlocking the Trillion Dollar Opportunity (2016), A Report by Deloitte in association with ASSOCHAM India;
- Deepak J.S. (2015), Digital India-The Way Forward, MyGov Blog, Government of India;
- Ghosh Shyamal (2015), Digital India-Way Forward, Broadband India Forum, The Broadcast and Cable Set, India;
- Sengupta Deb Deep (2015), Digital Transformation-An Only Way Forward, December 2, 2015, The Live Mint;
- Teletalk 2016 – Digital India: The Way Forward, (2016), MITSOT, MIT School of Telecom Management's Blog.

Data Analytics and Law

Lesson 6

KEY CONCEPTS

■ Data ■ Analytics ■ Data Analytics ■ Legal Analytics ■ Machine Learning ■ Logistic Regression ■ Triple C Theory ■ Data Assessment

Learning Objectives

To understand:

- What is Data analytics?
- Different analytical methods and techniques used by data analysts
- What is Machine Learning?
- What is Artificial Intelligence and how it helps human being
- What is Triple C Theory?

Lesson Outline

- Introduction to Data Analytics
- Introduction to Legal Analytics
- Introduction to Machine Learning for Lawyers
- Quantitative Legal Prediction vis-à-vis Business of Law
- Bias/ Variance, Precision/Recall & Dimensionality
- Overfitting, Underfitting, & Cross-Validation
- Logistic Regression and Maximum Likelihood
- Triple C Theory and Data Assessment
- Network Analysis and Law
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

INTRODUCTION

In modern times, industry whether legal or technology, academy, practitioners and scholars utilize Artificial Intelligence (AI) and machine learning to perform analysis which used to be labor-intensive endeavors decade back. Although technology can, in some instances, replicate human decision-making, yet professionals including lawyers, researchers and scholars play an essential role in compiling data sets, defining analytical queries, and, most importantly, interpreting findings and presenting them in an accessible way for a broad audience. Hence, this chapter aims to provide the basis for understanding data analytics, its role in various sectors and laws, if any, governing the same.

DATA ANALYTICS[1]

As data is becoming more prominent by the minute, organizations are becoming data-driven, which means adopting methods to collect more data. This data is then sorted, stored, and then analyzed to derive logical and valuable information. Data analytics makes the process possible.

Data analytics is the science of analyzing raw data to make conclusions about that information. Many of the techniques and processes of data analytics have been automated into mechanical processes and algorithms that work over raw data for human consumption.

- Data analytics is the science of analyzing raw data to make conclusions about that information.
- Data analytics help a business optimize its performance, perform more efficiently, maximize profit, or make more strategically-guided decisions.
- The techniques and processes of data analytics have been automated into mechanical processes and algorithms that work over raw data for human consumption.
- Various approaches to data analytics include looking at what happened (descriptive analytics), why something happened (diagnostic analytics), what is going to happen (predictive analytics), or what should be done next (prescriptive analytics).
- Data analytics relies on a variety of software tools ranging from spreadsheets, data visualization, and reporting tools, data mining programs, or open-source languages for the greatest data manipulation.

Data analytics is the process that refers to deriving valuable insights and information from data using quantitative and qualitative methods. It helps businesses and even in science - researchers use it to verify their theories. Data analytics is a broad term that encompasses many diverse types of data analysis. Any type of information can be subjected to data analytics techniques to get insight that can be used to improve things. Data analytics techniques can reveal trends and metrics that would otherwise be lost in the mass of information. This information can then be used to optimize processes to increase the overall efficiency of a business or system.

For example, manufacturing companies often record the runtime, downtime, and work queue for various machines and then analyze the data to better plan the workloads so the machines operate closer to peak capacity.

Data analytics is important because it helps businesses optimize their performances. Implementing it into the business model means companies can help reduce costs by identifying more efficient ways of doing business and by storing large amounts of data. A company can also use data analytics to make better business decisions and help analyze customer trends and satisfaction, which can lead to new—and better—products and services.

1. Source: Jake Frankefield at el (2023) Data Analytics: What it is, How It's Used and 4 Basic Techniques, Investopedia. Available at https://www.investopedia.com/terms/d/data-analytics.asp

Kinds of Data collected by Company

There are three primary kinds of data collected by the companies.

- *First-party data*: The data a company collects about its customers.
- *Second-party data*: The data a company gets from a known organization that collected it originally.
- *Aggregated data*: The data a company buys from a marketplace.

The Evolution of Data Analytics

Data analytics has become the next big thing in both large companies and small startups. The process of data analytics has evolved. Let's take a journey through the evolution of data analytics.

- **Data Analytics and Statistics:** Statistics has a pretty long history. Like, for example, in taxation, governments carried out planning activities for the creation of censuses. It was possible with the use of statistics. Data analytics stemmed from statistics, which analyzed the obtained data.

> Tabulating Machine* was counting machine which comprised of a punch for entering data onto a blank card, a tabulator for reading the cards and summing up information and a sorting box for sorting the cards for further analysis. The invention of the Tabulating Machine was a turning point as it transformed the census process and information processing in general.

- **Data Analysis and Computing:** Technology advancements were game-changers to how businesses adopted data analytics. In 1890, Herman Hollerith invented the "Tabulating Machine" to reduce the time taken to create the Census. This machine was highly useful in finishing the 1890 US Census in only 18 months.

- **Data mining:** Data mining got introduced in the 1990s, which is a process that discovers patterns in large data files. When data analytics moved from traditional methods to more modern means, you could obtain more positive results.

> Data mining refers to the process of sieving through large amounts of information for the purpose of extracting useful information.

- **Google Web Search:** When the Google search engine came into the picture, big data could be analyzed and processed quickly. It played an essential part in the evolution of Data Analytics because the search engine was more automated, scalable, and high-performing.

*(*Source: https://americanhistory.si.edu/collections/search/object/nmah_694410*)

- **Data Processing:** Today, Python & R are the leading technologies in data analytics. They are open-sourced and are capable of integrating with big data platforms and visualization tools. Businesses prefer R when the primary goal is exploratory analysis or modeling. At the same time, enterprises prefer Python to develop applications that have an embedded analytics engine.
- **Predictive Modeling:** Some advanced data analytics techniques that the data scientists and organizations are using are: Random Forests, Matrix Factorization, TensorFlow, Simulated Annealing, etc. For example, Random Forest is a machine learning algorithm which grows and combines multiple decision trees to create a forest. It is used for both classification and regression problems.
- **Visualization:** Many organizations are adopting more open-source technologies for their business. A few examples are D3 and Angular, which is popular development platform which strives to make web development easier through focus on developer's productivity, speed and testability. This decision relies on several factors like cost, customization options, visual appeal, and interactivity.

Data Analysis Steps

The process involved in data analysis involves several different steps:

- The first step is to determine the data requirements or how the data is grouped. Data may be separated by age, demographic, income, or gender. Data values may be numerical or be divided by category.
- The second step in data analytics is the process of collecting it. This can be done through a variety of sources such as computers, online sources, cameras, environmental sources, or through personnel.
- Once the data is collected, it must be organized so it can be analyzed. This may take place on a spreadsheet or other form of software that can take statistical data.
- The data is then cleaned up before analysis. This means it is scrubbed and checked to ensure there is no duplication or error, and that it is not incomplete. This step helps correct any errors before it goes on to a data analyst to be analyzed.

Types of Data Analytics

Following are the main types of data analytics: descriptive, diagnostic, predictive, and prescriptive. Each has its own set of goals and roles in the data analytics process.

1. **Descriptive Analytics:**

   This describes what has happened over a given period of time. Descriptive analytics answers the "what" questions in the data analytics process. It helps stakeholders understand large datasets by summarizing them. The descriptive analysis tracks the organization's past performance. It includes the following steps:

   - Data collection: It refers to the process of gathering data for a specific purpose.
   - Data processing: It refers to the process of converting raw data into useful information.
   - Data analysis: It refers to the process of inspecting, analyzing and transforming the data with the object of discovering useful information and conclusions to support decision making.
   - Data visualization: It refers to the process of representing the data into pictorial modes like graphs, charts, plots and animations.

2. **Diagnostic Analytics**

   This focuses more on why something happened. This involves more diverse data inputs and a bit of hypothesizing. Diagnostic analytics answers the "why" questions in the data analytics process. It analyzes the results from the descriptive analysis and then further evaluates it to find the cause. The diagnostic analysis process takes place in three steps:

   - Identifying any unexpected changes in the data.
   - Data related to the changes is collected.
   - Statistical techniques help find relationships and trends related to the changes.

3. **Predictive Analytics**

   This moves to what is likely going to happen in the near term. The purpose of predictive analytics is to answer questions about the future of the data analytics process. The past data identifies the trends. The techniques used in the process include statistical and machine learning techniques. A few of them

are neural networks, decision trees, and regression.

4. **Prescriptive Analytics**

   This suggests a course of action. Prescriptive analysis helps businesses make well-informed decisions and predict the analytics. This type of data analytics uses machine learning strategies that are capable of finding patterns in large datasets.

> **Note:** Data Set refers to an organized collection of data related to a particular subject.

Data Analytics Techniques

There are several different analytical methods and techniques data analysts can use to process data and extract information. Some of the most popular methods are listed below.

- **Regression analysis** entails analyzing the relationship between dependent variables (i.e. the variable which is being tested and measured in a scientific experiment) to determine how a change in one may affect the change in another.
- **Factor analysis** entails taking a large data set and shrinking it to a smaller data set. The goal of this maneuver is to attempt to discover hidden trends that would otherwise have been more difficult to see.
- **Cohort analysis** is the process of breaking a data set into groups of similar data, often broken into a customer demographic. This allows data analysts and other users of data analytics to further dive into the numbers relating to a specific subset of data.
- **Monte Carlo simulations** is a data analysis model which assesses the possible outcomes of an uncertain event. This method conducts repeated random sampling to make estimations of unknown parameters. Often used for risk mitigation and loss prevention, these simulations incorporate multiple values and variables and often have greater forecasting capabilities than other data analytics approaches.
- **Time series analysis** tracks data over time and solidifies the relationship between the value of a data point and the occurrence of the data point. This data analysis technique is usually used to spot cyclical trends or to project financial forecasts.

Data Analytics Tools

- In addition to a broad range of mathematical and statistical approaches to crunching numbers, data analytics has rapidly evolved in technological capabilities. Today, data analysts have a broad range of software tools to help acquire data, store information, process data, and report findings.
- Data analytics has always had loose ties to spreadsheets and Microsoft Excel. Now, data analysts also often interact with raw programming languages to transform and manipulate databases. Open-source language, which is a programming language that can be freely used and modified by users, for example Python, are often utilized. More specific tools for data analytics like R can be used for statistical analysis or graphical modeling.
- Data analysts also have help when reporting or communicating findings. Both Tableau and Power BI are data visualization and analysis tools to compile information, perform data analytics, and distribute results via dashboards and reports.

> Tableau is a popular tool for business intelligence which is used for the purpose of visually analyzing the data.

- Other tools are also emerging to assist data analysts. SAS is an analytics platform that can assist with

data mining, while Apache Spark is an open-source platform useful for processing large sets of data. Data analysts now have a broad range of technological capabilities to further enhance the value they deliver to their company.

INTRODUCTION TO LEGAL ANALYTICS

Traditionally, lawyers have won cases with only two weapons in their arsenal- Research and Reasoning. However, with legal data analytics, lawyers are gaining a critical advantage in their practice.

Legal Data Analytics: Meaning

Data analytics is the process of analyzing data collected over a long period of time to discover useful information. It can help gain insights on how the variables behave under different circumstances. Legal analytics serves as a supplement that boosts legal research. It can provide lawyers with the margin necessary for victory.

Legal analytics, with the help of data processing technologies, helps lawyers clean up, collate, and structurally analyze data. This data is collected from various cases, instances, law books, or online legal directories.

For example, through legal analytics, a lawyer can analyze past data to find out how long will a case run for, what were the previous outcomes of similar cases based on similar facts, how the judge behaved in similar scenarios, and so on.

With data analytics, lawyers can find out answers within minutes, which would have taken hours or weeks of manual efforts otherwise. Additionally, analytics software can catch simple variations in data that the human mind might not be able to comprehend.

Advantage of Legal Data Analytics:

Majority of legal professionals agree that using legal analytics makes them a better, more efficient, and effective legal practitioner.

1. **Edge over Competitors:**

   With data analytics, you get insights on judges' behavior, arguments made in the past, plea deals that have worked and so on. This data can help you predict the shape of the present case you are dealing with.

   In short, lawyers can build strong litigation strategies that succeed by deriving information from real-life scenarios. With data analytics, lawyers do not need to go over volumes of past case laws and law text books. Legal data analytics can strengthen the overall legal research methodology and enable the lawyers to arrive at a conclusion.

2. **Predict Results and Update Case Strategy:**

   Data analytics can aid lawyers in getting answers to client queries backed with illustrations and information. However, it is wrong to assume that legal analytics can only help lawyers in solving cases or doing research. It can also assist in making important business decisions related to the expansion or future planning of law firms. Other professionals in the legal domain can also use legal analytics. They can identify industry trends, run competitor analysis, study litigation history of opposition counsel, and so on.

3. **Exploring Strategies:**

   Lawyers can augment the ways of legal analytics to experiment with various legal strategies and scenarios. This way lawyers can predict case outcomes easily. Think of it as a science experiment where you play with the variables to come up with different results.

Implementing Data Analytics to Legal Practice:

Data in law industry can be broadly classified into individual data, law firm data, and industry data. Individual data is the data that one has in one's personal repository. The other two are broad-based organizational data available in law firm, companies, industry, on the internet, or in legal research libraries. With the advent of machine learning, artificial intelligence, and natural language processors, SaaS & service providers can make legal data analytics easy. They can do so by training computers to process a large amount of information at unmatchable speed and accuracy.

However, with the human element attached to each case, it cannot be said that legal output can be entirely depend on data analytics. We recommend to understand that legal analytics is tool of facilitation and improving efficiency of legal results rather than a replacement or a solution for all legal cases and client needs.

One has to note that Legal analytics support legal industry in decision-making in the following major areas:

- Compliance and regulatory support
- Internal investigations
- Fraud, waste, and abuse
- Incident response.

Business of Law Analytics vis-à-vis Practice Law Analytics[2]

Business of law analytics is used by legal operations and generally includes data related to legal spend, vendors, billing, and matters. These metrics enable functioning of legal operations as in a cost-controlled manner. Additionally, business of law analytics gives legal departments data-based evidence to prove how their work helps businesses.

1. **Spend analytics**

   Spend analytics are based on the total legal spend as well as details like spend to budget, spend by practice area, timekeeper rates, and more.

2. **Vendor analytics**

   Vendor analytics are based on assessment of the total list of vendors along with information like average matter cycle times, hourly rates, the use of alternative fee arrangements, and more. Vendor analytics also serve as evidence to back up departmental decisions to end vendor relationships. Vendor analytics enables assessment of the individual performance of each vendor, which is then compared with performance of other vendors, to understand which vendors are meeting expectations and thus deserve to be retained in the firm's portfolio.

   Without this type of detailed insight, it's difficult to figure out which vendors are (or aren't) worth working with.

3. **Billing analytics**

   Billing analytics are based on the total list of invoices along with information like status of invoice approval, status of accrual, violation of billing guidelines, and more. With insights from billing analytics, legal departments have a clearer idea of what's going on and can take the initiative to communicate with vendors and resolve issues before final invoices reach accounting.

2. Reproduced from Wen Kara (2022) What are the different types of legal data analytics? SimpleLegal. Available on https://www.simplelegal.com/blog/legal-data-analytics.

4. **Matter analytics**

Matter analytics are based on the total list of legal matters along with details like status of matters, vendors assigned to each matter, when the matter was worked, and more. Detailed matter analytics allow corporate legal departments to make educated decisions on using certain outside counsels vs. in-house counsels. After identifying the practice areas, they can use this information along with vendor costs to explore reducing the number of vendors and consolidating into law firms with multiple legal services. Legal departments can also assign standard, due diligence and compliance work to in-house attorneys to save money.

Practice of Law Analytics

Practice of law analytics gives in-house counsels insight that supports the legal practice, including data on legal contracts and cases. These metrics help attorneys with legal decision-making and risk management.

Contract Analytics

Contract analytics are based on the total list of legal contracts as well as detailed information on their status, type, renewal dates, content, and more.

As legal technology continues to evolve, contract analytics has also grown more advanced to include suggested revisions from artificial intelligence. While many basic legal platforms can sort and categorize contracts, AI legal software reviews them. With machine learning, these tools flag issues in contracts and offer changes based on their analysis of others contracts in the system. This saves lawyers "hundreds of hours" a year.

Case Analytics

Case analytics are based on the total list of legal cases along with information on prior and similar cases, case types, clients, judges, and more. Case analytics help in-house counsels to prepare their case strategy by learning from previous cases. With case analytics, attorneys can see trends on what worked and what didn't and apply those lessons to strengthen their legal approach towards complex legal issues.

INTRODUCTION TO MACHINE LEARNING FOR LAWYERS

Whenever any professional sector faces new technology, concern arises regarding how that technology will transform operations and the careers of those who choose that profession. And lawyers and the legal profession are no exception. Today, artificial intelligence (AI) is beginning to transform the legal profession in many ways and aims to take on higher-level tasks such as providing advice to clients, negotiating deals and drafting standard contracts.

Use of Artificial Intelligence and Machine Learning in Law[3]

Artificial intelligence mimics certain operations of the human mind and is the term used when machines are able to complete tasks that typically require human intelligence. The term machine learning is when computers use rules (algorithms) to analyze data and learn patterns and gain insights from the data. Artificial intelligence is aims to bring about a major shift in the way legal work is done.

Review Documents and Legal Research

AI-powered software improves the efficiency of document analysis for legal use and machines can review documents and flag them as relevant to a particular case. Once a certain type of document is denoted as

3. Bernard Marr and Company, How AI and Machine Learning Are Transforming Law Firms and The Legal Sector, Forbes. Available at https://bernardmarr.com/how-ai-and-machine-learning-are-transforming-law-firms-and-the-legal-sector/

relevant, machine learning algorithms can get to work to find other documents that are similarly relevant. Machines are much faster at sieving through documents as compared to humans and can produce output and results that can be statistically validated. They can help reduce the load on the human workforce by forwarding only those documents which are questionable rather than requiring humans to review all documents. Despite the monotony that legal research entails, it is important that legal research is done in a timely and comprehensive manner. AI systems such as the one offered by ROSS Intelligence leverages natural language processing to help analyze documents.

For example, when lawyers using AI-powered software flag certain documents as relevant, the AI learns what type of documents it's supposed to be looking for. Hence, it can more accurately identify other relevant documents. This is called "predictive coding." Predictive coding offers many advantages over old-school manual document review. Among other things, it:

- leverages small samples to find similar documents;
- reduces the volume of irrelevant documents that attorneys must wade through;
- produces results that can be validated statistically;
- is at least modestly more accurate than human review;
- is much faster than human review.

Help perform Due Diligence

In law offices around the world, paralegals and other legal professionals are kept busy conducting due diligence to uncover background information on behalf of their clients. This works includes confirming facts and figures and thoroughly evaluating the decisions on prior cases to effectively provide counsel to their clients. Artificial intelligence tools can help these paralegals to conduct their due diligence more efficiently and with more accuracy since this work is often tedious for humans.

Contract Review and Management

A big portion of work that legal professionals do on behalf of clients is to review contracts to identify risks and issues with how contracts are drafted that could have negative impacts for their clients. They redline items, edit contracts and counsel clients if they should sign or not or help them negotiate better terms.

For example, analysis of all contracts a company has signed can identify risks, anomalies, future financial obligations, renewal and expiration dates, etc. For companies with hundreds or thousands of contracts, this can be a slow, expensive, labour-intensive, and error-prone process (assuming the contracts aren't already entered into a robust contract management system). It's also boring for the lawyers (or others) tasked with doing it.

On a day-to-day basis, lawyers review contracts, make comments and redlines, and advise clients on whether to sign contracts as it is or try to negotiate better terms. These contracts can range from simple (e.g., NDAs) to complex (share subscription agreements). A backlog of contracts to review can create a bottleneck that delays deals (and the associated revenues). Lawyers (especially inexperienced ones) can miss important issues that can come back to bite their clients later.

AI can help analyze contracts in bulk as well as individual contracts.

Predict Legal Outcomes

AI has the capability of analyzing data to help it make predictions about the outcomes of legal proceedings better than humans. Clients are often asking their legal counsels to predict the future with questions such as "If we go to trial, how likely will it be that I win?" or "Should I settle?". With the use of AI that has access to years of trial data and record, lawyers are able to better predict the answers to such questions.

Legal Research

Any lawyer who has ever done research using legal research tools has used legal automation. Finding relevant cases in previous and recent years involves the laborious process of looking up headnote numbers and going through voluminous paper volumes. But AI takes legal research to the next level. For example, Ross Intelligence uses the power of IBM's Watson supercomputer to find similar cases. It can even respond to queries in plain English. The power of AI-enabled research is striking: using common research methods, a bankruptcy lawyer found a case nearly identical to the one he was working on in 10 hours; Whereas Ross's AI found it almost instantly.

Data Incorporated into Legal Analytics [4]

Legal analytics tools collect three broad categories of data and turn it into useful insights:

- Individual data,
- Internal data, and
- Legal industry data.

Individual data is information about a firm's current and future clients, including information that is collected whenever someone peruses the firm's website. This encompasses information collected from consultation request forms and data about how potential clients interact with the website, such as search terms used and time spent on particular pages. Individual data can also include client data stored within a firm or corporate law firm's secure file storage system. With that data, certain legal analytics tools can analyze documents and document metadata to inform case management and guide eDiscovery strategy.

Note: eDiscovery is a resource that seeks to find evidence in emails, business communications and other electronic data and collects, preserves, reviews and exchanges information in electronic format for use in litigation and investigation.

Internal data is information about a firm or law department's business practices, such as billing rates, legal expenditure incurred in practice areas, and billable hours. This data might also include productivity data related to individual lawyers and support staff.

Legal industry data is data that has been externally collected from outside research groups, court dockets, and sources that cover the wider trends within the legal community. This might include data about case outcomes or trends about hot practice areas or changing client preferences.

Ways to use Legal Analytics[5]

Legal analytics has changed over the years, and providers are constantly updating their software and improving functionality to adapt. While early legal analytics software generally provided fewer features, the advanced tools available today serve a wide range of goals for legal professionals. Below are five ways to use legal analytics tools.

1. **Streamlining eDiscovery**

   While eDiscovery was once tedious and time-consuming, legal analytics tools have helped lawyers simplify its complex processes, making it both more efficient and more useful for determining likely

4. Reproduced from Wolff Jeffrey (2021) 5 Ways to Use Legal Analytics Tools to Work Smarter, Not Harder, JD SUPRA. Available at https://www.jdsupra.com/legalnews/5-ways-to-use-legal-analytics-tools-to-5039823/

5. Reproduced from Wolff Jeffrey (2021) 5 Ways to Use Legal Analytics Tools to Work Smarter, Not Harder, JD SUPRA. Available at https://www.jdsupra.com/legalnews/5-ways-to-use-legal-analytics-tools-to-5039823/

case outcomes and guiding litigation or settlement strategies. These tools detect trends and patterns in client data using artificial intelligence to help lawyers understand data better and make better strategic decisions.

- Structural analytics can give an overview of the scope of a data set. For example, analytics tools can study file metadata to organize files, while email threading and duplicate and near-duplicate detection can streamline data sets.
- Conceptual analytics can help lawyers understand the relationships between documents and provide a high-level overview of a corpus of documents. These tools can recognize concepts and use them to group related documents together and can even identify the sentiment or emotion behind documents, flagging concerning documents for review.
- Finally, predictive analytics, such as technology-assisted review, can prioritize the documents most likely to be relevant and make informed predictions about privileged documents or content; they can also detect and classify contract clauses.

With these insights, legal teams can conduct more accurate early case assessment, reduce the volume of eDiscovery data advancing to review, accelerate and improve the quality of document review, and substantially lower the total cost of eDiscovery.

2. Facilitating Law Firm Marketing and Increasing Client Satisfaction

A law firm is, quite literally, nothing without its clients. Fortunately, legal analytics tools have revolutionized lawyers' ability to recognize "ideal" clients and design effective marketing strategies to capture those clients. Many helpful tools can analyze the characteristics of the ideal client, identify the target market to maximize profitability, and channel business to the firm.

These tools can also help with benchmarking. For example, law firm can compare their performance against peer firms. Similarly, instead of wasting money on unsuccessful marketing campaigns, legal analytics tools can help a firm craft a plan—based on real data—to target and draw in lucrative clients and increase the firm's profitability.

3. Making Informed, Risk-based Litigation Decisions

Clients are in the pesky habit of asking their lawyers to predict the future, but few lawyers are naïve enough to make the attempt. Predictive legal analytics tools, however, give lawyers the next best thing: a way to accurately predict the specific characteristics of a case based on real case data.

For example, modern analytics tools can predict the likelihood of winning a case, the probable length of litigation, and the number of hours that the firm should allocate to working on it, all based on past data. This insight is invaluable for saving time and money because it lets the counsel know which battles are worth fighting and which should be promptly settled (and for how much). The best part is that these predictions are personalized based on the specific jurisdiction, judge, and even opposing counsel in question.

> **Note:** Jurisdiction refers to the authority of a court to hear, decide and rule on cases within a particular geographical limit. In other words, it is the territory over which the court can exercise its authority.

4. Improving Legal Research

Lawyers are intimately familiar with legal research and are accustomed to digging through reams of case law to identify the nuggets of wisdom they need. Luckily, legal research has been revolutionized in the past few decades so that lawyers no longer need to spend hours flipping through dense books in the law library. Instead, relevant legal precedents from around the country, and even around the world,

are available with a few keystrokes and clicks on a keypad through popular legal research websites like SCC and Manupatra.

Analytics tools for legal research save lawyers time and effort—and helps them win cases—by rapidly identifying relevant and significant cases that can inform their arguments and strategy. Searches can be narrowed by practice area, date, location, or even the number of times that a search term appears in the result. All of these capabilities arise from data analytics.

Therefore, in this manner, not only do legal research tools create an easy way to sort through legal cases, but they also provide access to treatises, pleadings, guidelines laid down by the court, and other helpful materials. In fact, many state bar associations provide free access to legal research tools so that all lawyers can benefit from this powerful technology.

5. Promoting Lawyer Productivity

Legal analytics don't just help clients; legal analytics software can also tell partners and heads of law firm which lawyers are the most productive, efficient, and cost-effective and which lawyers need to improve. This data is critical for making decisions about assignments and promotions and deciding how to manage attorneys and their workload.

For instance, with legal analytics tools that track billable hours, you can see how long a lawyer spends working on a specific case and dedicate more expensive resources (partners and senior associates) for only the most important work. Law firms and corporate law offices can also explore hiring remote lawyers and see how the costs and benefits stack up against full-time employees.

Not only can managers get unparalleled access to data about associates, but legal analytics can also provide tools to help underperforming lawyers get back on track. Many products have attorney dashboards, automated document management, and client collaboration tools to boost productivity.

QUANTITATIVE LEGAL PREDICTION VIS-À-VIS BUSINESS OF LAW[6]

Overview of Quantitative Legal Prediction (QLP)

This current wave of legal artificial intelligence has abandoned the idea of algorithms mimicking the thought process of lawyers. Rather, the predictive justice algorithms turn to quantitative approaches, i.e., utilizing brute-force processing of data.[7] The development in this field is propelled by the increasing computing power, declining data storage costs, better access to data and improvements in machine learning and other artificial intelligence technologies.[8]

Specifically, quantitative legal prediction is based on supervised machine learning techniques which employ data of previous cases as input to predict the result of a future case.[9] This method applies statistical means to "induce a prediction model (or function) from a dataset that can be used to predict an outcome for a new case."[10]

---

6. Reproduced from Trasberg Henrik (2019) Quantitative Legal Prediction and the Rule of law, Master Thesis, Law and Technology LLM, TILBURG University Law School.

7. Greenleaf (n 17) 312; For a further description of utilizing big data for building legal prediction models see Richard Susskind and Daniel Susskind, The Future of the Professions: How Technology Will Transform the Work of Human Experts (Oxford University Press 2015) 226–228 and 276–278.

8. An overview of advances in computer hardware and artificial intelligence powering the development of quantified legal prediction is provided by Katz (n 5) 913–923.

9. It is regarded as "supervised" since it involves inferring a classification model from labeled training data. See Ashley (n 6) 109. Ashley further explains the functioning of supervised machine learning: "The training data comprise a set of examples that have been assigned outcomes. Each example is a pair consisting of an input object (often a vector of feature values) and a desired output value. The learning algorithm needs to generalize from the training data to unseen situations."

10. ibid.

Quantitative Legal Prediction thus creates an "inverse" model in which correlations are created between certain elements available in the case (such as specific words used) and the outcome of a case, as a result of which certain value is assigned to each element.

As described by Katz, "simply put, one uses the observables to build the model rather than using the model to assign causal weight to those observables."[11] In context of legal prediction, this means that certain parameters or features of a case (e.g. who is the judge, what is the subject-matter of the case, which words or phrases are present in the case documentation, etc.) are assigned a value that would indicate which way a case would be decided based on past patterns.[12] It is worth noting that the QLP tools will not discover the features that influence outcomes, but instead learn the weights of such features.[13]

Quantified legal prediction is what Daniel Katz categorizes as "soft artificial intelligence" in the sense that the algorithms aim to achieve outcome that would mimic human intelligence while the process to achieve the outcome does not.[14] There is thus no legal reasoning employed in the predictions of the quantified prediction models. Importantly, data-based prediction models require elements that are relatively simple to extract – there is no input needed from the larger body of legal system. There is also no knowledge representation bottleneck that arises with the legal expert systems as the model does not require semantic understanding or the context of the information extracted.

Applications of Quantitative Legal Prediction

QLP can serve many purposes, one of the more intriguing of which is predicting outcomes of court cases – seemingly with a better precision than legal experts. An example of such functionality is the algorithm developed by Katz et al. which enables prediction of US Supreme Court case outcomes with 70.2 % accuracy.[15] While such prediction models largely dismiss legal causality, Katz considers that "it is not always necessary to have a deep theory in order to generate a well-functioning prediction engine."[16] The algorithm by Katz et al. uses input information about the case (e.g., who are the parties, type of law, the source circuit court, the judgement at lower court, issue area), background information (e.g. name of judge(s), age and gender of judge, party of the appointing president) and trends (e.g., historic trends of Supreme Court, current trends of Supreme Court, trends of lower courts, trends specific to individual Supreme Court justice) in creating the outcome prediction.[17] In a study conducted by Blackman et al. in 2012, three distinguished legal experts were tasked with predicting outcomes of 171 SCOTUS cases, predicting correctly only 59 % of the cases.[18] While this sample is too small to make exhaustive conclusions, it does give promise to the idea that QLP can predict case outcomes, on average, with a better accuracy than expert lawyers and could thus emerge as a genuine mechanism for making litigation decisions.

Using meta-data from previous cases to draw conclusions about emerging legal matters is also employed by many commercialized predictive justice products (for example, Premonition, Blue J Legal, Courtquant and Predictice). In some domains of law this may be particularly effective: a prediction model developed by Dunn et al. was able to predict judge's ruling in asylum applications with 80 % accuracy while merely having information about the judge and the applicant's nationality.[19] Blue J Legal, which creates its predictions by combining data-

11. Katz (n 5) 952

12. See ibid 952–953.

13. Ashley (n 6) 125.

14. See Katz (n 5) 913 and 918.

15. Katz, Bommarito and Blackman (n 7).

16. Katz (n 5) 950.

17. Katz, Bommarito and Blackman (n 7) 7.

18. Blackman and Carpenter (n 8).

19. Dunn and others (n 25).

based prediction based on patterns from prior case laws with input provided by the user, is able to consistently predict correctly over 90 % of outcomes of tax law cases in Canada.[20]

Note: Meta-data refers to that data which provides information about one or more aspects of data.

The algorithm developed by Aletras et al., which predicts cases of European Court of Human Rights with a 79 % accuracy, has adopted a different direction – instead of assigning value to certain meta-data, it creates correlations between sequences of words (n-grams)[21] available in certain parts of a case (e.g., the legal circumstances and facts) and case outcome. For example, the term 'second applicant' has a significant correlation with ECtHR identifying an infringement. Another similar model was able to predict ECtHR i.e. European Court of Human Rights, case outcomes with 75 % accuracy.[22] Potentially, such algorithm could be provided with the pleadings/ complaint concerning the case and/or other case documentation as input and, based on the language used in the input, it predicts (the likelihood of) positive/negative outcome.

There are many other models developed to predict, for example, security fraud class actions and settlement amounts,[23] likelihood of patent being litigated,[24] and appeal decisions in tax law in Germany.[25] The knowledge that these tools provide can enable valuable input for significant litigation decisions, for example whether to litigate or not and whether to seek compromise or discard specific claims. One could envision that if the prediction accuracy of these models continues to significantly rise, they may be adopted by courts and other public institutions for making administrative decisions and solving legal disputes.

In addition to case outcome prediction, QLP also provides other benefits. To bring a few examples, QLP-based algorithms can mine and aggregate information from past case precedents that enables, for example, to predict how long the case might take, what are the likely legal costs, what is the best way to remedy a particular legal dispute, etc.[26] But most significantly, predictive justice tools can identify certain patterns about how the courts and the judges operate, such as which prior case laws a particular judge likes to refer to, how the judge tends to decide in non-obvious cases in respect of a particular subject-matter, whether there are certain lawyers that tend to win with a particular judge, what are the types of arguments that the judge tends to embrace, etc. These patterns, which are largely based on the data about how the judge has ruled in the past, render the adjudication process more transparent as they provide insight into what a particular judge might find relevant in respect of a certain legal debate. This enables legal counsels to make better strategic decisions and tailor the legal arguments within the adjudication process for the particular judge. In light of the notion that the judge's decision is influenced by its attitudes, biases and other cognitive processes, the input into tendencies of a judge can have transformational impact on the transparency of adjudication and the predictability of a judge's actions.

As another use-case, there are some QLP-based software being adopted by the stake-holders before the case even proceeds for trial, i.e. at the pre-trial stage. For example, a few US courts are using data-based tools to assess the risk of recidivism of convicted criminals – a major factor in contemplating the choice and extent of

20. Benjamin Alarie, Anthony Niblett and Albert Yoon, 'Using Machine Learning to Predict Outcomes in Tax Law' (2017) SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2855977>

21. N-grams are contiguous word sequences within the text. See Aletras and others (n 9) 8–9.

22. Masha Medvedeva, Michel Vols and Martijn Wieling, 'Judicial Decisions of the European Court of Human Rights: Looking into the Crystall Ball' (2018) University of Groningen, Department of Legal Methods 1 <http://martijnwieling.nl/files/Medvedeva-submitted.pdf>.

23. Blakeley B Mcshane and others, 'Predicting Securities Fraud Settlements and Amounts: A Hierarchical Bayesian Model of Federal Securities Class Action Lawsuits' (2012) 9 Journal of Empirical Legal Studies 482.

24. Colleen V Chien, 'Predicting Patent Litigation' (2011) 90 Texas Law Review 283.

25. Bernhard Waltl and others, 'Predicting the Outcome of Appeal Decisions in Germany's Tax Law' (2017) 10429 (eds) Electronic Participation. ePart 89 <http://link.springer.com/10.1007/978-3-319-64322-9_8>.

26. Katz (n 5); Hildebrandt, 'Law as Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics' (n 12) 11.

punishment.[27] In law enforcement, predictive justice tools are used for assessing whether a suspect should be held in pre-trial detention or not.[28]

Note: Recidivism refers to the tendency of a convicted criminal to relapse into criminal behavior.

What QLP thus promises is an augmented insight into what might be the outcome of a particular case, enabling the counsel to make smarter whether to commence litigation or not. This value should not be understated – lawyers are surprisingly bad at predicting outcomes of court cases that exceed certain basic level of difficulty.[29]

Furthermore, while a lawyer's ability to reason far exceeds any algorithm, humans' capacity to sift through thousands of court cases and identify correlations from historic patterns that may play a significant role in the outcome of a current case or provide insight into behavior of the judge is dwarfed compared to the ability of AI. QLP thus enables lawyers to overcome some of the cognitive limitations of the human brain.

Limitations of Quantitative Legal Prediction

Despite its potential, QLP simultaneously contains some significant limitations which hinders its adoption within the adjudication process.

- Firstly, the usefulness of a prediction algorithm depends on identifying variables that reliably correlate with case outcome while also being readily available prior to or in an early stage of the adjudication. For example, the model developed by Aletras et al. was trained by seeking correlations between case outcome and the procedure, facts, law and circumstances of the case that were written in the actual judgment. It is evident that the choices made in drafting the document on facts and circumstances of the case will be significantly influenced by the outcome that is established in the same judgment. Thus, it is unknown (not to say: extremely unlikely) that the model of Aletras et al. would have any reliability when it is ordered to predict outcome based on the input that is extracted from the case pleadings/document or any other documentation available before the judgment.
- Secondly, many of the correlations between input data and output that the QLP algorithms identify may be misleading. As framed by Cashwell and Pasquale, "Any student of statistics knows, if one tests enough data sets against one another, spurious correlations will emerge."[30] There is thus a considerable likelihood that the correlations between majority of the n-grams or other factors taken into account by the QLP algorithms, in reality, do not provide any useful knowledge about the outcome but are, in fact, spurious.
- In addition to the (current) technical limitations which restrict the usefulness of the QLP algorithms, their approach to solving legal disputes fundamentally clashes with the notion of law and the rule of law, causing a great number of legal challenges. The issue emerges from the fact that the output of QLP is based on the seemingly random correlations that the algorithm has identified, rather than "inferences from any causal model."[31]As such, the insights it provides ignore the substantial merits of the case. In fact, the current quantitative legal prediction models give no regard to semantic understanding of legal

27. For example, Compas software by Equivant is used by several courts in US. See Adam Liptak, 'Sent to Prison by a Software Program's Secret Algorithm', The New York Times, 01.05.2017. <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secretalgorithms.html>. However, it must be noted that using the Compas software has been met with significant scepticism – see for example Jason Tashea, 'Courts Are Using AI to Sentence Criminals. That Must Stop Now', Wired Magazine, 17.04.2017 <https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stopnow/>. See also Ed Yong, 'A Popular Algorithm Is No Better at Predicting Crimes Than Random People', The Atlantic, 17.01.2018. <https://www.theatlantic.com/technology/archive/2018/01/equivant-compasalgorithm/550646/>

28. Nick Statt, 'UK police will start using AI to decide whether suspects should be kept in custody', The Verge, 10.05.2017. <https://www.theverge.com/2017/5/10/15614980/uk-durham-police-ai-risk-assessment-policing>

29. See analysis of the study by Jane Goodman-Delahunty, Maria Hartwig, and Elizabeth F Loftus in Section 3.3.

30. Pasquale and Cashwell (n 19) 9.

31. See Greenleaf (n 15) 312.

arguments or legal deduction. Consequently, these algorithms are not able to provide an explanation, not to mention legal reasoning, for the conclusions reached. On this note, Susskind argues that in many areas "we can develop high performing, non-thinking machines that can outperform the best human experts, even though they go about their business in quite unhuman ways" and thus "we will not need to understand and then replicate the way human experts work, nor will we need to develop thinking machines to replace much of the work currently undertaken by human professionals."[32] Yet, does our idea of law permit a situation where important (legal) decisions have no causative basis in law?

- Evidently, it raises some significant concerns. For example, as the output of QLP is not cast into form of legal argumentation and the reasoning (logic) based on which the algorithms reach conclusions remains opaque and unintelligible, the decision or a suggestion of a QLP-based algorithm effectively cannot be contested.
- Furthermore, these models are never unbiased, objective nor neutral in their prediction; but are affected by a series of design decisions by its developers."[33] Notably, developing the model requires a trade-off, between volume, relevance, completeness, accuracy and correctness of the training dataset, the dimensionality and aptitude of the hypotheses space, the time taken for iterant testing, and the availability of the relevant domain expertise."[34] Since these choices will significantly influence the conclusions reached by the model, it essentially means that the developers of the algorithms will have the power to direct the output of a model and thereby influence legal decision-making.

The above-described limitations hint towards some of the rule of law implications that arise with the emergence of data-based legal decision-making.

Using QLP to Predict Court Case Outcomes

Adoption of QLP algorithms to predict case outcome essentially provides individuals a risk management tool when deciding whether to adjudicate or not. This risk management tool can predict a case outcome, on average, with a better accuracy than a lawyer, promising a new era in how litigation decisions are made. Yet, I claim that widespread adoption of QLP for predicting case outcome and using these predictions for making litigation decisions undermines the value of adjudication and thereby the realization of rule of law, as it dismisses the role of adversarial legal argumentation.

Note: Adjudication refers to the legal process by which a judge gives a decision which determines the rights an liabilities of the parties involved in a case.

The legal disputes for which insight from QLP is sought are presumably cases where no axiomatic solutions exist. Questions of law in such cases cannot be solved purely by having knowledge of the legal system or the existing case law, which is why relying on a data-based prediction tool that has a good track record seems tempting. Yet, such approach misrepresents the adjudication process: It is argued that it is the adversarial legal argumentation that takes place within the adjudication process, which forges the result of non-obvious cases. Therefore, the outcome of a dispute (i.e., how legal rule applies in the particular situation) is created within the adjudication process. Consequently, what a lawyer does in the adjudication process is not just a prediction – the legal arguments it creates and submits are proposals for regulation of behavior which, if convincing to the court, are materialized into a legal norm. It is only through this adversarial argumentation that the resolution on how the disputed behavior is to be regulated comes into existence. As such, QLP misrepresents adjudication by purporting predetermination where there is none.

32. Susskind and Susskind (n 35) 276; See also Greenleaf (n 17) 312.

33. Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) <http://dx.doi.org/10.1098/rsta.2017.0355>.

34. Hildebrandt, 'Law as Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics' (n 12) 10.

The principal issue with the above emerges from the fact that the adjudication process carries a fundamental role in safeguarding the realization of rule of law. The principle of rule of law postulates that no one is above the law and law applies equally to all citizens irrespective of their ranks, other distinctions, etc. The rule of law is evidently an elusive concept with a wide array of objectives, but one of its key aspects is treating individuals as moral agents entitled to dignity and respect. The adjudication process ensures such treatment by accepting that law has an arguable character and by providing a procedure where a question of how a certain behavior should be governed is argued. Thus, the adjudication process is not only a place for reaching a conclusion, but functions as a forum where the understanding of the law is debated and formed, and the individual is entitled to participate and influence that procedure. The preemptive character of QLP impedes the adjudication process in acting as such an institution.

Using QLP for Profiling Judges and its Rule of Law Implications

The second significant rule of law interference relates to applying QLP technology for identifying and exploiting specific patterns of judges, with the purpose of exploiting these tendencies for one's advantage. The commercialized products that have adopted QLP technology increasingly promise the possibility to outline certain patterns of a judge to better understand what are the arguments, cases, types of evidence, etc., that a particular judge likes, enabling a more insightful prediction on what might be the most fruitful strategy or a set of argumentations for a particular case. The value proposal of such use of QLP is thus a more transparent and predictable adjudication through identification of adjudication patterns otherwise inaccessible to human cognition.

Simultaneously, the adjudication process is riddled with biases and inconsistencies. The more significant the patterns these predictive justice tools are able to identify, the more it enables to exploit the disparities that exist within the judiciary. If patterns of judges become increasingly visible, the extent to which the biases are exploited will inevitably increase, tilting case outcomes by engaging factors that are not rooted in law or the legal system at large. This apparent lack of concern for substantive justice would undermine fair adjudication as well as erode public confidence in the adjudication system.

Joseph Raz states that insufficient regard for the rule of law can lead to uncertainty or it may lead to frustrated and disappointed expectations.[35] Adoption of QLP-based algorithms for identifying patterns of adjudication affects both of these aspects – on one hand it enhances transparency and foreseeability; on the other, it enables unfair exploitation of the system, eroding public confidence and giving rise to frustration about the adjudication process by the courts.

Reconciliation comes in the form of adequate reaction to the developments enabled by QLP – in order to mitigate the risks on fairness of adjudication and the perception thereof. The emergence of QLP requires attention and willingness from the judiciary to evolve adjudication in line with the capabilities of the QLP technology. This includes the need to further understand, embrace and develop a theoretical framework about the role of biases within adjudication and provide judicial education on understanding significance of the adjudication data extracted by QLP.

BIAS/ VARIANCE, PRECISION/RECALL & DIMENSIONALITY

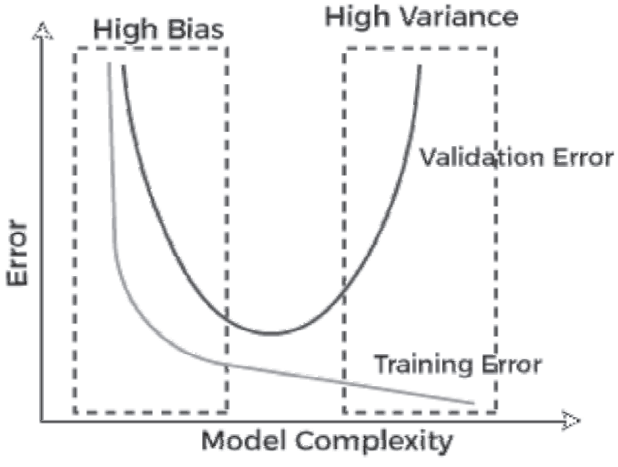
Bias and Variance in Machine Learning[36]

Machine learning is a branch of Artificial Intelligence, which allows machines to perform data analysis and make predictions. However, if the machine learning model is not accurate, it can make predictions errors, and these prediction errors are usually known as Bias and Variance. In machine learning, these

35. See Raz (n 22) 222.

36. Bias and Variance in Machine Learning, Java T Point. Available at https://www.javatpoint.com/bias-and-variance-in-machine-learning

errors will always be present as there is always a slight difference between the model predictions and actual predictions. The main aim of ML/data science analysts is to reduce these errors in order to get more accurate results. In this portion, we are going to discuss bias and variance, Bias-variance trade-off, Underfitting and Overfitting.

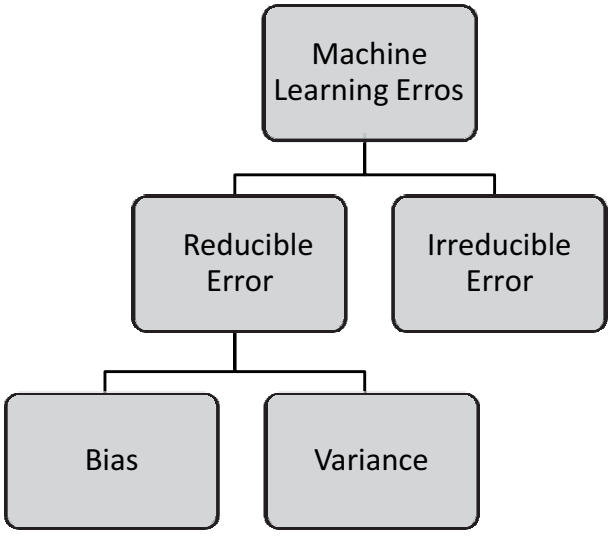


Source: https://www.javatpoint.com/bias-and-variance-in-machine-learning

Errors in Machine Learning

In machine learning, an error is a measure of how accurately an algorithm can make predictions for the previously unknown dataset. On the basis of these errors, the machine learning model is selected that can perform best on the particular dataset. There are mainly two types of errors in machine learning, which are:

- ***Reducible Errors:*** These errors can be reduced to improve the accuracy of the mode. Such errors can further be classified into bias and Variance.



Source: https://www.javatpoint.com/bias-and-variance-in-machine-learning

- ***Irreducible Errors:*** These errors will always be present in the model regardless of which algorithm has been used. The cause of these errors is unknown variables whose value cannot be reduced.

Let's understand the entire concept of bias, in detail.

What is Bias?

In general, a machine learning model analyses the data, find patterns in it and make predictions. While training, the model learns these patterns in the dataset and applies them to test data for prediction. While making predictions, a difference occurs between prediction values made by the model and actual values/expected values, and this difference is known as bias errors or Errors due to bias. It can be defined as an inability of machine learning algorithms such as Linear Regression to capture the true relationship between the data points. Each algorithm begins with some amount of bias because bias occurs from assumptions in the model, which makes the target function simple to learn. A model has either:

- **Low Bias:** A low bias model will make fewer assumptions about the form of the target function.
- **High Bias:** A model with a high bias makes more assumptions, and the model becomes unable to capture the important features of our dataset. A high bias model also cannot perform well on new data.

Generally, a linear algorithm has a high bias, as it makes them learn fast. The simpler the algorithm, the higher the bias it has likely to be introduced. Whereas a nonlinear algorithm often has low bias.

Some examples of machine learning algorithms with low bias are Decision Trees, k-Nearest Neighbors and Support Vector Machines. At the same time, an algorithm with high bias is *Linear Regression, Linear Discriminant Analysis and Logistic Regression*.

Ways to reduce High Bias:

High bias mainly occurs due to a much simple model. Below are some ways to reduce the high bias:

- Increase the input features as the model is underfitted.
- Decrease the regularization term.
- Use more complex models, such as including some polynomial features.

What is a Variance Error?

The variance would specify the amount of variation in the prediction if the different training data was used. In simple words, *variance tells that how much a random variable is different from its expected value*. Ideally, a model should not vary too much from one training dataset to another, which means the algorithm should be good in understanding the hidden mapping between inputs and output variables. Variance errors are either of *low variance or high variance.*

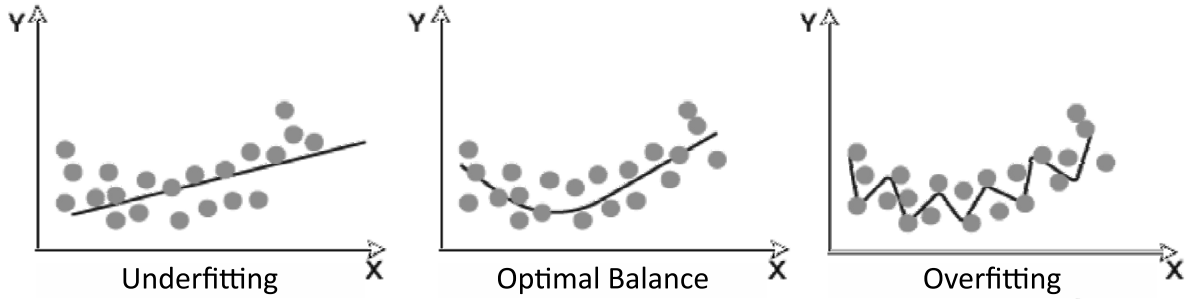
Low variance means there is a small variation in the prediction of the target function with changes in the training data set. At the same time, High variance shows a large variation in the prediction of the target function with changes in the training dataset.

A model that shows high variance learns a lot and performs well with the training dataset, and does not generalize well with the unseen dataset. As a result, such a model gives good results with the training dataset but shows high error rates on the test dataset.

Since, with high variance, the model learns too much from the dataset, it leads to overfitting of the model. A model with high variance has the below mentioned problems:

- A high variance model leads to overfitting.
- Increased model complexities.

Usually, nonlinear algorithms have a lot of flexibility to fit the model, have high variance.



Source: https://www.javatpoint.com/bias-and-variance-in-machine-learning

Some examples of machine learning algorithms with low variance are, Linear Regression, Logistic Regression, and Linear discriminant analysis. At the same time, algorithms with high variance are decision tree, Support Vector Machine, and K-nearest neighbours.

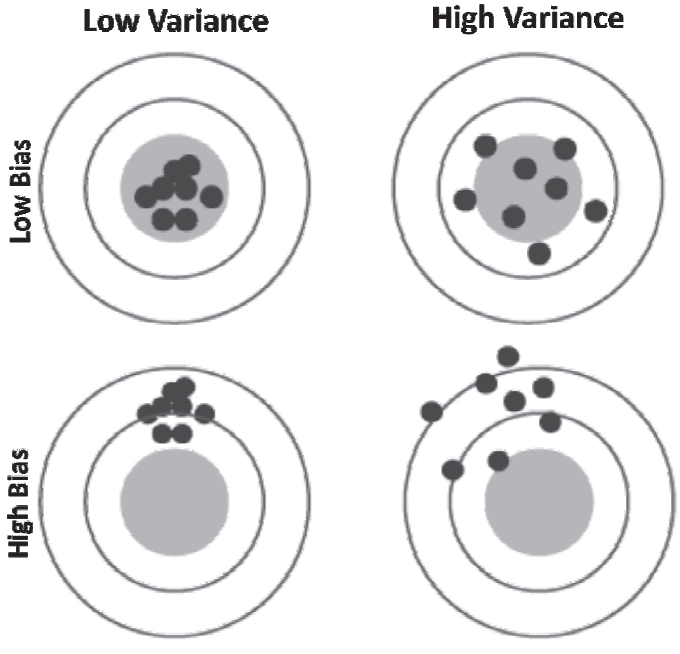
Ways to Reduce High Variance:

Reduce the input features or number of parameters as a model is overfitted.

- Do not use a much complex model.
- Increase the training data.
- Increase the Regularization term.

Different Combinations of Bias-Variance

There are four possible combinations of bias and variances, which are represented by the diagram below:



Source: https://www.javatpoint.com/bias-and-variance-in-machine-learning

1. **Low-Bias, Low-Variance:**

   The combination of low bias and low variance shows an ideal machine learning model. However, it is not possible practically.

2. **Low-Bias, High-Variance:**

   With low bias and high variance, model predictions are inconsistent and accurate on average. This case occurs when the model learns with a large number of parameters and hence leads to an overfitting

3. **High-Bias, Low-Variance:**

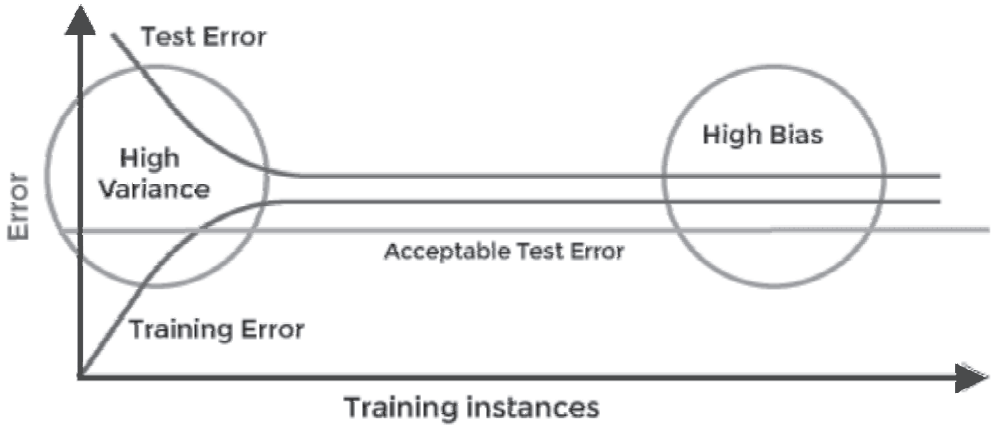
   With high bias and low variance, predictions are consistent but inaccurate on average. This case occurs when a model does not learn well with the training dataset or uses few numbers of the parameter. It leads to underfitting problems in the model.

4. **High-Bias, High-Variance:**

   With high bias and high variance, predictions are inconsistent and also inaccurate on average.

How to identify High variance or High Bias?

High variance can be identified if the model has:



Source: https://www.javatpoint.com/bias-and-variance-in-machine-learning

- Low training error and high-test error.

High Bias can be identified if the model has:

- High training error and the test error is almost similar to training error.

Trade Offs and Bias

Trade-offs are the one thing that is between sane but boring life and complicated, risky but adventurous life. At every point in life, even every second, we make some kind of 'Trade-Off'. Risky or not, Trade-Offs always help us to find the sweet spot or middle ground. As we are turning the machine to think like humans, they too, are haunted by 'Trade-Offs'.

Machine Learning mostly have to deal with two Trade-offs:

- Bias-Variance Trade-offs
- Precision-Recall Trade-offs

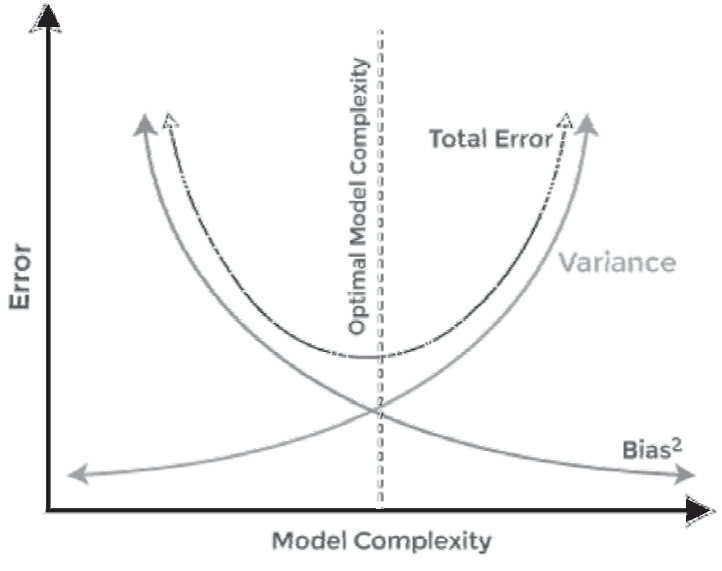
Bias-Variance Trade-Off

While building the machine learning model, it is really important to take care of bias and variance in order to avoid overfitting and underfitting in the model. If the model is very simple with fewer parameters, it may have low variance and high bias. Whereas, if the model has a large number of parameters, it will have high variance and low bias. So, it is required to make a balance between bias and variance errors, and this balance between the bias error and variance error is known as the Bias-Variance Trade-Off.

For an accurate prediction of the model, algorithms need a low variance and low bias. But this is not possible because bias and variance are related to each other:

- If we decrease the variance, it will increase the bias.
- If we decrease the bias, it will increase the variance.

Bias-Variance trade-off is a central issue in supervised learning. Ideally, we need a model that accurately captures the regularities in training data and simultaneously generalizes well with the unseen dataset. Unfortunately, doing this is not possible simultaneously. Because a high variance algorithm may perform well with training data, but it may lead to overfitting to noisy data. Whereas, high bias algorithm generates a much simple model that may not even capture important regularities in the data. So, we need to find a sweet spot between bias and variance to make an optimal model.



Source: https://www.javatpoint.com/bias-and-variance-in-machine-learning

Hence, ***the Bias-Variance trade-off is about finding the sweet spot to make a balance between bias and variance errors.***

Overfitting, Underfitting, & Cross-Validation[37]

Overfitting and Underfitting are the two main problems that occur in machine learning and degrade the performance of the machine learning models. It is pertinent to note that 'Machine Learning' is a type of Artificial Intelligence that enables systems and software applications to become more accurate at making prediction of outcomes, without being explicitly programmed to do so.

37. Reproduced from Overfitting and Underfitting in Machine Learning, Java T Point. Available at https://www.javatpoint.com/overfitting-and-underfitting-in-machine-learning

The main goal of each machine learning model is to generalize well. Here generalization defines the ability of an ML model to provide a suitable output by adapting the given set of unknown input. It means after providing training on the dataset, it can produce reliable and accurate output. Hence, the underfitting and overfitting are the two terms that need to be checked for the performance of the model and whether the model is generalizing well or not.

Before understanding the overfitting and underfitting, let's understand some basic term that will help to understand this topic well:

- **Signal:** It refers to the true underlying pattern of the data that helps the machine learning model to learn from the data.
- **Noise:** Noise is unnecessary and irrelevant data that reduces the performance of the model.
- **Bias:** Bias is a prediction error that is introduced in the model due to oversimplifying the machine learning algorithms. Or it is the difference between the predicted values and the actual values.
- **Variance:** If the machine learning model performs well with the training dataset, but does not perform well with the test dataset, then variance occurs.

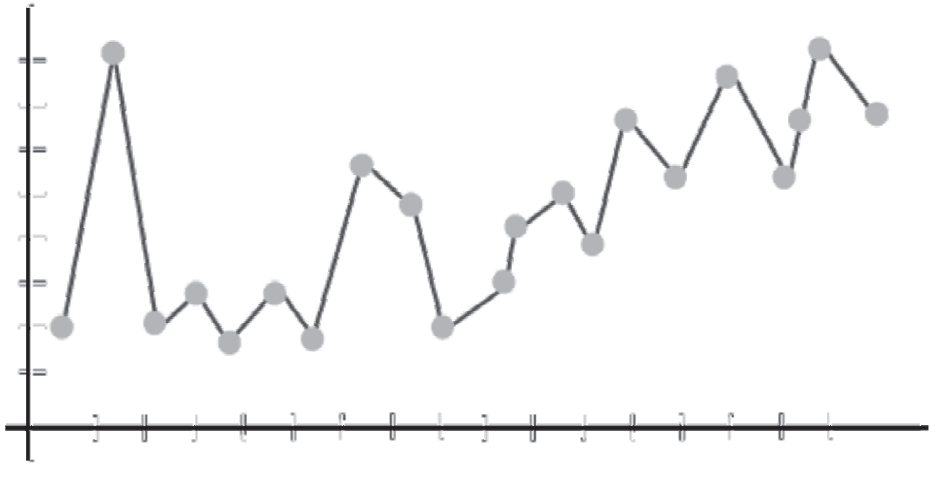
Overfitting

Overfitting occurs when our machine learning model tries to cover all the data points or more than the required data points present in the given dataset. Because of this, the model starts caching noise and inaccurate values present in the dataset, and all these factors reduce the efficiency and accuracy of the model. The overfitted model has **low bias** and **high variance.**

The chances of occurrence of overfitting increase as much we provide training to our model. It means the more we train our model, the more chances of occurring the overfitted model.

Overfitting is the main problem that occurs in supervised learning.

Example: The concept of the overfitting can be understood by the below graph of the linear regression output:



Source: https://www.javatpoint.com/overfitting-and-underfitting-in-machine-learning

As we can see from the above graph, the model tries to cover all the data points present in the scatter plot. It may look efficient, but in reality, it is not so. Because the goal of the regression model to find the best fit line, but here we have not got any best fit, so, it will generate the prediction errors.

How to avoid the Overfitting in Model

Both overfitting and underfitting cause the degraded performance of the machine learning model. But the main cause is overfitting, so there are some ways by which we can reduce the occurrence of overfitting in our model.

- Cross-Validation
- Training with more data
- Removing features
- Early stopping the training
- Regularization
- Ensembling

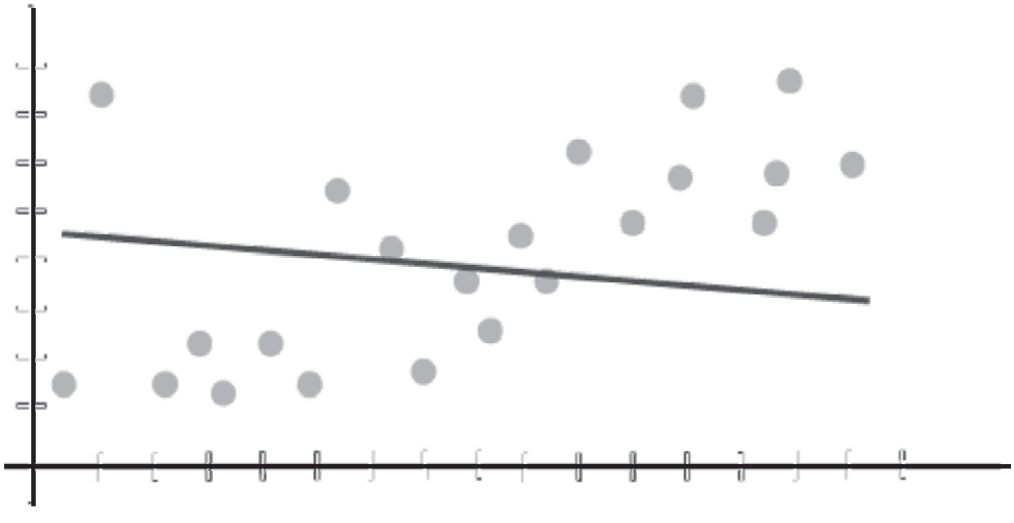
Underfitting

Underfitting occurs when our machine learning model is not able to capture the underlying trend of the data. To avoid the overfitting in the model, the feed of training data can be stopped at an early stage, due to which the model may not learn enough from the training data. As a result, it may fail to find the best fit of the dominant trend in the data.

In the case of underfitting, the model is not able to learn enough from the training data, and hence it reduces the accuracy and produces unreliable predictions.

An underfitted model has high bias and low variance.

Example: We can understand the underfitting using below output of the linear regression model:



As we can see from the above diagram, the model is unable to capture the data points present in the plot.

How to avoid underfitting:

- By increasing the training time of the model.
- By increasing the number of features.

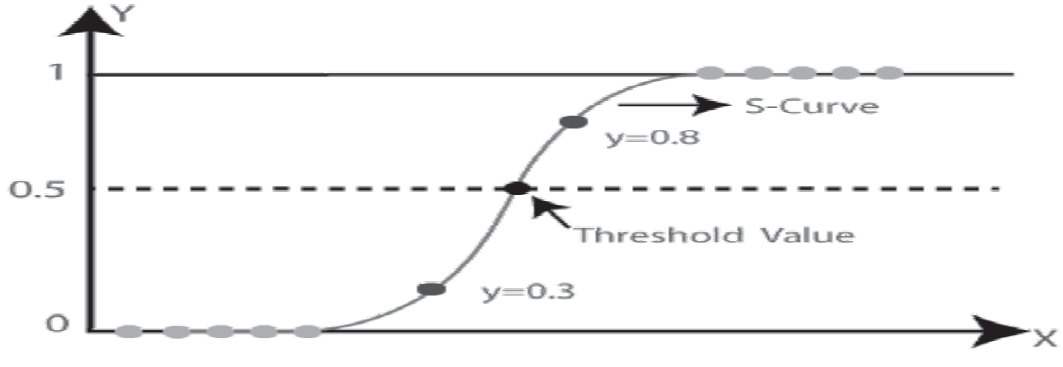
LOGISTIC REGRESSION AND MAXIMUM LIKELIHOOD

Logistic Regression in Machine Learning

- Logistic regression is one of the most popular Machine Learning algorithms, which comes under the Supervised Learning technique. It is used for predicting the categorical dependent variable using a given set of independent variables.

> **Note:** Logistic Regression is a supervised machine learning algorithm which is mainly used for classification tasks where the goal is to predict a probability that an instance is belonging to a particular class or not.

- Logistic regression predicts the output of a categorical dependent variable. Therefore, the outcome must be a categorical or discrete value. It can be either Yes or No, 0 or 1, true or False, etc. but instead of giving the exact value as 0 and 1, it gives the probabilistic values which lie between 0 and 1.
- Logistic Regression is much similar to the Linear Regression except that how they are used. Linear Regression is used for solving Regression problems, whereas Logistic regression is used for solving the classification problems.
- In Logistic regression, instead of fitting a regression line, we fit an "S" shaped logistic function, which predicts two maximum values (0 or 1).
- The curve from the logistic function indicates the likelihood of something such as whether the cells are cancerous or not, a mouse is obese or not based on its weight, etc.
- Logistic Regression is a significant machine learning algorithm because it has the ability to provide probabilities and classify new data using continuous and discrete datasets.
- Logistic Regression can be used to classify the observations using different types of data and can easily determine the most effective variables used for the classification. The below image is showing the logistic function:



Maximum Likelihood Estimation (MLE)[38]

Maximum Likelihood Estimation (MLE) is a technique used for estimating the parameters of a given distribution, using some observed data. MLE is a probabilistic based approach to determine values for the parameters of the model. MLE is a widely used technique in machine learning, time series, panel data and discrete data. Maximum Likelihood Estimation (MLE) is a probabilistic based approach to determine values for the parameters of the model. Parameters could be defined as blueprints for the model because based on that, the algorithm works. The motive of MLE is to maximize the likelihood of values for the parameter to get the desired outcomes.

38. Mehta Sourabh (2022) How is Maximum Likelihood Estimation used in Machine Learning, The Analytics India MAG.

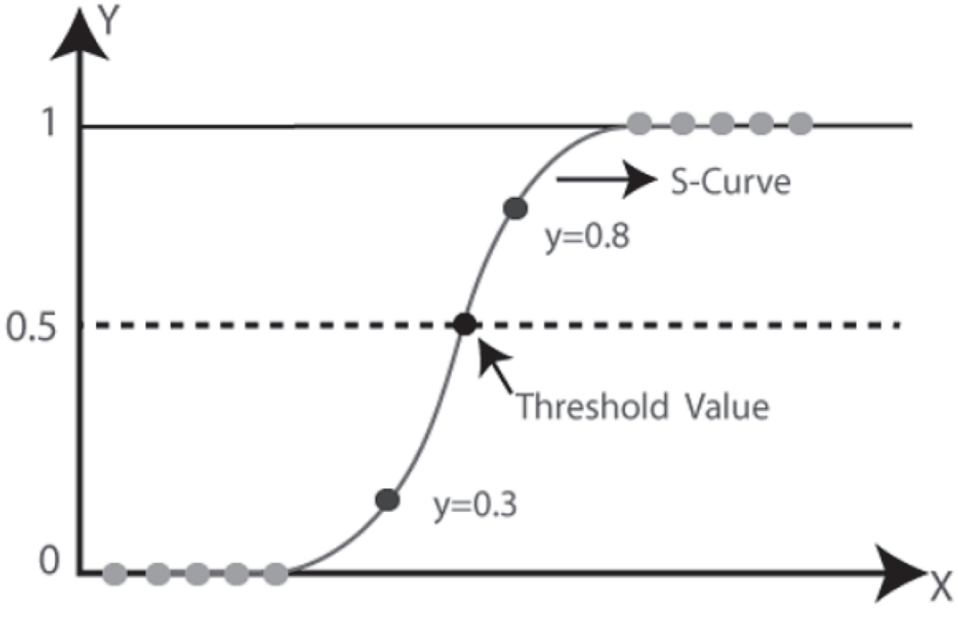
What is the likelihood?

The likelihood function measures the extent to which the data provides support for different values of the parameter. It indicates how likely it is that a particular population will produce a sample. For example, if we compare the likelihood function at two-parameter points and find that for the first parameter the likelihood is greater than the other it could be interpreted as the first parameter being a more plausible value for the learner than the second parameter. More likely it could be said that it uses a hypothesis for concluding the result. Both frequentist and Bayesian analyses consider the likelihood function. The likelihood function is different from the probability density function.

Working of Maximum Likelihood Estimation

The maximization of the likelihood estimation is the main objective of the MLE. Let's understand this with an example. Consider there is a binary classification problem in which we need to classify the data into two categories either 0 or 1 based on a feature called "salary".

So MLE will calculate the possibility for each data point in salary and then by using that possibility, it will calculate the likelihood of those data points to classify them as either 0 or 1. It will repeat this process of likelihood until the learner line is best fitted. This process is known as the maximization of likelihood.



Source: https://analyticsindiamag.com/how-is-maximum-likelihood-estimation-used-in-machine-learning/

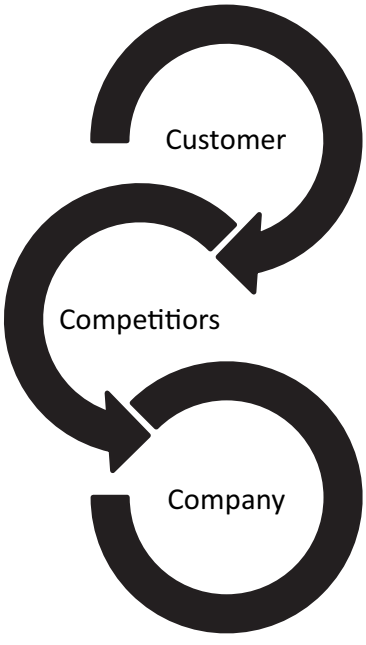
The above explains the scenario, as we can see there is a threshold of 0.5 so if the possibility comes out to be greater than that it is labelled as 1 otherwise 0.

TRIPLE C THEORY AND DATA ASSESSMENT

In a perfect world, data would always be complete, accurate, current, pertinent, and unambiguous. In the real world, data is generally flawed on some or all of these dimensions. Data assessment in practice has tended to focus on completeness and accuracy, and that is the focus of these notes. Currency, pertinence and clarity deserve more attention than they receive, perhaps, but their assessment requires very different methods.

Assessment is sometimes thought of as a preliminary to analysis proper. This is a useful distinction in some circumstances, but in general the assessment of error and the drawing of substantive conclusions are two

sides of the same coin. This is suggested by the symbolic equation "Data = Reality + Error", in which "Reality" represents conclusions drawn from the data that are valid despite the error and "Error" represents spurious conclusions suggested by the data as a result of error. Since all conclusions fall into one or the other of these two categories, conclusions about error are at the same time conclusions about reality, and conversely.



Direct Assessment

There are two general approaches to the assessment of data, direct and indirect. Direct assessment consists of evaluating the coverage and content of a data set. Coverage refers to the faithfulness of the correspondence between the records that constitute the data set and the statistical aggregate the data set represents. Data sets may omit records for some entities that should be represented and include records that should not be included. Improper inclusions occur when a data set includes more than one record for the same entity, includes records for entities not in the statistical aggregate, or includes fictitious records. Content refers to the completeness and accuracy of the information contained on the records in the data set.

Indirect Assessment

Direct assessment of data sets is expensive, both because a second data set is required for comparison and because matching is often a complex and difficult process. The results of direct assessment are, moreover, limited by response correlation bias and by the tendency of data sets collected at the same or nearly the same time to have similar content error. The indirect approach, by which data sets are assessed by analyzing the accuracy of statistics derived from them, is generally far less expensive and will often give results as good as or better than direct assessment.

Triple C Theory and Data Analysis

- **The First C – Customer Analysis**
    - Doing in-depth consumer research is the best way for you to figure out how to appeal to your target market. Being able to create catchy catchphrases and creative ads is going to be your bread and butter.

- Demographic data, that is, information on groups of people or population as per certain attributes like age, sex and place of residence, plays a huge part in this analysis. Figuring out your business's target market and their desires will drastically improve the success rate of your marketing strategies after they are put into circulation.

- **The Second C – Competitor Analysis**
  - Competitor analysis is mainly done by visiting their websites, subscribing to their newsletters, visiting their stores and/or receiving the service (heuristic analysis) they offer.

- **The Third C – Corporation Analysis**
  - The last step you'll want to take with this method requires you to analyze your own client's corporation. You'll want to know what marketing strategies have worked for them in the past and what ideas have failed. The best way for you to do this is, again, from the customer's viewpoint.

NETWORK ANALYSIS AND LAW[39]

While legal scholars have not adopted network analytic methods to the same extent as those in other fields of study, there have been a variety of legal network studies, and the trend appears to be increasing. This section will briefly review the legal scholarship applying network analyses before the following part explores more fully the future potential for legal network studies and the challenges faced by legal scholars working in the field.

Researchers have used network analytic techniques in a variety of contexts relevant to legal scholars. These include the analysis of legal social networks[40] examining statutes and regulatory codes as networks,[41] studying the networks of criminals and terrorists,[42] and studying the structure created by case law citations.[43] As case law citation network analyses are the most common and perhaps the most accessible of these, we will begin the review by looking at the history of this body of study.

Note: Case law citation refers to a referencing system used by legal professional to identify judicial decisions, either in series of books called Reporters, or on Legal research websites, or a neutral style which identifies the case regardless of where it is reported.

Examples of Network Analysis and Law

a. Judicial Citation Networks

One very fruitful application for the tools of network science is to study the 'evolution' of the common law through the prism of judicial citations. Indeed, a distinguishing feature of a common law system is the precedential weight that judicial actors attach to prior decisions. Judges presented with questions in a given case consider how to apply doctrines from prior cases. Taken in the aggregate, common law systems produce vast amounts of citation data and although there is a rich literature studying these citations, relatively little scholarship has applied the tools of network science.

b. Visualisation of Relations

Visualising connected nodes leverages humans' perceptual abilities to discover patterns from data

39. Whalen Ryan (2016) Legal Networks: The Promises and Challenges of Legal Network Analysis, 2016 Mich. ST. L. Rev. 539

40. See, e.g., John P. Heinz & Edward O. Laumann, Chicago Lawyers: The Social Structure of the Bar (1982).

41. See, e.g., Romain Boulet, Pierre Mazzega & Danièle Bourcier, A Network Approach to the French System of Legal Codes—Part I: Analysis of a Dense Network, 19 Artificial Intelligence & L. 333 (2011).

42. See, e.g., Jialun Qin et al., Analyzing Terrorist Networks: A Case Study of the Global Salafi Jihad Network, in 3495 Lecture Notes in Computer Science: Intelligence & Security Informatics 287 (Paul Kantor et al. eds., 2005).

43. See, e.g., Fowler & Jeon.

associated with nodes and edges. The network data in this article were acquired from external data sources. The network is represented by nodes and edges: the nodes are the relational data such as sources (cases on the one hand, and Roman law, customary law and case law on the other hand), while the edges represent the citations between these nodes. On all occasions, the cases records are the sources because only these records contain references.

Research Case of Network Analysis in Law[44]

Court proceedings and its records are interesting for the legal historian, specifically from a perspective of law and its development over the centuries. Such cases are commonly analyzed by intensive reading and note-taking and by identifying commonalities, differences and relationships between documents or elements of documents.

We use these cases to explore whether human analysis can be improved, or at least complemented, by applying network analysis. The latter is a computer science method that allows for the mapping, measuring and visualising of relationships between individuals, groups and other types of information.[45] In this form of analysis, nodes are connected through edges, with the nodes being individuals, groups or information, and the edges being used to link the nodes. By treating court decisions as nodes, and linking the allegations in those cases to legislation and to other cases or scholarly work, network analysis can create a citation network that signals how information flows or has flown, and the extent to which certain nodes in the network are authoritative.

Network analysis has been used for several purposes in the legal field:

- for analyzing criminal behaviour and terrorist networks;
- for finding authoritative cases at courts; and
- for examining legal social networks, networks of statutes and regulatory codes and patent citations.

Volkaert[46] argues that network analysis can be both conceivable and useful in legal history. His recent article provides an overview of research in digital legal history using network analysis and focusing on case citation networks and what he refers to as 'digital-dogmatic legal history'. According to Volkaert, network analysis can complement dogmatic and contextual legal history, although qualitative juridical interpretations for understanding law remain necessary. By applying network analysis to a selected number of cases of the Court of Friesland, we further explore its potential for legal history research purposes.

Recovery from a third party

For the purposes of the examination, three civil court records with similar cases were selected dealing with the same legal question. Two of these cases could be joined by close reading the court records, while the third was found in a footnote in one of the other case studies. The facts in these three cases were broadly similar in that all three involved an object being sold at an auction. In the first two cases, the object was a black mare, whereas in the third case it was a red spotted cow. All three objects sold were encumbered with a mortgage and all three buyers failed to pay the purchase price, even after being reminded. The auctioneer who had sold the object subsequently had to recover it from a third party. In all three cases, the latter refused to surrender the object, claiming that it had been sold to him in a legally valid way and that he was therefore an (unassailable) possessor in good faith. Each time, the corresponding legal question was whether the security right (i.e. the

44. Reproduced from Hylkje De Jong and Gijs Van Dijck (2022) Network analysis in legal history: an example from the Court of Friesland, The Brill. Available at https://brill.com/view/journals/lega/90/1-2/article-p250_9.xml?language=en

45. J.H. Fowler et al., Network analysis and the law: measuring the legal importance of precedents at the U.S. Supreme Court, Political Analysis, 15 (2007), p. 324-325. See also M.G.H. Schaper, A computational legal analysis of acte clair rules of EU law in the field of direct taxes, World Tax Journal, 6 (2014), p. 77 and 80, which provides references.

46. F. Volkaert, OK computer? The digital turn in legal history: a methodological retrospective', Tijdschrift voor Rechtsgeschiedenis, 89 (2021), p. 1-46, especially p. 37 et seq

mortgage) was valid only if the object was still with the debtor. Or could it also be valid and invoked if the object had been sold to a third party? In other words: did the security right include a right of pursuit, and could the auctioneer recover the object from the possessor in good faith?

Although the facts in the three cases were largely the same, the conditions of the sales were not. In the first case, the auctioneer had added the auction condition clausula constituti (a clause from respective constitution) and two sureties, which the plaintiff initially failed to call upon. As a result, and as far as we can reconstruct, the claim was rejected by the court. In the second case (, the auction condition clausula constituti was not added, but a specific mortgage was taken out, and there was no surety. Here, it would appear, the security right included the right of pursuit. In the final judgment, the defendant was ordered to hand over the black mare or pay the purchase price to the plaintiff (the auctioneer). The conditions in the third case were the same as in the second case, with the exception of the mortgage. In this case, the mortgage was not a specific mortgage, but a general one, which implied the privilege of the right of eviction. The plaintiff should, therefore, have first sued the non-paying buyer, which he had neglected to do. The Court of thus rejected the claim.

Simple interrelationships

Both the second and third case contains references to one of the preceding cases. In his reply, the plaintiff in the second case, copied 26 articles – the claim, the reply etc. were enumerated – verbatim from the first case. Indeed, he explicitly mentioned this first case at the end of his reply. In the third case, the plaintiff, copied 11 articles verbatim from the second case. These articles also happened to correspond with articles in the first case, although the judgement mentioned only the second case. The three lawyers would appear to have considered their cases to be similar and may have thought they could benefit from the earlier case(s). This interrelationship between the cases was found coincidentally, through close reading. New questions arise from this finding, including how did the lawyers acquire procedural documents from the other cases? Did they have access to them in some way? Was it common to refer verbatim to articles from other court cases? Interestingly, and even without going into the cases in depth, we can also identify another simple interrelationship: the auctioneers from the first two cases and the red spotted cow from the third case all came from a different locational background. Did the lawyers then work together? Did they exchange procedural documents? Linking more cases of a similar nature could provide new answers to questions about legal practice in the early modern period.

Problematic in the study of court records is that it takes a long time to identify allegations in the text and to find relationships between them. One has to be both conscientious and fortunate to recognize interrelationship between litigations. Moreover, based on the sample used for the present study it is hard to draw conclusions. And although the interrelationships mentioned in the three cases studies here were easy to recognize, recognition will be more difficult where the numbers of entities are higher.

Relations between references: Roman law, customary law and case law

Since the facts and the legal questions in the three cases under consideration are similar, it would not be surprising if the references to the sources also prove to be similar. And, indeed, this turned out to be true. The three cases contain a total of 55 references; of these, 30 were unique references, not including the two references to the other two cases studied here. There is thus an overlap: more than once, the lawyers used the same reference. It is difficult to identify patterns of references through close reading. Instead, therefore, we labelled the nodes (i.e. information entities) and analysed the relationships between them by using network analysis. Before applying this analysis, however, we first had to categorise the various sources to which the allegations referred, given that conclusions can only be drawn on well-defined entities.

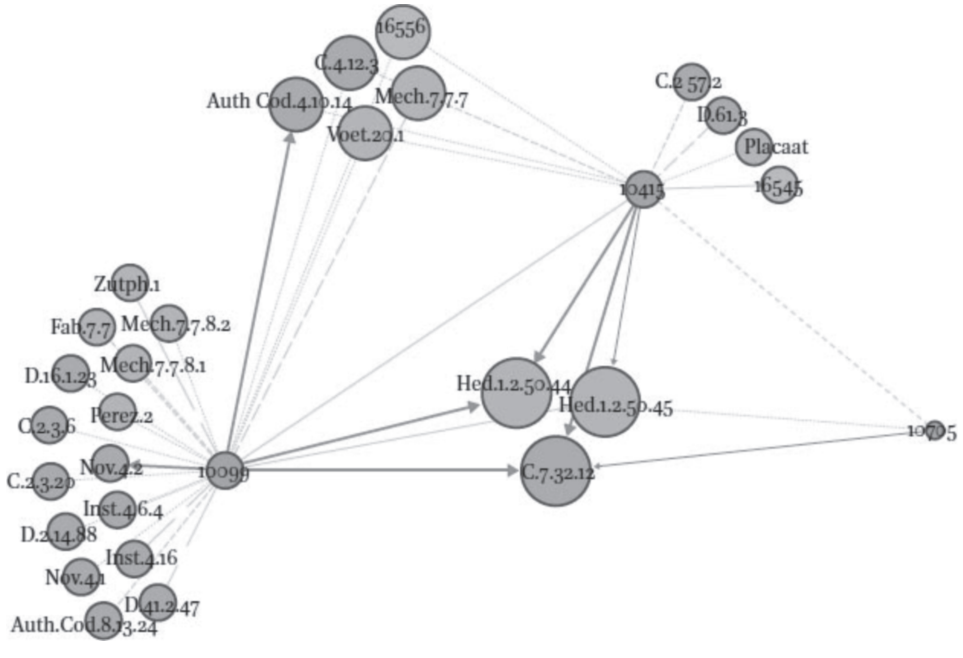
For this case study, we distinguished three categories of references, defined more or less by content, Roman law (15 times)25, customary law (10 times) and case law (5 times). The three cases are separated from these categories. We are aware that this categorisation is not exhaustive and can be more accurately expanded in future studies, focusing more on the defining of the information entities. Some shortcomings arising from the use

of inadequate definitions are that the legal commentaries and works on Roman-Frisian law were classified – for the sake of convenience – under customary law. We also did not take the classification of the use of allegations into consideration, for example, are they copied or are they used by analogy? In addition, no distinction was made between data pertaining to the plaintiff and data pertaining to the defendant. The extent to which references were used at different stages in the legal proceedings was also neglected. However, the three categories chosen were considered sufficient for the purposes of this article, which sets out only to demonstrate the benefit of network analysis for this dataset.

Visualisation of relations

Visualising connected nodes leverages humans' perceptual abilities to discover patterns from data associated with nodes and edges. The network data in this article were acquired from external data sources. The network is represented by nodes and edges: the nodes are the relational data such as sources (cases on the one hand, and Roman law, customary law and case law on the other hand), while the edges represent the citations between these nodes. On all occasions, the cases records are the sources because only these records contain references.

The visualisation of the references in the three cases is presented in figure 1. The layout of the network is based on the Force Atlas 2 algorithm28, with the three cases illustrated in orange as set out below. As mentioned above, the first case has inventory number 10099 (1716), the second 10415 (1718) and the third 10705 (1720). The figure should be read chronologically, from left to right, with references to Roman law being shown in purple, references to customary law in green and those to case law in blue. The node size depends on the incoming references: the more incoming references, the larger the node size (or, in network analysis terms, the larger the in-degree value). The same applies in respect of the thickness of the arrows: the thicker the arrow, the more often the lawyer referred to the particular source.



Source: https://brill.com/view/journals/lega/90/1-2/article-p250_9.xml?language=en

What can we generally deduce – despite the limited categories – from the network? The three nodes in the middle are the largest and therefore have the highest number of incoming references. All three cases refer to these fragments. The high (in-degree) centrality of these nodes suggests that these fragments are authoritative in this kind of legal issue. The first case in time (10099) contains the most references, while the second case

contains substantially fewer references. This second case refers to the first case, as the third case does to the second one. In its references, the third case is limited to the most important references, while the first two cases have some references in common, as shown at the top left. Both these cases refer to other case law in blue (16556). This case is from 20 December 1687. The second case also refers to other case law, specifically the judgment issued on 1 February 1676 (shown as 16545).

References to Roman law account for 50.0% of the references, those to customary law for 33.3% and those to case law for 6.7%, with the remainder comprising references to either or both of the other two cases. It is not surprising that most of the references are to Roman law, given that the Frisians chose Roman law to be applicable. If customary law could be further specified within the category, for example, of Roman-Frisian law, the reception of Roman law could be calculated more precisely. The more accurate the definitions of information entities are, the more specific the information generated will be. However, qualitative juridical research will continue to be necessary.

Future of network analysis in legal history

For what other legal questions may network analysis be useful? As well as identifying meaningful relations between entities within a dataset, it could be helpful for combining similar sets of entities. If other court archives in the other countries were to be unlocked, relations between these courts could also be revealed.

Today, entire archives of centuries-old material are available digitally and have been made searchable. Although such initiatives have commonly been undertaken in (digital) history departments, initiatives in the legal domain are under development. Fortunately, important initiatives are taken to change this situation. In, for instance, a pilot study, focusing on legal history, at the Department of Legal Theory and Legal History at VU Amsterdam, 48 metres of archives from the Court of Friesland (1499-1811) are being made accessible. The resultant data will be from 2273 civil cases from the period 1716-1730 (all documents in manuscript). This will be the first time that such a large amount of historical material from legal practice will be available.

A challenge resulting from the increased availability of data is that identifying relationships between documents or parts of documents become unmanageable if only human analysis is applied. Computational methods can assist in analysing historical data by, for instance, automatically recognising references in the text. This can then result in more data becoming available metadata; that is, data about the data (e.g. citations). The availability of more digitalised documents in the field of legal history will also allow leveraging of computational methods and techniques for analysing the documents, with network analysis then being used, for instance, to explore relationships between large numbers of cases and between references to and from those cases. However, this type of research requires new (digital) skills and implies a transformation, at least in part, of academic research in the sense that the very nature and scope of historical research will change.

Concluding Remark

This article discusses three similar cases, in which the legal question at stake was whether security rights (i.e. mortgages) included a right of pursuit. Could the auctioneer recover the object if the buyer failed to pay? The answer to this question depended on the contractual conditions. The lawyers in the three cases from the Court of Friesland appear to have used some of the same references. Network analysis of these references was used to visualize the relationships between these three cases, with the most important references also being made visible. A network can also be customized to suit specific purposes: the more entities (big data) that are defined, the more information that can be generated.

By comparing legal practice in civil court records in various provinces, or even internationally, network analysis will also make it possible to explore the mode of operation in these courts. This type of research in legal history will then generate new information that will add knowledge to historical legal practice, as well as uncovering information about daily life in early modern history and possibly also leading to a new understanding of the identities of the various provinces.

LESSON ROUND-UP

- In the modern times, industry whether legal or technology, academy, practitioners and scholars utilize artificial intelligence (AI) and machine learning to perform analyses which used to be labor-intensive endeavors a decade back.
- Data analytics is the science of analyzing raw data to make conclusions about the information.
- Many of the techniques and processes of data analytics have been automated into mechanical processes and algorithms that work over raw data for human consumption.
- Data analytics is the process that refers to deriving valuable insights and information from data using quantitative and qualitative methods.
- Legal analytics, with the help of data processing technologies, helps lawyers clean up, collate, and structurally analyze data.
- Data in the law industry can be broadly classified into individual data, law firm data, and industry data.
- Individual data is the data that one has in one's personal repository.
- Legal analytics is tool of facilitation and improving efficiency of legal results rather than a replacement or a solution for all legal case and client needs.
- Practice of law analytics gives in-house counsel insight that supports the legal practice, including data on legal contracts and cases.
- Artificial Intelligence (AI) is beginning to transform the legal profession in many ways and aims to take on higher-level tasks such as advising to clients, negotiating deals and drafting of standard contracts and agreements.
- Adoption of QLP algorithms to predict case outcome essentially provides individuals a risk management tool when deciding whether to adjudicate or not. This risk management tool can predict a case outcome, on average, with a better accuracy than a lawyer, promising a new era in how litigation decisions are made.
- Machine learning is a branch of Artificial Intelligence, which allows machines to perform data analysis and make predictions.
- Maximum Likelihood Estimation (MLE) is a probabilistic based approach to determine values for the parameters of the model.
- The likelihood function measures the extent to which the data provide support for different values of the parameter.
- While legal scholars have not adopted network analytic methods to the same extent as those in other fields of study, there have been a variety of legal network studies, and the trend appears to be increasing.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. Write a short note on Data Analytics.
2. What is Artificial Intelligence (AI) and Machine Learning (ML)? Discuss the role of AI and ML in Law and Legal Industry.

3. Write Short Note on any two of the following:
    a. Bias/Variance
    b. Overfitting and Underfitting
    c. Legal Analysis.
4. Discuss 3 Ways to use Legal Analytics. Substantiate the same with suitable examples.

LIST OF FURTHER READINGS

- Machine Learning for Lawyers, LWN. Available at https://lwn.net/Articles/721540/
- Novotna Tereza, Network Analysis in Law: A Literature Overview and Research Agenda
- James H. Flower et al (2007) Network Analysis and the Law: Measuring the Legal Importance of Precedents at the U.S. Supreme Court, Advance Access Publication, 2007. Available at https://home.gwu.edu/~wahlbeck/articles/Fowler-Johnson-Spriggs-Jeon-Wahlbeck%202007%20PA.pdf
- Park So-Hui et al (2021) A Survey of Research on Data Analytics-Based Legal Tech, MDPI, Volume 13, Issue 14
- Trasberg Henrik (2019) Quantitative Legal Prediction and the Rule of law, Master Thesis, Law and Technology LLM, TILBURG University Law School. Available at http://arno.uvt.nl/show.cgi?fid=149307

LIST OF OTHER REFERENCES

- An Introduction to Artificial Intelligence for Law Firms (2021) Lateral
- Artificial Intelligence for Lawyers Explained, Bloomberg Law
- Biswal Avijeet (2023) What is Data Analytics and its future scope in 2023, Simplilearn. Available at https://www.simplilearn.com/tutorials/data-analytics-tutorial/what-is-data-analytics#:~:text=Data%20analytics%20is%20the%20process,and%20efficiency%20of%20your%20business
- Columbia Law School on Data Analytics. Available on https://www.law.columbia.edu/areas-of-study/data-analytics
- Embroker (2022) What is the Legal Analytics and How you can use it to benefit your law firm. Available on https://www.embroker.com/blog/what-is-legal-analytics/
- Emily Stevens (2023) What is data Analytics? A Complete Guide for Beginners, CF Blog. Available at https://careerfoundry.com/en/blog/data-analytics/what-is-data-analytics/
- Jake Frankefield at el (2023) Data Analytics: What it is, How It's Used and 4 Basic Techniques, Investopedia. Available at https://www.investopedia.com/terms/d/data-analytics.asp
- James H. Fowler et al (2017) Network Analysis and the Law: Measuring the Legal Importance of Precedents at the U.S. Supreme Court, Cambridge University Press.
- Jong and Dijck (2022) Network Analysis in Legal History: An Example from the Court of Friesland, Brill. Available at https://brill.com/view/journals/lega/90/1-2/article-p250_9.xml

- Marios Koniaris et al (2018) Network analysis in the legal domain: a complex model for European Union legal sources. Get access Arrow, Journal of Complex Networks, Volume 6, Issue 2, April 2018, Pages 243–268.
- Network Analysis and Law: Introductory Tutorial, Computer Legal Studies, Jurix 2011
- Lauri Donahue (2018) A Primer on Using Artificial Intelligence in the Legal Profession, JOLT Digest, Harvard University. Available on https://jolt.law.harvard.edu/digest/a-primer-on-using-artificial-intelligence-in-the-legal-profession
- Legal Analytics: Definition and Advantage, Legal Practice, Lego Desk. Available at https://legodesk.com/legopedia/legal-analytics-definition-advantage/#:~:text=This%20data%20is%20collected%20from,similar%20scenarios%2C%20and%20so%20on.

  Lexis Insights (2023) What is Legal Analytics, Lexis Nexis. Available on https://www.lexisnexis.com/community/insights/legal/b/thought-leadership/posts/what-is-legal-analytics

PART II

TECHNOLOGICAL PERSPECTIVE

Computer Hardware and Software

Lesson 7

KEY CONCEPTS

■ Computer System ■ Primary Storage ■ Secondary Storage ■ Computer Peripherals – Inputs, Output, and Storage Devices ■ Computer Software ■ Software Trends ■ Multi-Programming ■ Multi-Processing ■ Time Sharing ■ Batch Processing ■ On-Line and Real-Time Processing ■ Application Software

Learning Objectives

To understand:

- The basic functions of hardware parts of the computer
- Identify the names and distinguishing features of different kinds of devices
- Identify the names, and distinguishing features, of memory and storage devices
- Identifies BIOS and System software
- Lists jobs of the operating system
- Features of different operating systems

Lesson Outline

- An Introduction – Computer System Concept, Types, Categories and Emerging Technologies
- Components of a Computer System
- Primary and Secondary Storage
- Computer Storage Capacities
- Computer Peripherals – Inputs, Output and Storage Devices
- Computer Software: An Introduction
- Software Trends
- Multi-Programming
- Multi-Processing
- Time Sharing
- Batch Processing
- On-Line and Real Time Processing
- Application Software
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

AN INTRODUCTION

A computer is an electronic device that receives information and data, automatically stores it and retrieves it at any time, and uses it in a useful manner. The computer converts different types of numbers and solves intractable mathematical equations very quickly and with high accuracy.

The computer was invented in the second half of the twentieth century and now it has become the backbone of life. Some operations before the invention of the computer were very difficult, including searches and doing some arithmetic activities. In 1642 AD, the calculator was invented to facilitate arithmetic operations such as addition, subtraction, and other arithmetic operations.

Presently, in the world of digital economies, computers play an important role. Further, computer is vital in people's day to day life. It will be apt to state that computer is indispensable, and its presence has become very important and necessary in our daily life, and it has become easier for us to do many operations and activities.

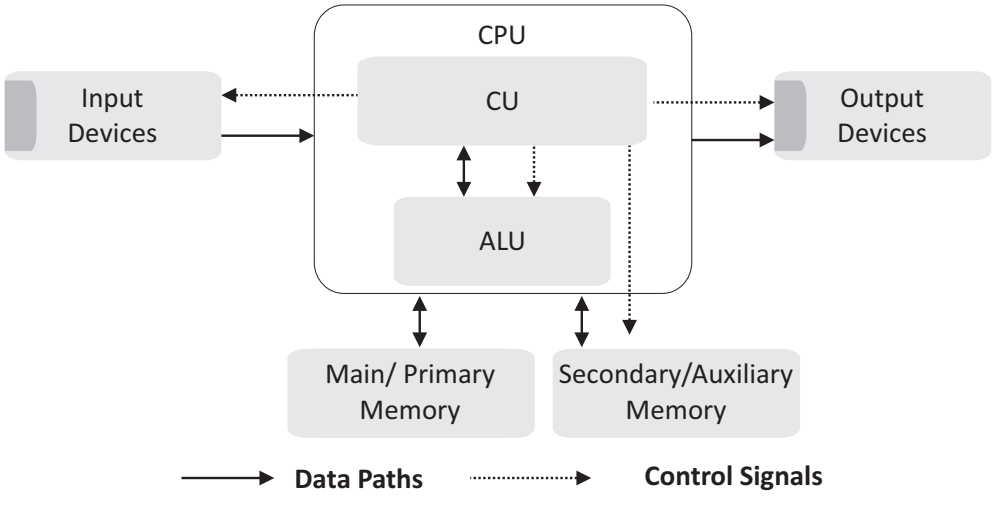
The computer has been able to invade the lives of individuals in a large way, and it is used in all areas of their lives. Computer use is common in homes, institutions, businesses, and education, it is also an integral part of the services, entertainment, and other sectors.

Based on this great position that it has enjoyed, the manufacturers have been interested in producing many shapes and types for it in line with the user's need, including the mobile device, office devices, and others.

The more advanced the device is, the more benefits will be gained from it. Hence the hardware and software are getting updated in the market time and again. One cannot understand the functioning of the computer without understanding the role of hardware and software in it. Hence this chapters dedicates to provide a clear understanding of Hardware and Software.

COMPUTER SYSTEM: CONCEPT

A computer is an electronic device that can be programmed to accept data (input), process it, and generate results (output). A computer along with additional hardware and software together is called a computer system. A computer system primarily comprises a Central Processing Unit (CPU), memory, input/output devices, and storage devices. All these components function together as a single unit to deliver the desired output. A computer system comes in various forms and sizes. It can vary from a high-end server to a personal desktop, laptop, tablet computer, or smartphone. The directed lines represent the flow of data and signal between the components.[1]



Source: https://ncerthelp.com/

1. Reproduced from https://ncert.nic.in/textbook/pdf/kecs101.pdf

Characteristics of a Computer[2]

High Speed

- Computer is a very fast device.
- It is capable of performing calculations of very large amounts of data.
- The computer has units of speed in microseconds, nanoseconds, and even the picosecond.
- It can perform millions of calculations in a few seconds as compared to a man who will spend many months performing the same task.

Accuracy

- In addition to being very fast, computers are very accurate.
- The calculations are 100% error free.
- Computers perform all jobs with 100% accuracy provided that the input is correct.

Storage Capability

- Memory is a very important characteristic of computers.
- A computer has much more storage capacity than human beings.
- It can store a large amount of data.
- It can store any type of data such as images, videos, text, audio, etc.

Diligence

- Unlike human beings, a computer is free from monotony, tiredness, and lack of concentration.
- It can work continuously without any error and boredom.
- It can perform repeated tasks with the same speed and accuracy.

Versatility

- A computer is a very versatile machine.
- A computer is very flexible in performing the jobs to be done.
- This machine can be used to solve problems related to various fields.
- At one instance, it may be solving a complex scientific problem, and the very next moment it may be playing a card game.

Reliability

- A computer is a reliable machine.
- Modern electronic components have long lives.
- Computers are designed to make maintenance easy.

Automation

- Computer is an automatic machine.
- Automation is the ability to perform a given task automatically. Once the computer receives a program

2. Reproduced from Introduction to Computer Hardware, Sathyabama Institute of Science and Technology

i.e., the program is stored in the computer memory, then the program and instruction can control the program execution without human interaction.

Reduction in Paper Work and Cost

- The use of computers for data processing in an organization leads to reduction in paper work and results in speeding up the process.
- As data in electronic files can be retrieved as and when required, the problem of maintenance of large number of paper files gets reduced.
- Though the initial investment for installing a computer is high, it substantially reduces the cost of each of its transactions.

CATEGORIES: TYPES OF COMPUTER SYSTEM[3]

There are various types of computer system. Major categories are discussed below:

1. Supercomputer

Supercomputers are the fastest and the most expensive computers. These huge computers are used to solve very complex science and engineering problems. Supercomputers get their processing power by taking advantage of parallel processing; they use lots of CPUs at the same time on one problem. A typical supercomputer can do up to ten trillion individual calculations every second. Example Supercomputers:

Categories of Computers

Category	*Physical Size*	*Number of Simultaneously Connected Users*
Personal computers (desktop)	Fits on a desk	Usually one (can be more if networked
Mobile computers and mobile devices	Fits on your lap or in your hand	Usually one
Game consoles	Small box or handheld device	One to several
Servers	Small cabinet	Two to thousands
Mainframes	Partial room to a full room of equipment	Hundred to thousands
Supercomputers	Full room of equipment	Hundreds to thousands
Embedded computers	Miniature	Usually one

Source: https://portal.abuad.edu.ng/

There are two types of supercomputers: General Purpose and Special Purpose.[4]

General Purpose: This form of a supercomputer can be divided into three subtypes.

- Vector processing supercomputers rely on array processors. These are similar to the central processing unit (CPU) of a standard computer. However, they perform rapid mathematical operations on a large

3. Reproduced from https://en.wikiversity.org/wiki/Types_of_computers

4. https://blog.udemy.com/categories-of-computer/

number of data elements. These were the basis of the supercomputer industry in the 1980s and 90s, and today's devices still have some form of vector processing instruction.

- Clusters refer to groups of connected computers that work together as a supercomputing unit. An example is a group that runs high-powered database programs that help produce results from the compilation of Big Data.
- Commodity clusters are large numbers of standard-issued personal computers (PCs). They're connected through high-bandwidth and low-latency local area networks (LANs).

Special Purpose: Special purpose computers are supercomputers designed with an explicit purpose to achieve a particular task or goal. They normally use application-specific integrated circuits (ASICs) for better performance. IBM's Deep Blue is an example of one of these devices.

2. Quantum Computer

The industry is replacing supercomputers with Quantum Computers. A quantum computer is a computer that exploits quantum mechanical phenomena. It measures in "Qubits".

3. Mainframe

Mainframe (colloquially, "big iron") computers are similar to supercomputers in many aspects, the main difference between them is the fact that a supercomputer uses all its raw power to focus on very few tasks, while a mainframe performs thousands or millions of operations concurrently. As discussed, mainframes are not supercomputers. Here are a few differences.

- They serve a large number of users.
- They're used as storage space for the collection, compilation, and release of multiple database arguments.
- Mainframe computations are recorded in MIPS instead of quadrillions of instructions.
- They cost less to purchase and maintain.
- They can run multiple operating systems at the same time.

Due to their nature, mainframes are often employed by large organizations for bulk data processing, such as census, industry and consumer statistics, enterprise resource planning, and transaction processing.

4. Server Computer

A server is a central computer that contains collections of data and programs. Also called a network server, this system allows all connected users to share and store electronic data and applications. Two important types of servers are file servers and application servers.

Servers are a step below supercomputers because they don't focus on trying to solve one very complex problem but try to solve many similar smaller ones. An example of servers would be the computers that Wikipedia stores its encyclopedia. Those computers have to go and find the page you're looking for and send it to you. In itself, it's not a big task, but it becomes a job for a server when the computers have to go and find lots of pages for a lot of people and send them to the right place. Some servers, like the ones Google uses for something like Google Documents, have applications on them instead of just files, like Wikipedia.

5. Midrange Computers

The midrange is a step down from a mainframe. About the size of a regular refrigerator, this multiprocessing machine supports a maximum of 200 users at the same time. Despite its name, a midrange computer isn't considered a PC.

This category of machine, originally named minicomputer, was developed in the 1960s as an affordable alternative to mainframes. However, it had higher processing power. The main reason is that midrange computers are capable of running on higher-level programming languages. For example, in the 70s and 80s, they processed data through Fortran or BASIC.

While midrange computers still exist, they are nearly obsolete. The processing power they possessed is now found in desktops, laptops, and even smart devices.

6. Microcomputers

A microcomputer is a smaller machine that runs on a microprocessor. This category costs far less than larger computers with immense power. Such "minicomputers" are used for regular and practical use.

The age of the microcomputer began in 1970 when the microprocessor was released. Rather than a series of circuit boards or vacuum tubes, a single central processing unit was established. Since the size of a computer could be greatly reduced, the company MITS was able to release the first personal microcomputer, the ALTAIR 8800, in 1974.

7. Workstation Computer

Workstations are high-end, expensive computers that are made for more complex procedures and are intended for one user at a time. Some of the complex procedures consist of science, math, and engineering calculations and are useful for computer design and manufacturing. Workstations are sometimes improperly named for marketing reasons. Real workstations are not usually sold in retail, but this is starting to change; Apple's Mac Pro would be considered a workstation.

8. Personal Computer or PC

PC is an abbreviation for a Personal Computer, it is also known as a Microcomputer. It's physical characteristics and low cost are appealing and useful for its users. The capabilities of a personal computer have changed greatly since the introduction of electronic computers. By the early 1970s, people in academic or research institutions had the opportunity for single-person use of a computer system in interactive mode for extended durations, although these systems would still have been too expensive to be owned by a single individual. The introduction of the microprocessor, a single chip with all the circuitry that formerly occupied large cabinets, led to the proliferation of personal computers after about 1975. Early personal computers, generally called microcomputers, were sold often in kit form and in limited volumes and were of interest mostly to hobbyists and technicians. By the late 1970s, mass-market pre-assembled computers allowed a wider range of people to use computers, focusing more on software applications and less on the development of processor hardware. Throughout the 1970s and 1980s, home computers were developed for household use, offering some personal productivity, programming, and games, while somewhat larger and more expensive systems (although still low-cost compared with minicomputers and mainframes) were aimed for office and small business use.

Today a personal computer is an all-around device that can be used as a productivity tool, a media server, and a gaming machine. The modular construction of the personal computer allows components to be easily swapped out when broken or upgraded.

9. Microcontroller

Microcontrollers are mini-computers that enable the user to store data and execute simple commands and tasks. Many such systems are known as embedded systems. The computer in your car, for example, is an embedded system. A common microcontroller that one might come across is called Arduino.

10. Mobile Computers

Mobile computers are small and meant to be taken from place to place. Today, many mobile devices have the same power, if not more, as a desktop computer. Furthermore, because they are destined for use in different locations, they are more versatile.

There have been waves of mobile computing over the years. Each of them has seen advancements that made the devices smaller. Yet, they still had the same performance abilities.

- *Portability*: This concept began with the introduction of the Dynabook in 1968. Though it was originally considered for children, developers realized a portable computer could be used for everyday needs. The first official portable computer, the GRiD Compass, came out in 1981 and was the size of half a briefcase.
- *Miniaturization*: By the 1990s, the size of computer hardware had reached a stage where small mobile computers could be introduced into the market. Thus, the concept of the personal digital assistant (PDA) was created. The PDA wasn't considered a substitute for a desktop. Rather, it was a supplement for those who spent long periods away from their PCs.
- *Connectivity*: This wave is connected to wireless communications. In 1973, a team at Motorola patented a mobile phone concept. A decade later, it produced the DynaTAC 8000X, the first commercial mobile phone small enough to carry. As technology improved, items like a short message service (SMS), calendars, and internet browsing were introduced to extend connectivity.
- *Convergence*: The next wave took place when manufacturers decided to combine specialized mobile devices into hybrids. The first phase was the smartphone. This combined a PDA's functionality with mobile phone operations. This created a large series of innovations that included mini-QWERTY keyboards and touchscreens.
- *Divergence*: Meanwhile, other manufacturers suggested an "information appliance" approach. Here, a mobile computer was designed to perform a specific activity. This is where machines such as the iPod and the Sony PlayStation Portable (PSP) appeared on the market.

  The concepts created during these waves are still active today. Those that aren't, like PDAs, are incorporated into other devices. Below is a list of contemporary mobile computers.

11. Laptops

Laptops are designed to be used in different locations. Components are contained within a single panel that has the functions of a keyboard, mouse, and power switch. An attached screen folds over, so the laptop is easily carried. As their size and weight decreased over the years, laptops have become more popular. When attached to a docking station, they have the same abilities as a desktop. For instance, multiple monitors can be attached to the station for a larger display.

12. Netbook

The netbook is a smaller version of a laptop. It's intentionally designed to be lighter and less expensive. For instance, it might have a screen that's six or seven inches wide, compared to the 11-inch to 13-inch screen of a standard laptop.

Everything in a netbook is miniaturized. Low-voltage, low-power CPUs are installed due to size restraints. To maintain its lightness, a netbook has smaller hard drives.

While popular in the late 2000s and early 2010s, the netbook market has eroded in place of smart tablets.

13. Tablet

A tablet, also called a smart tablet, is a flat mobile computer. Rather than having a keyboard and mouse, it uses touch-screen functionality for navigation. Tablets tend to be more versatile due to the wide range of third-party applications they can leverage.

Several types of tablets exist. Specialized models like the Amazon Kindle are primarily used for items like reading eBooks. However, they also allow users to watch videos and play games.

Hybrid tablets, like Microsoft Surface, have a similar style to this mobile computer. However, they come with a desktop-style OS and keyboard extensions to act like a microcomputer.

14. Handheld game console

Before the popularity of smart devices, handheld game consoles ruled the market. Some of the most popular of these were Nintendo's Game Boy & DS and the Sony PSP. Currently, the Nintendo Switch is the market leader as other consumers turn to their smartphones and tablets to play games.

15. Smartphone

A smartphone is a mobile device that combines cellular and mobile computing functions into one unit. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging. Smartphones typically contain a number of metals–oxide–semiconductor (MOS) integrated circuit (IC) chips, including various sensors that can be leveraged by their software (such as a magnetometer, proximity sensors, barometer, gyroscope, or accelerometer), and support wireless communications protocols (such as Bluetooth, Wi-Fi, or satellite navigation).

16. Microcontrollers

Microcontrollers, also known as embedded systems, are minicomputers that store data. Additionally, they execute simple commands and tasks. These are located in places that form the world called the "Internet of Things" (IoT).

IoT comprises those computing devices that operate out of other systems. Your vehicle's onboard computer is an example. Not only does it maintain the regular operations of your car, but it also sends information to the manufacturer or, in the case of trouble, a third party that alerts emergency services.

Microcontrollers are also part of appliances, including smart refrigerators and manufacturing machines. If it can reach the internet through an app or a wireless connection, the microcontroller is part of the IoT.

EMERGING TECHNOLOGIES

Emerging technologies are technologies whose development, practical applications, or both are still largely unrealized. These technologies are generally new but also include older technologies finding new applications. Emerging technologies are often perceived as capable of changing the status quo.[5]

Emerging technologies are characterized by radical novelty (in the application even if not in origins), relatively fast growth, coherence, prominent impact, and uncertainty and ambiguity. In other words, an emerging technology can be defined as "a radically novel and relatively fast-growing technology characterized by a certain degree of coherence persisting over time and with the potential to exert a considerable impact on the socio-economic domain(s) which is observed in terms of the composition of actors, institutions, and patterns

5. Rotolo, Daniele; Hicks, Diana; Martin, Ben R. (December 2015). "What is an emerging technology?" (PDF). Research Policy. 44 (10): 1827–1843.

of interactions among those, along with the associated knowledge production processes. Its most prominent impact, however, lies in the future and so in the emergence phase is still somewhat uncertain and ambiguous."[6]

Technologies[7]	*Key Benefits*	*Use Cases*
Artificial Intelligence (AI) and Machine Learning (ML)	Automate and optimize processes, provide insights	Chatbots, fraud detection, image recognition, predictive maintenance, personalization, recommendation engines, etc.
Robotic Process Automation (RPA)	Automation of repetitive and rule-based tasks	Data entry, invoicing, HR onboarding, financial reporting, etc.
Edge Computing	Reduced latency, improved performance	Autonomous vehicles, real-time analytics, video streaming, IoT, etc.
Quantum Computing	Solve complex problems traditional computers cannot	Cryptography, drug discovery, optimization, machine learning, etc.
Virtual Reality (VR) and Augmented Reality (AR)	Immersive experiences, user interaction with digital environments	Gaming, education, training, marketing, tourism, etc.
Blockchain	Secure and transparent transactions	Supply chain tracking, digital identity, voting, payment processing, etc.
Internet of Things (IoT)	Improved efficiency, automation, and monitoring	Smart homes, industrial automation, healthcare monitoring, energy management, etc.
5G	Increased speed, reduced latency	Enhanced mobile broadband, autonomous vehicles, smart cities, etc.
Cybersecurity	Protection of data, networks, and systems	Network security, threat intelligence, identity management, encryption, etc.
Full Stack Development	End-to-end development of software applications	Web development, mobile app development, e-commerce, etc.
Computing Power	Increased computing power for complex calculations	Scientific research, weather forecasting, financial modelling, artificial intelligence, etc.
Datafication	Collection, analysis, and use of data	Marketing analytics, customer insights, operational efficiency, personalized experiences, etc.
Digital Trust	Building trust in digital interactions	Online banking, e-commerce, social media, digital identity, etc.
Internet of Behaviours	Analysis and use of data from human behaviour	Retail analytics, healthcare monitoring, smart cities, etc.

6. Ibid

7. Reproduced from Koenig India – Step Forward

Predictive analytics	Analysis and use of data to predict outcomes	Customer retention, fraud detection, supply chain optimization, risk management, etc.
DevOps	Integration of development and operations processes	Continuous integration/continuous deployment (CI/CD), software testing, infrastructure as code, etc.
3D Printing	Printing of physical objects from digital designs	Prototyping, product design, medical implants, customized manufacturing, etc.
AI-as-a-Service	Access to AI technology through cloud computing	Chatbots, predictive analytics, natural language processing, image recognition, etc.
Genomics	Study of genes and their functions	Precision medicine, genetic engineering, disease diagnosis, personalized

Following are the emerging technologies related to computer systems and information and communication technologies:[8]

1. ***Computing Power***

   Computing power has already established its place in the digital era, with almost every device and appliance being computerized. And it's here for even more as data science experts have predicted that the computing infrastructure we are building right now will only evolve for the better in the coming years. At the same time, we have 5G already; gear up for an era of 6G with more power in our hands and devices surrounding us.

2. ***Smarter Devices***

   Artificial intelligence has played an essential role in making our world smarter and smoother. It is not just simulating humans but going the extra mile to make our life hassle-free and simpler. These smarter devices are here to stay in 2023 and even further, as data scientists are working on AI home robots, appliances, work devices, wearables, and so much more! Almost every job needs smart software applications to make our work life more manageable. Smarter devices are another addition to the IT industry that is of high requirement and demand as more companies transform into digital spaces.

3. ***Datafication***

   Datafication is simply transforming everything in our life into devices or software powered by data. So, in short, Datafication is the modification of human chores and tasks into data-driven technology. From our smartphones, industrial machines, and office applications to AI-powered appliances and everything else, data is here to stay for longer than we can ever remember! So, to keep our data stored the right way and secure and safe, it has become an in-demand specialization in our economy.

4. ***Artificial Intelligence (AI) and Machine Learning***

   Artificial Intelligence, or AI, has already received a lot of buzz in the past decade, but it continues to be one of the new technology trends because its notable effects on how we live, work, and play are only in the early stages. AI is already known for its superiority in image and speech recognition, navigation apps, smartphone personal assistants, ride-sharing apps and so much more.

8. Reproduced by Nikita Duggal (2023) Top 18 New Technology Trends for 2023, Simplilearn.com. Available at https://www.simplilearn.com/top-technology-trends-and-jobs-article

Other than that AI will be used further to analyze interactions to determine underlying connections and insights, to help predict demand for services like hospitals enabling authorities to make better decisions about resource utilization, and to detect the changing patterns of customer behavior by analyzing data in near real-time, driving revenues and enhancing personalized experiences. Machine Learning is the subset of AI.

5. Extended Reality

Extended reality comprises all the technologies that simulate reality, from Virtual Reality, Augmented Reality to Mixed Reality, and everything else in between. It is a significant technology trend presently as all of us are craving to break away from the so-called real boundaries of the world. By creating a reality without any tangible presence, this technology is massively popular amongst gamers, medical specialists, and retail and modeling.

6. Digital Trust

With people being accommodated and tangled with devices and technologies, confidence and trust have been built towards digital technologies. This familiar digital trust is another vital trend leading to more innovations. With digital conviction, people believe that technology can create a secure, safe, and reliable digital world and help companies invent and innovate without worrying about securing the public's confidence.

7. 3D Printing

A key trend in innovation and technology is 3D printing which is used to formulate prototypes. 3D printing is another innovation that's here to stay. Companies in the data and healthcare sector require a lot of 3D printing for their products. All you need is a sound knowledge of AI, Machine Learning, Modeling, and 3D printing.

8. Genomics

Imagine a technology that can study your DNA and use it to improve your health, helping you fight diseases and whatnot. Genomics is precisely that technology that peruses upon the make-up of genes, DNAs, their mapping, structure, etc. Further, this can help quantify your genes and result in finding diseases or any possible problems that can later be a health issues.

9. New Energy Solutions

The world has agreed to be greener for the sake of its landscapes and the energy we use. This results in cars running on electricity or battery and houses using greener choices like solar and renewable energy. What's even better is that people are conscious of their carbon footprints and waste; thus, minimizing it or turning those into renewable energy is even more helpful.

10. Robotic Process Automation (RPA)

Like AI and Machine Learning, Robotic Process Automation, or RPA, is another innovative technology. RPA is the use of software to automate business processes such as interpreting applications, processing transactions, dealing with data, and even replying to emails. RPA automates repetitive tasks that people used to do.

11. Edge Computing

Formerly a new technology trend to watch, cloud computing has become mainstream, with major players AWS (Amazon Web Services), Microsoft Azure, and Google Cloud Platform dominating the market.

12. Quantum Computing

The next remarkable technology trend is quantum computing, which is a form of computing that takes advantage of quantum phenomena like superposition and quantum entanglement. This amazing technology trend is also involved in preventing the spread of the coronavirus, and to develop potential vaccines, thanks to its ability to easily query, monitor, analyze, and act on data, regardless of the source. Another field where quantum computing is finding applications is banking and finance, to manage credit risk, for high-frequency trading and fraud detection.

13. Virtual Reality and Augmented Reality

The next exceptional technology trend - Virtual Reality (VR) and Augmented Reality (AR), and Extended Reality (ER). VR immerses the user in an environment while AR enhances their environment.

14. Blockchain

Although most people think of blockchain technology in relation to cryptocurrencies such as Bitcoin, we have to understand that blockchain offers security that is useful in many other ways. In the simplest of terms, blockchain can be described as data you can only add to, not take away from, or change. Hence the term "chain" because you're making a chain of data. Not being able to change the previous blocks is what makes it so secure. In addition, blockchains are consensus-driven, so no one entity can take control of the data. With blockchain, you don't need a trusted third-party to oversee or validate transactions.

15. Internet of Things (IoT)

Another promising new technology trend is IoT. Many "things" are now being built with WiFi connectivity, meaning they can be connected to the Internet—and to each other. Hence, the Internet of Things, or IoT. The Internet of Things is the future and has already enabled devices, home appliances, cars, and much more to be connected to and exchange data over the Internet.

16. 5G

The next technology trend that follows the IoT is 5G. Where 3G and 4G technologies have enabled us to browse the internet, use data driven services, increased bandwidths for streaming on Spotify or YouTube and so much more, 5G services are expected to revolutionize our lives. by enabling services that rely on advanced technologies like AR and VR, alongside cloud-based gaming services like Google Stadia, NVidia GeForce Now, and much more. It is expected to be used in factories, HD cameras that help improve safety and traffic management, smart grid control, and smart retail too.

17. Cybersecurity

Cybersecurity might not seem like an emerging technology, given that it has been around for a while, but it is evolving just as other technologies are. That's in part because threats are constantly new. The malevolent hackers who are trying to illegally access data are not going to give up any time soon, and they will continue to find ways to get through even the toughest security measures. It's also in part because new technology is being adapted to enhance security. As long as we have hackers, cybersecurity will remain a trending technology because it will constantly evolve to defend against those hackers.

COMPONENTS OF COMPUTER SYSTEM

From the computer system perspective, the computer can be defined as a collection of entities (hardware, software, and liveware) that are designed to receive, process, manage, and present information in a meaningful format.

(A) Computer hardware – They are physical parts/ intangible parts of a computer. For example Input devices, output devices, central processing unit, and storage devices.[9]

9. Students to note that Input Device, Output Device and Storage Device is being discussed in below mentioned sub-section of this Chapter.

(B) Computer software[10] – They also known as programs or applications. They are classified into two classes namely - system software and application software.

(C) Liveware – It is the computer user. Also, known as orgware or the humanware. The user commands the computer system to execute instructions.

PRIMARY AND SECONDARY STORAGE[11]

Primary Memory

Primary memory is the internal memory of a computer system. It stores and retrieves data, instructions, and information. The CPU directly and randomly accesses primary memory; hence primary memory is also referred to as Random Access Memory or RAM. It is a volatile memory and loses data and instructions when the power turns off.

Primary Memory: Types

1. ***RAM (Random Access Memory)***

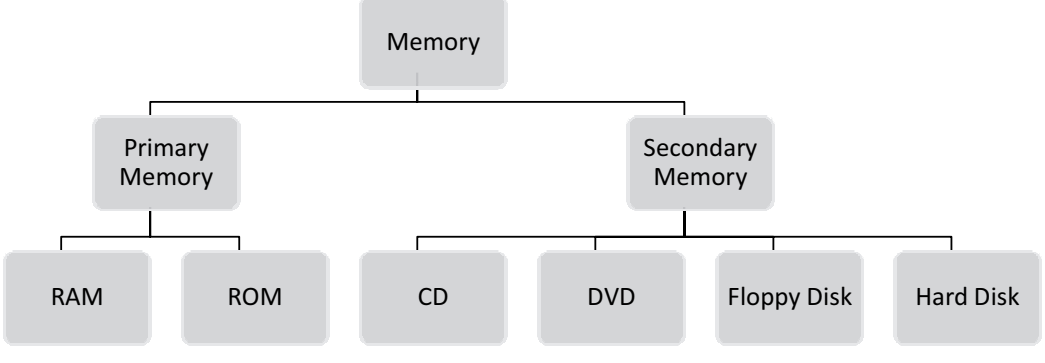
   Random Access Memory or RAM is usually provided as the computer system's main memory. It is also regarded as temporary or cache memory constantly being written to and read. You will lose information saved in primary memory when the power supply of the computer or laptop turns off. Simply put, RAM is a primary memory from which information can only be read.

2. ***ROM (Read-Only Memory)***

   ROM is a non-volatile memory containing data that we cannot change. In this case, information is not lost when the power supply is turned off. ROM information is determined by the computer manufacturer and is permanently stored at the time of manufacture so that the user cannot overwrite it.

Primary Memory: Characteristics

- The computer cannot function without primary memory.
- It is known as the main memory.
- You may lose data in case the power is off.
- Also known as volatile memory.
- It is the working memory of the computer.
- It is faster as compared to secondary memory.
- Examples: RAM, ROM, cache, PROM, EPROM, registers, etc.



Source: https://www.shiksha.com/

10. Students to note that Software is discussed in detail in the other sub-sections of this chapter.

11. Reproduced from https://www.shiksha.com/online-courses/articles/difference-between-primary-memory-and-secondary-memory/

Secondary Memory: Meaning

Secondary memory is a storage device that the CPU cannot access directly. It is used as a permanent storage device.

The CPU accesses these devices through an input/output channel, and data is first transferred to primary from secondary storage before being accessed. Modern computers often use hard drives and optical storage devices (CDs, DVDs) as secondary storage devices.

A secondary storage device organizes data into files and directories based on a file system. It also allows the user to access or use additional information like access permissions, owner, last access time, etc. Also, secondary memory is used temporarily to keep less used data when primary memory gets full.

Secondary memory devices are less expensive and can store vast amounts of data, audio, video, and multimedia files. Organizations can store the equivalent of a roomful of data on disks that consume dramatically and significantly less physical space.

Secondary Memory: Types

- Solid-state storage devices, such as USB memory sticks.
- Optical storage devices, such as CDs, DVDs, and Blu-ray discs.
- Magnetic storage devices include zip, floppy, and hard disk drives.

Secondary Memory: Characteristics

- These are magnetic and optical memories.
- It is a type of non-volatile memory.
- Data is permanently stored even when the computer is turned off
- It helps store data on a computer
- The computer can function without secondary memory
- Slower than primary memory
- Examples: magnetic tapes, optical discs, floppy disks, flash memory [USB drives], paper tape, punched cards, etc.

COMPUTER STORAGE CAPACITIES

Storage capacity is an important factor when deploying infrastructure in the data center. Storage capacity refers to the disk space one or more storage devices provide. It measures how much data a computer system may contain. For example, a computer with a 500GB hard drive has a storage capacity of 500 gigabytes A network server with four 1TB drives, has a storage capacity of 4 terabytes. Storage capacity is often used synonymously with “disk space.” However, it refers to overall disk space, rather than free disk space. For example, a hard drive with a storage capacity of 500GB may only have 150MB available if the rest of the disk space is already used up. Storage vendors describe capacity in different ways, and it’s essential that you know how to interpret them properly for sizing the infrastructure that your organization really needs, and for comparing the cost of capacity (cost divided by gigabytes) between different storage systems. However, interpreting the capacity of modern storage systems can be surprisingly tricky. Different vendors use wildly different metrics to advertise the capacity of their systems, including:

Raw Capacity

This is the total capacity of the storage media in the system. For example, if your system contains 20 drives at 5TB each, the raw capacity is 100 TB. Vendors sometimes mistakenly price their systems based on raw

capacity, but users should focus on usable capacity instead because usable capacity can be significantly lower than raw capacity. That is why raw capacity is generally reported in decimal terabytes.

Usable Capacity

This is how much data can be stored in the system in the absence of any data reduction, meaning before data reduction. The use of the term usable capacity to mean capacity before data reduction. Usable capacity is lower than raw capacity because of overheads such as RAID (redundant array of independent disks) and flash over-provisioning. The ratio of the usable capacity to the raw capacity is referred to as the "usable ratio", which by definition is usable capacity divided by raw capacity is greater or equal to one.

Usable Capacity / Raw Capacity = Usable Ratio

COMPUTER PERIPHERALS – INPUTS, OUTPUT, AND STORAGE DEVICES

1. ***Input Unit:***

   The input unit consists of input devices that are attached to the computer. These devices take input and convert it into binary language that the computer understands. Some of the common input devices are keyboard, mouse, joystick, scanner etc.

   The Input Unit is formed by attaching one or more input devices to a computer.

   A user input data and instructions through input devices such as a keyboard, mouse, etc. The input unit is used to provide data to the processor for further processing.

2. ***Central Processing Unit/Storage[12]:***

   Once the information is entered into the computer by the input device, the processor processes it. The CPU is called the brain of the computer because it is the control Centre of the computer. It first fetches instructions from memory and then interprets them so as to know what is to be done. If required, data is fetched from memory or input device. Thereafter CPU executes or performs the required computation, and then either stores the output or displays it on the output device. The CPU has three main components, which are responsible for different functions: Arithmetic Logic Unit (ALU), Control Unit (CU) and Memory registers.

   a. *Arithmetic and Logic Unit (ALU):* The ALU, as its name suggests performs mathematical calculations and takes logical decisions. Arithmetic calculations include addition, subtraction, multiplication and division. Logical decisions involve the comparison of two data items to see which one is larger or smaller or equal. Arithmetic Logical Unit is the main component of the CPU. It is the fundamental building block of the CPU. Arithmetic and Logical Unit is a digital circuit that is used to perform arithmetic and logical operations.

   b. *Control Unit:* The Control unit coordinates and controls the data flow in and out of the CPU, and also controls all the operations of ALU, memory registers and also input/output units. It is also responsible for carrying out all the instructions stored in the program. It decodes the fetched instruction, interprets it and sends control signals to input/output devices until the required operation is done properly by ALU and memory.

      - The Control Unit is a component of the central processing unit of a computer that directs the operation of the processor.
      - It instructs the computer's memory, arithmetic and logic unit, and input and output devices on how to respond to the processor's instructions.
      - In order to execute the instructions, the components of a computer receive signals from the control unit.

      It is also called the central nervous system or brain of the computer.

12. Students to note - Primary and Secondary Storage is already discussed in the above mentioned sub-sections of the Chapter.

c. *Memory Registers:* A register is a temporary unit of memory in the CPU. These are used to store the data, which is directly used by the processor. Registers can be of different sizes (16-bit, 32-bit, 64 bit and so on) and each register inside the CPU has a specific function, like storing data, storing an instruction, storing address of a location in memory etc. The user registers can be used by an assembly language programmer for storing operands, intermediate results etc. Accumulator (ACC) is the main register in the ALU and contains one of the operands of an operation to be performed in the ALU.

- Memory Unit is the primary storage of the computer.
- It stores both data and instructions.
- Data and instructions are stored permanently in this unit so that they are available whenever required.

3. Output Unit:

The output unit consists of output devices that are attached to the computer. It converts the binary data coming from the CPU to human understandable form. The common output devices are monitor, printer, plotter, etc.

- The output unit displays or prints the processed data in a user-friendly format.
- The output unit is formed by attaching the output devices of a computer.
- The output unit accepts the information from the CPU and displays it in a user-readable form.

COMPUTER SOFTWARE[13] : AN INTRODUCTION

Software is a set of computer programs and associated documentation and data. This is in contrast to hardware, from which the system is built and which actually performs the work. In the previous sections of this chapter, we have read in detail about the hardware of the computer system. But the hardware is of no use on its own. Hardware needs to be operated by a set of instructions. These sets of instructions are referred to as software. It is that component of a computer system, which we cannot touch or view physically. It comprises of the instructions and data to be processed using the computer hardware.

The computer software and hardware complete any task together. The software comprises of set of instructions which on execution deliver the desired outcome. In other words, each software is written for some computational purpose. Some examples of software include operating systems like Ubuntu or Windows 7/10, word processing tools like LibreOffice Writer or Microsoft Word, video player like VLC Player, photo editors like Paint and LibreOffice Draw. A document or image stored on the hard disk or pen drive is referred to as a softcopy. Once printed, the document or an image is called a hardcopy.

Software is a set of instructions, data or programs used to operate computers and execute specific tasks. It is the opposite of hardware, which describes the physical aspects of a computer. Software is a generic term used to refer to applications, scripts and programs that run on a device. It can be thought of as the variable part of a computer, while hardware is the invariable part.

The two main categories of software are:

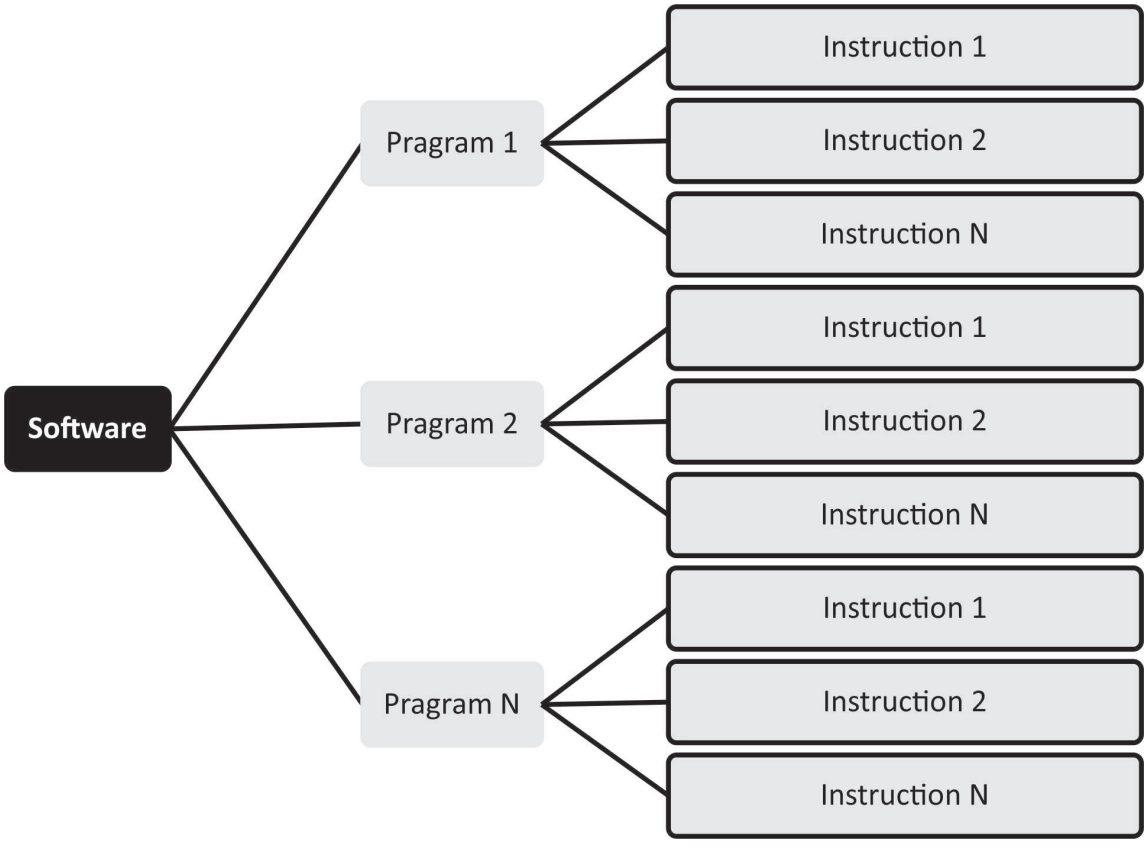
- Application software, and
- System software.

An application is software that fulfills a specific need or performs tasks. System software is designed to run a computer's hardware and provides a platform for applications to run on top of.

13. Source: https://www.techtarget.com/searchapparchitecture/definition/software

Other types of software include programming software, which provides the programming tools software developers need; middleware, which sits between system software and applications; and driver software, which operates computer devices and peripherals.

Set of instructions that tells the computer hardware what to do is known as computer program. This program or collection of such programs is known as computer software. Concept of software is illustrated in following figure:



Source: https://www.codesansar.com/

Among the various categories of software, the most common types include the following:

- **Application software:** The most common type of software, application software is a computer software package that performs a specific function for a user, or in some cases, for another application. An application can be self-contained, or it can be a group of programs that run the application for the user. Examples of modern applications include office suites, graphics software, databases and database management programs, web browsers, word processors, software development tools, image editors and communication platforms.
- **System software:** These software programs are designed to run a computer's application programs and hardware. System software coordinates the activities and functions of the hardware and software. In addition, it controls the operations of the computer hardware and provides an environment or platform for all the other types of software to work in. The OS is the best example of system software; it manages all the other computer programs. Other examples of system software include the firmware, computer language translators and system utilities.
- **Driver software:** Also known as device drivers, this software is often considered a type of system software. Device drivers control the devices and peripherals connected to a computer, enabling them

to perform their specific tasks. Every device that is connected to a computer needs at least one device driver to function. Examples include software that comes with any nonstandard hardware, including special game controllers, as well as the software that enables standard hardware, such as USB storage devices, keyboards, headphones and printers.

- **Middleware:** The term middleware describes software that mediates between application and system software or between two different kinds of application software. For example, middleware enables Microsoft Windows to talk to Excel and Word. It is also used to send a remote work request from an application in a computer that has one kind of OS, to an application in a computer with a different OS. It also enables newer applications to work with legacy ones.
- **Programming software:** Computer programmers use programming software to write code. Programming software and programming tools enable developers to develop, write, test and debug other software programs. Examples of programming software include assemblers, compilers, debuggers and interpreters.

SOFTWARE TRENDS

An article published in DevTeam.Space[14] highlighted the key trends in software development are as follows:

1. ***Mixed Reality (MR): High potential in enterprise solutions***

   Mixed Reality (MR), i.e., a combination of Augmented Reality (AR) and Virtual Reality (VR) has significant potential in enterprise applications. AR integrates digital content with the physical environment of users, whereas VR creates an immersive experience for users. Organizations in many sectors like defense, tourism, architecture, construction, gaming, healthcare, etc. are realizing key business value with the help of this technology.

2. ***Blockchain: Augmenting enterprise solutions with transparency, efficiency and security***

   While cryptocurrencies like Bitcoin and Ether have made us sit up and notice blockchain, the technology has wide implications for enterprise systems. Blockchain is a Peer-To-Peer (P2P) network, and it offers decentralization, a distributed ledger, security features, and transparency.

   Smart contracts running on blockchain networks are tamper-proof and transparent, therefore, they improve trust. Their execution is irreversible, which can make contract administration easier. Businesses and governments are keenly exploring blockchain, therefore, its global market is growing rapidly.

3. ***Artificial Intelligence (AI): Ushering in intelligent enterprise systems***

   Artificial Intelligence (AI) is a multi-disciplinary branch of computer science, which intends to make machines perform tasks that only human beings could do earlier. It is a vast field, and while parts of it have been commercialized, research & development continue on its other dimensions.

   AI includes various capabilities like machine learning (ML), deep learning, vision, natural language processing, speech, etc.

4. ***The Internet of Things (IoT)***

   As technology trends go, the Internet of Things (IoT) is one that could have far-reaching impacts on our world, and not just on businesses. IoT is a network of physical objects like gadgets, devices, vehicles, appliances, etc., and these devices use sensors. Devices on these networks use application programming interfaces (APIs) to exchange data over the Internet.

14. Source: https://www.devteam.space/blog/10-trends-in-software-development/

IoT is a result of the integration of various technologies like sensors, Big Data, AI, ML, Radio-Frequency Identification (RFID), and APIs. Read more about it in "What is the Internet of Things (IoT)?".

5. Language and framework trends for developing enterprise apps

Both Kotlin and Swift, the popular languages for native development on Android and iOS respectively, figure prominently in the list of "most preferred languages".

6. Cybersecurity: A Key consideration when building enterprise solutions

Experts consistently point out how cybercrimes cause trillions of dollars in losses, therefore, it is no surprise that cybersecurity is a prominent consideration when developing an enterprise app. Cybercriminals are organized, moreover, they are continuously upgrading their capabilities.

One ought to proactively mitigate the key application security risks. More often than not, mitigating application security risks boils down to managing the project well, adhering to IT architecture and coding guidelines, etc.

Key applications security risks are as follows:

- Injection;
- Ineffective Authentication;
- Exposure of Sensitive Data;
- XML External Entities (XXE);
- Incorrect Implementation of Identity and Access Management;
- Inadequate Security Configurations;
- Cross-Site Scripting (XSS);
- Deserialization without Adequate Security;
- Using Outdated Software with Known Vulnerabilities;
- Sub-Optimal Logging and Monitoring Processes.

7. ***"Progressive Web Applications" (PWAs)***

"Progressive Web Apps" (PWAs) are web apps; however, they deliver a user experience partly similar to native mobile apps. They are responsive, speedy, and secure, moreover, they can work offline. While PWAs fall short of the native app user experience, developing them can be a good option if the development budget is your priority. There is only one codebase to develop and maintain, therefore, PWAs are less costly. In recent years, several businesses have seen improved customer engagement with the help of PWAs, as you can read in "Progressive Web Apps (PWA): Source materials".

8. Low-Code Development

A key trend that has emerged in recent years is low-code development. Businesses using this approach have the objective of improving software development efficiency, and they seek to minimize hand-coding for this.

Low-code development platforms offer GUIs, and developers use them to draw flowcharts depicting the business logic. The platform then generates code for implementing that business logic.

If you plan to take advantage of such platforms then you should look for enterprise-grade platforms with industry-standard security features. Appian and Mendix are good examples of low-code development platforms.

9. Code quality

Some things never change. And that's why the importance of code quality in software development will never decrease. Since many projects involve continuous integration of code from multiple contributors, this process can throw up many code issues. Software development teams that maintain a high quality of code enable their organizations to maintain the code easily.

10. Outsourcing

As the global business environment grows more and more complex, businesses are striving to make the best use of the capabilities they have. Businesses have found out the importance of focusing on their core competencies and offloading the peripheral tasks to partners that have core competencies there. This realization continues to drive the trend of IT outsourcing.

One might need to outsource software development for its business too, however, focus on the right priorities. E.g., in the longer term, delivering a quality product to your customers matters more than reducing cost.

MULTI-PROGRAMMING

Multi-programming is the allocation of more than one concurrent program on a computer system and its resources. Multiprogramming allows using the CPU effectively by allowing various users to use the CPU and I/O devices effectively. Multiprogramming makes sure that the CPU always has something to execute, thus increases the CPU utilization.

MULTI-PROCESSING

Multi-processing is the use of two or more central processing units (CPUs) within a single computer system. The term also refers to the ability of a system to support more than one processor or the ability to allocate tasks between them. There are many variations on this basic theme, and the definition of multiprocessing can vary with context, mostly as a function of how CPUs are defined (multiple cores on one die, multiple dies in one package, multiple packages in one system unit, etc.). According to some on-line dictionaries, a multiprocessor is a computer system having two or more processing units (multiple processors) each sharing main memory and peripherals, in order to simultaneously process programs

TIME SHARING

Time sharing is the sharing of computing resources among several users simultaneously. Since this will allow many users to work in a single computer system simultaneously, it would lower the cost of providing computing capabilities.

BATCH PROCESSING

Batch processing is the method computers use to periodically complete high-volume, repetitive data jobs. Certain data processing tasks, such as backups, filtering, and sorting, can be compute intensive and inefficient to run on individual data transactions. Instead, data systems process such tasks in batches, often in off-peak times when computing resources are more commonly available, such as at the end of the day or overnight. For example, consider an ecommerce system that receives orders throughout the day. Instead of processing every order as it occurs, the system might collect all orders at the end of each day and share them in one batch with the order fulfillment team.

A good example of batch processing is how credit card companies do their billing. When customers get their credit card bills, it isn't a separate bill for each transaction; rather, there is one bill for the entire month.

ON-LINE AND REAL TIME PROCESSING[15]

Online Systems

Online systems are the type of systems that are logged in or connected to the internet, such systems include online gaming platforms, chatting through different social media platforms, etc. A number of applications are available which are online in nature.

Advantages of Online Systems:

- Online systems help in making communication possible in the whole world at a faster speed.
- Online systems are less costly when compared to real-time systems, anyone can use them with the help of the internet.
- Response time is really good in the case of many online systems like booking systems or online shopping sites.
- These systems do not have heavy hardware requirements means they can be used with simple hardware resources.

Limitations of Online Systems:

- There are times when a large number of data is fetched or either sent to online systems and in such cases, these systems fail to handle that data.
- They are not providing in-time information means these systems lag when compared to real-time systems hence these systems cannot be used for high-priority tasks.

Real-Time Systems:

Real-time systems are those systems that do not lag and respond instantly. These are different from online systems in the sense that they transform their state with correspondence to real or physical time.

Advantages of Real-Time Systems:

- These are the fastest available systems and hence are used in top-priority operations like rocket launching systems, military communications, etc.
- The response time of these systems is instant, they don't lag and provide real-time information or services.
- Real-time systems are the foundation of advanced technology in various fields like communication, information retrieval, etc.
- These systems are able to handle a huge amount of data.

Limitations of Real-Time Systems:

- These systems are expensive so they are not available for use to everybody.
- Heavy system requirements to use these systems, these systems need special software and hardware resources.

Online and real-time systems are two different types of computer systems used in organizations.

- Online systems are computer systems that are connected to a network and are accessible to users from anywhere at any time. These systems typically allow users to interact with data stored in databases and perform operations such as data entry, data retrieval, and data modification. Examples of online systems include e-commerce websites, banking systems, and online booking systems.

15. Reproduced from https://www.geeksforgeeks.org/

- Real-time systems, on the other hand, are computer systems that are designed to process data in real-time, as soon as it is generated. These systems typically have strict timing constraints and must be able to respond to events in a timely manner. Examples of real-time systems include control systems for manufacturing plants, traffic control systems, and flight control systems.

Key differences between online and real-time systems include:

- **Timing**: Online systems allow users to access and interact with data at any time, while real-time systems are designed to respond to events in real time.
- **Latency**: Online systems may have higher latency as data is transmitted over a network, while real-time systems typically have very low latency.
- **Response time**: Online systems may have longer response times as they must wait for user input and may require additional processing time, while real-time systems must respond to events quickly and have very short response times.
- **Reliability**: Real-time systems must be highly reliable and ensure that data is processed accurately and on time, while online systems may not require the same level of reliability.

In summary, while online systems allow users to interact with data stored in databases and are accessible from anywhere at any time, real-time systems are designed to process data in real time and must respond to events quickly and accurately.

APPLICATION SOFTWARE[16]

The term "application software" refers to software that performs specific functions for a user. When a user interacts directly with a piece of software, it is called application software. The sole purpose of application software is to assist the user in doing specified tasks. Microsoft Word and Excel, as well as popular web browsers like Firefox and Google Chrome, are examples of application software. It also encompasses the category of mobile apps, which includes apps like WhatsApp for communication and games like Candy Crush Saga. There are also app versions of popular services, such as weather or transportation information, as well as apps that allow users to connect with businesses. Global Positioning System (GPS), Graphics, multimedia, presentation software, desktop publishing software, and so on are examples of such software.

Function of application software:

Application software programs are created to help with a wide range of tasks. Here are a few examples:

- Information and data management;
- Management of documents (document exchange systems);
- Development of visuals and video;
- Emails, text messaging, audio and video conferencing, and cooperation are all options;
- Management of accounting, finance, and payroll;
- Management of resources (ERP and CRM systems);
- Management of a project;
- Management of business processes;
- Software for education (LMS and e-learning systems);
- Software for healthcare applications.

16. Reproduced from https://www.geeksforgeeks.org/what-is-application-software/

Types of application software:

Application software can also be categorized based on its chargeability and accessibility. Here is some application software:

- **Freeware**: It is offered for free, as the name implies. You can utilize freeware application software that you can obtain from the Internet. This software, on the other hand, does not allow you to change it or charge a fee for sharing it. Examples include Adobe PDF, Mozilla Firefox, and Google Chrome.
- **Shareware**: This is given away to users for free as a trial, usually with a limited-time offer. If consumers want to keep using this application software, they will have to pay. WinZip, Anti-virus, and Adobe Reader are instances of shareware.
- **Open-source**: This type of application software comes with the source code, allowing you to edit and even add features to it. These could be offered for free or for a fee. Open-source application software includes Moodle and Apache Web Server.
- **Closed source**: This category includes the majority of the application software programs used nowadays. These are normally charged, and the source code is usually protected by intellectual property rights or patents. It usually comes with a set of restrictions. Microsoft Windows, Adobe Flash Player, WinRAR, macOS, and other operating systems are examples.

Examples of application software:

Some of the examples of application software are:

- **System for Hotel Management:** It relates to the hotel industry's management strategies. Hotel administration, accounting, billing, marketing, housekeeping, and front office or front desk.
- **System for Payroll Management:** It is a term used by all modern businesses to refer to every employee who receives a regular salary or another form of payment. The payroll software calculates all different payment options and generates the relevant paychecks. Employee salary slips can also be printed or sent using this software.
- **System for Human Resources Management:** It describes the systems and activities that exist at the nexus of Human Resource Management (HRM) and Information Technology (IT). The HR department's role is primarily administrative and is found in all businesses.
- **Attendance Recording System:** It's a piece of software that tracks and optimizes a person's or student's presence in an organization or school. Nowadays, customers' existing time/attendance recording devices, such as biometrics/access cards, can be connected with attendance systems. Attendance management can be accomplished in two ways: Integration of biometrics & Integration of manual attendance
- **System of Billing:** It is the billing software that is utilized to complete the billing process. It keeps track of marked products and services given to a single consumer or a group of customers.

LESSON ROUND-UP

- A computer is an electronic device that receives information and data, automatically stores it and retrieves it at any time, and uses it in a useful manner.
- One cannot understand the functioning of the computer without understanding the role of hardware and software in it.

- Hence this chapters dedicates to provide a clear understanding of Hardware and Software.
- Computer system primarily comprises a central processing unit (CPU), memory, input/output devices and storage devices.
- All these components function together as a single unit to deliver the desired output.
- There are majorly eight types of computer system.
- Emerging technologies are characterized by radical novelty (in application even if not in origins), relatively fast growth, coherence, prominent impact, and uncertainty and ambiguity.
- From the computer system perspective, computer can be defined as a collection of entities (hardware, software and liveware) that are designed to receive, process, manage and present information in a meaningful format.
- Primary memory is the internal memory of a computer system. It stores and retrieves data, instructions, and information.
- Secondary memory is a storage device that the CPU cannot access directly. It is used as a permanent storage device.
- Storage capacity is an important factor when deploying infrastructure in the data center.
- Storage capacity refers on disk space one or more storage devices provides.
- It measures how much data a computer system may contain.
- Software is a set of computer programs and associated documentation and data. This is in contrast to hardware, from which the system is built and which actually performs the work.
- The computer software and hardware complete any task together. The software comprises of set of instructions which on execution deliver the desired outcome.
- In other words, each software is written for some computational purpose.
- Software is a generic term used to refer to applications, scripts and programs that run on a device.
- Some examples of software include operating systems like Ubuntu or Windows 7/10, word processing tools like LibreOffice Writer or Microsoft Word, video player like VLC Player, photo editors like Paint and LibreOffice Draw.
- Multi-programming is the allocation of more than one concurrent program on a computer system and its resources.
- Multi-processing is the use of two or more central processing units (CPUs) within a single computer system.
- Time sharing is the sharing of computing resources among several users simultaneously.
- Batch processing is the method computers use to periodically complete high-volume, repetitive data jobs.
- Real-time systems are those systems that do not lag and respond instantly.
- These are different from online systems in the sense that they transform their state with correspondence to real or physical time.
- The term “application software” refers to software that performs specific functions for a user.
- When a user interacts directly with a piece of software, it is called application software.

- The sole purpose of application software is to assist the user in doing specified tasks.
- Microsoft Word and Excel, as well as popular web browsers like Firefox and Google Chrome, are examples of application software.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. Briefly describe any four types of computer system prevalent in present digital era in India.
2. Write a short note on emerging technologies in the world of information and communication technologies.
3. What do you mean by Primary and Secondary Storage? Also state the difference between the two.
4. What is Software? Discuss five recent trends in software in 2023.
5. Write a note on Application Software. Give some example of Application Software.

LIST OF FURTHER READINGS

- Archana Charles (2023) Top 19 New Technology Trends Emerging in 2023, Koenig India – Step Forward
- Basic Concepts in Computer Hardware and Software, Wikieducator.
- Categories of Computers: Types and Components, Udemy Team. Available at https://blog.udemy.com/categories-of-computer/
- Computer System, Book by NCERT. Available at https://ncert.nic.in/textbook/pdf/kecs101.pdf
- Introduction to Computer Hardware, Satyabhama Institute of Science and Technology, 2021.
- Kaur Gurneet (2023) 10 Emerging Technologies in Computer Science that will shape our future, The Coin Telegraph.
- Udemy Team (2022) Categories of Computers: Types and Components, Blog Udemy.

LIST OF OTHER REFERENCES

- https://ncerthelp.com/cbse%20notes/class%2011/ip/NotsForIPClass11Chapter%20(1).pdf
- https://byjus.com
- https://static.vikaspedia.in/media/files_en/education/Digital%20Litercy/it-literacy-courses-in-associating-with-msup/computer-hardware-and-software-stu.pdf
- https://www.takshilalearning.com/importance-of-computer/#:~:text=The%20use%20of%20a%20computer%20at%20home%20provides%20great%20advantages,learning%20new%20skills%20and%20hobbies.
- https://www.geeksforgeeks.org/
- https://www.koenig-solutions.com/blog/top-new-technology-trends
- https://www.javatpoint.com/multiprogramming-vs-time-sharing-operating-system#:~:text=The%20main%20difference%20between%20Multi,is%20to%20minimize%20response%20time.
- https://aws.amazon.com/what-is/batch-processing/#:~:text=Batch%20processing%20is%20the%20method,run%20on%20individual%20data%20transactions.

Network Basics and Security

Lesson 8

KEY CONCEPTS

■ Network ■ Wired Network ■ Wireless Network ■ Computer Security ■ Network Security ■ Internet Security ■ Network Protocol ■ IP Address ■ Nodes and Hosts ■ Protocols ■ Data Packets ■ Domain Name

Learning Objectives

To understand:

- The concept of network and computer security
- And get acquainted with different types of network
- And gather an understanding of how networks operate along with relevant networking models
- The common threats to network security
- Measures to protect against attacks to network

Lesson Outline

- Computer and Network Security: An Introduction
- Intranets
- Extranets
- Internet
- Networking concepts OSI models TCP/IP model
- Ports
- Secure protocols
- Common network attacks
- Network Devices Hubs
- Bridges
- Switch
- Security Devices
- Firewall
- Lesson Round-Up
- Glossary
- Test Yourself
- List of Further Readings

INTRODUCTION

In today's technologically driven world, computers are used to network and connect on a daily basis throughout organizations, businesses, schools, government institutions and authorities. The importance of network and security can be understood by way of the following example:

In a multinational corporation having corporate offices around the world, employees are dependent upon computers to connect with clients, hold meetings and execute projects. In order to connect the huge workforce, such corporations have networks which host multiple servers at the same time. The workstations of the employees may have varied types of operating systems, hardware, software configuration, IP protocols and the employees using them may have different levels of awareness regarding cyberspace. Considering that thousands of employee workstations are connected to the internet, such a company network can become a potential target of cyber-attacks.

In this Lesson, an attempt has been made to trace the basic concepts of network and network security.

NETWORK SECURITY

A computer network is a group of two or more devices/computers connected to one another for efficient exchange of information. Networks are connected through networking devices like computer, switches, routers, modems, etc. These networking devices may be connected through wires (for example, cables) resulting in a wired network or through wireless media (for example, air) resulting in a wireless network.

It is important to note that data on a network is transmitted for communication in the form of packets, which are nothing but small chunks of data[1].

Network Security refers to the protective measures undertaken by an organization or individual to secure its network systems and data from unauthorized access and attacks by hackers. The basic aim of any network security system is to safeguard the accessibility, accuracy and confidentiality of sensitive data.

The importance of network security can be understood by way of the following example: Most businesses have moved to an electronic mode where transactions are conducted online and goods are sold through company owned websites or e-commerce websites. In order to facilitate such operations on the internet, it is important to safeguard company resources and information, as any unauthorized attack can leak sensitive company and customer information into the public domain. Even a minor security threat has the potential to disrupt the company's efficiency and reputation in the market.

Network security seeks to protect data in order to ensure and maintain the following[2]:

Data confidentiality: Assures that the data does not fall in the hands of unauthorized users.

Privacy: Assures that individuals are able to decide what data belonging to them may be disclosed, to whom it is disclosed and the extent of disclosure.

Data Integrity: Assures that the data remains in its intended form, subject to modification only in authorized manner.

System Integrity: Assures that systems perform their intended function, unhampered by any external manipulation.

Availability: Assures that data available on the system is readily accessible and not denied to authorized users.

1 Computer Networks, Available at: https://ncert.nic.in/textbook/pdf/lecs110.pdf.
2 William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Publication Ltd. 2017, England.

Objectives of Network Security

It must be noted that a secure network is one which is able to:

a. Control the physical access to the network.

b. Prevent any accidental deletion, modification or tampering of data.

c. Detect and prevent internal network security breaches.

d. Detect and prevent external network attacks.

INTRANETS

It refers to a private network within organizations for ensuring secure data sharing and communication among all the employees[3]. It enables the organization to safely transmit sensitive and confidential data. The term 'intra' means 'inside'. Therefore, it can be said that intranet centralises the digital workplace of an organisation, so that documents, projects, databases, etc. can be shared securely within the organization[4]. Intranet is used by departments and all employees of a company.

Intranet enables the organization to not only benefit from time and cost savings but also increases the productivity and efficiency of workforce, by making the information available on a real time basis. Intranet also serves as a tool to facilitate easy communication between the workforce.

EXTRANETS

It refers to a private network existing within an organization which uses the internet to connect with people outside the organization, like customers and suppliers. This network is controlled in a manner that allows customers, third parties or partners to access specific information only without providing them with access to entire network[5].

Extranet is used by business partners, suppliers and customers for collaboration with the company[6]. Benefits of extranet include flexibility, reduced time in processing of orders, timely updation of information and reduction of errors.

INTERNET

A worldwide network of inter-connected computers, servers, phones, and electronic devices is referred to as the internet. These devices communicate with one another using the transmission control protocol (TCP) standard to allow for the quick exchange of data and files as well as other services[7].

Internet is a global hub of computer networks which enables a user at one computer system/workstation to not only interact but also share and receive data and resources from any other user working on any other system/ workstation[8].

The internet is widely used for purposes of communication, transmission of information and sharing of resources across devices on a network. Whenever a user tries to visit a website, a request is made by protocol to the server, which is a collection of web pages. The server in turn, looks for the exact webpage and delivers the same to the user's computer/device, resulting into an 'end-to-end' user experience[9].

3 Difference between Intranet and Extranet, Available at: https://byjus.com/gate/difference-between-intranet-and-extranet/.
4 Ibid.
5 Supra, Note 2.
6 Ibid.
7 Chiradeep BasuMallick, What Is the Internet: Meaning, Working and Types, SPICEWORKS, (February 22, 2022); Available at: https://www.spiceworks.com/tech/networking/articles/what-is-the-internet/.
8 Ibid.
9 Ibid

NETWORKING CONCEPTS

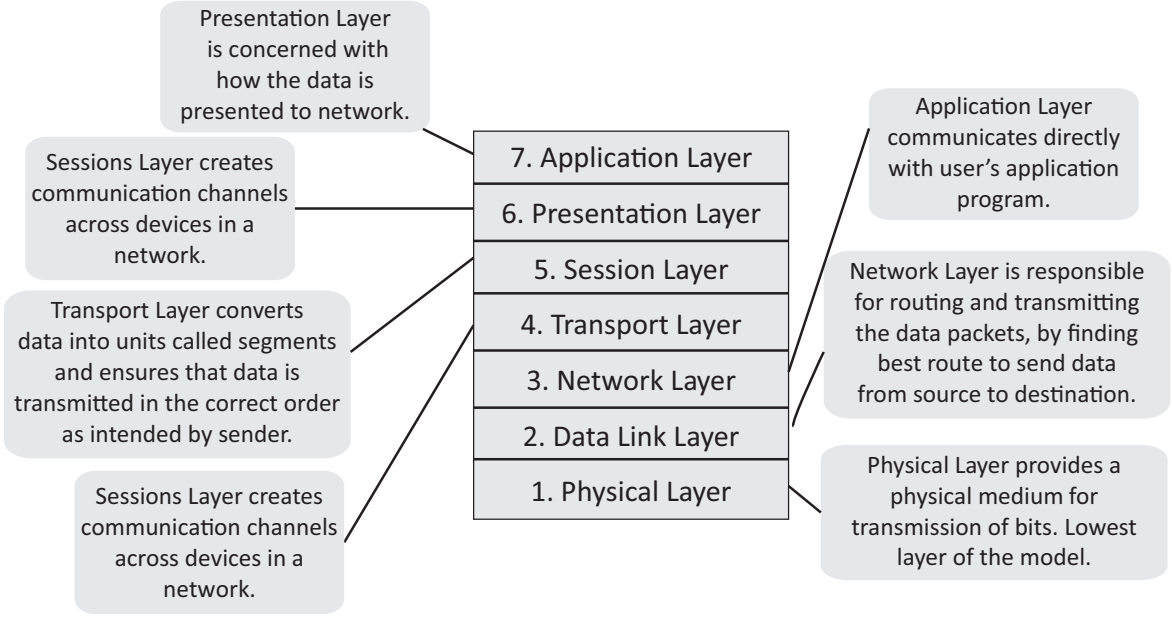
OSI model

Open Systems Interconnection (OSI) model is reference framework created by the International Standards Organization to foster an understanding of how technologies and devices interact with each other on a network. This model consists of different layers which work together to move data around a network[10]. The different layers of OSI Network will be discussed as follows:

- **Physical Layer:** This is the lowest layer in OSI model and is concerned with physical aspect of data transmission. Here, information is contained in the form of bits, which is transmitted to network notes. The transmission takes place through optical fibre, metallic cable, wireless radio wave, etc.
- **Data Link Layer:** This layer breaks the data into smaller units called frames and adds a header and trailer to each frame. The header contains a destination address to which the frame is transferred. This layer ensures that data is transferred from node to node without any error.
- **Network Layer:** This layer determines the best route to transmit the data packet to its destination and this function is known as 'routing'. The Network Layer also places the IP addresses of sender and receiver on header of each frame.
- **Transport Layer:** This layer takes data from higher levels of OSI model and breaks the same into 'segments', which are then sent to lower layers of the model for data transmission.[11] It also undertakes sequencing of data so that it is received and reassembled in correct order at the destination.
- **Session Layer:** This layer is responsible for establishing, maintaining and terminating connections between networked devices[12]. It initiates a session and ensures that the session remains active while data is being transmitted. After successful transmission, this layer closes the session. It also establishes checkpoints, from where date transfer can be resumed in case of interruption during any session.
- **Presentation Layer:** This layer is responsible for ensuring how data is presented to the network. It undertakes three primary operations, namely Translation, Compression and Encryption. Translation is done to convert data in form which can be understood by differently configurated computers. Compression is done to reduce the size of data so that it can be transferred in a speedier manner. Encryption involves encoding the data to protect it from getting tampered.
- **Application Layer:** This layer works as an interface to provide network services to the end user[13]. The network applications produce data which is then transmitted over a network[14]. This layer allows network applications to access the network and display information to the user.

10 Computer Network, Available at: https://mrcet.com/downloads/digital_notes/CSE/III%20Year/COMPUTER%20NETWORKS%20NOTES.pdf.
11 Resource Material on Computer Networks, Available at: https://mrcet.com/downloads/digital_notes/CSE/III%20Year/COMPUTER%20NETWORKS%20NOTES.pdf.
12 Ibid.
13 OSI Model, Available At: https://www.javatpoint.com/osi-model.
14 Layers of OSI Model, Available at: https://www.geeksforgeeks.org/layers-of-osi-model/.

Please Note: This Model is only used for reference purposes and the current model being used on the internet is TCP/IP model.

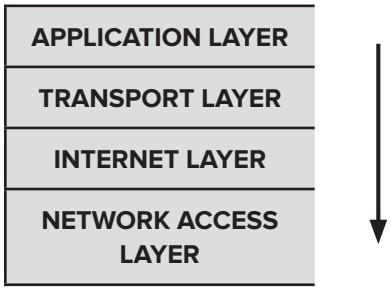


TCP/IP model (the Internet Protocol Suite)

The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a set of protocols that make up the network layer of the internet.[15] TCP/IP model is an inter-networking solution which was initially developed for communication within a limited network but later on turned out to be the standard protocol for unsecured communication over the internet.

It is interesting to note that Advanced Research Projects Administration Network, i.e., APRANET (1975) was actually the earliest version of TCP/IP model. However, in 1983, the name was changed when the model turned into an open standard that could be used on any network.[16]

The TCP/IP model consists of the following layers, where data moves from top to bottom:



The Internet Protocol Suite

i. **Application Layer:** This is the top most layer that acts as an interface through which applications and programs communicate with the user. Commonly used protocols in this layer have been discussed below:

15 Kartik Menon, The best guide to understand what is TCP/IP model, (February 26, 2023), Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model.
16 Supra, Note 18.

- **HTTP:** The Hyper Text Transfer Protocol (HTTP) is the foundation of data exchange over the World Wide Web as it makes data (be it in the form of files, images, sound clips, etc) easily accessible to the user through hyperlinks. HTTP further specifies how data requests by the user will be processed by sending it to the appropriate server, which in turn will send respond to such request[17].
- **SMTP:** Simple Mail Transfer Protocol (SMTP) is entrusted with the task of sending and receiving electronic mails[18].
- **FTP**: File Transfer Protocol (FTP) is concerned with transfer of files over a network[19].

ii. **Transport Layer:** This layer is concerned with packaging of data into smaller packets and segments so that they can be transmitted over the network. This layer also creates a communication channel between the sender and receiver device for an error-free transmission of data without any hindrance.

Some of the protocols used in transport layer are:

- **TCP:** Transmission Control Protocol (TCP) is the protocol which establishes a connection between the source and destination system and further ensures proper movement of segments over communication channel.[20]
- **UDP:** User Diagram Protocol (UDP) is mainly responsible for detection of errors during transmission of data over the network[21].

iii. **Internet Layer:** This layer is responsible for routing the data during transmission by pointing out the path which the data packets will use for transmission. This layer also helps in identification of data over the network by providing IP addresses to the system.

The protocols used in this layer are discussed below:

- **IP:** Internet Protocol (IP) is the most important protocol in internet layer, as it is responsible for sending data packets across a network from the source to destination.
- **ARP:** Address Resolution Protocol (ARP) uses the IP address to locate the physical address of the host[22].
- **IGMP:** Internet Group Management Protocol (IGMP) is used for data transmission to a group of networks[23].

iv. **Network Access/Interface Layer:** This layer is concerned with physical aspect of data transmission in raw form, i.e. binary format, through physical communication modes over a network[24]. This layer makes use of protocols like ethernet cables, fibre links and token rings.

---

17 HTTP overview, Available At: https://www.tutorialspoint.com/http/http_overview.htm.
18 Ujjwal Abhishek, TCP/IP Reference Model I Computer Networks, Available At: https://workat.tech/core-cs/tutorial/tcp-ip-reference-model-in-computer-networks-4c9jodl67ax5.
19 Ibid.
20 Kartik Menon, The best guide to understand what is TCP/IP model, (February 26, 2023), Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model.
21 Ibid.
22 Supra, Note 21.
23 Ibid.
24 Supra, Note 23.

PORTS

Ports are network points allotted to specific process or service, where connections begin and end[25]. Ports are managed by a computer's operating system[26].

Ports helps to make network connections more efficient and flawless. At any particular point of time, a computer may receive and send varied kind of data over the same network connection. In this scenario, ports help the computer to sieve through the data traffic and directs the computer what to do with the data.

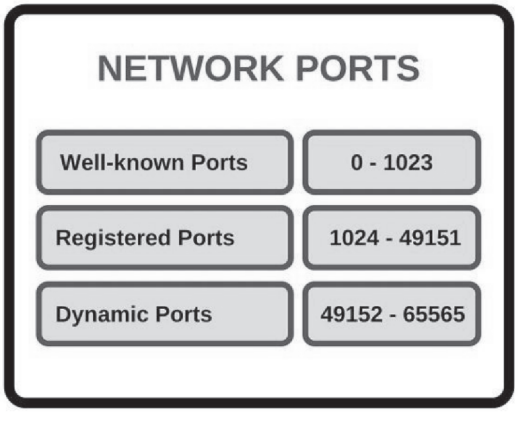
Ports can be both physical as well as virtual. Physical ports serve as connection points from where external devices can be connected to the computer. Virtual ports are connection points that allows data to freely flow between a program and the computer or over the internet[27].

In simple terms, port is an address which is assigned to every application running on a computer which utilises the internet for communication[28]. Port helps to transmit data between a computer application and computer network[29].

Every process or service (which is run by an application) is connected to a separate port. Every port has a port number which helps to identify which application is running on a device. Sometimes, this number is automatically assigned to the application running on the computer by the operating system[30].

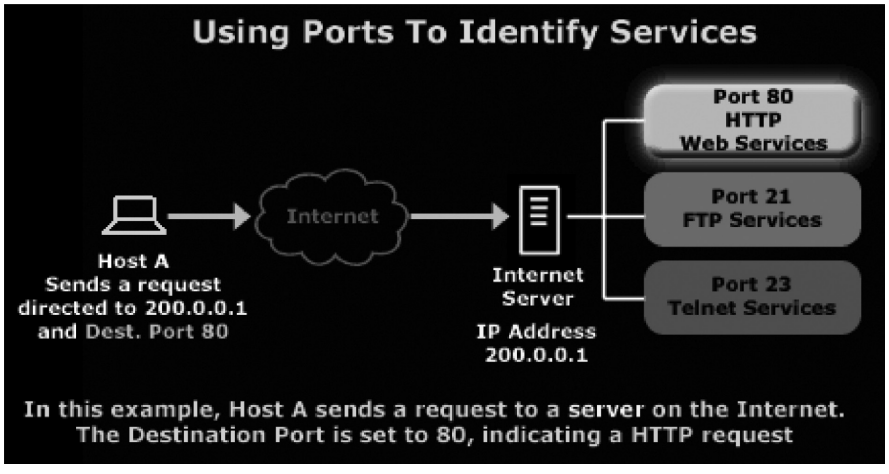
In a network, port numbers fall in the range between 0 to 65535[31]. The range of Port Numbers are as follows:

- Well known/System ports (falling in the range between 0 to 1023) are associated with common applications and services such as FTP, HTTP and SMTP[32]. For example, port number 80 is used with HTTP, whereas FTP uses port number 20 and 21.
- Registered Ports (falling in the range between 1024-49151) are assigned for specific use on application to Internet Assigned Numbers Authority[33].
- Dynamic Ports (falling in range between 49152-65565), which are also called Unassigned or Ephemeral Ports, are utilised for any type of service[34].



25 *What is a Port?, CLOUDFARE, Available at: https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/.*
26 *Ibid.*
27 *What is a Network Port?, TUTORIALS POINT, Available at: https://www.tutorialspoint.com/what-is-network-port.*
28 *What is a Port? SCALER TOPICS, Available at: https://www.scaler.com/topics/computer-network/what-is-port/.*
29 *Ibid.*
30 *Ibid.*
31 *Ibid.*
32 *Supra, Note 30.*
33 *What is a Port? SCALER TOPICS, Available at: https://www.scaler.com/topics/computer-network/what-is-port/.*
34 *Supra, Note 36.*

Ports are concerned with Transport Layer of the Internet Protocol Suite or TCP/IP model. Only protocols like the Transmission Control Protocol (TCP) or User Diagram Protocol (UDP) found in the Transport Layer are able to indicate the exact port to which a data packet is required to be sent.



SECURE PROTOCOLS

The communication protocols which are structured to transmit data between two connection points in a secure and encrypted form are called secure protocols. Such protocols aim to preserve the security, integrity and authenticity of data during communication through network channels, including the internet. Such protocols prevent unauthorized access to data in a network.

Secure Protocols usually make use of cryptography and encryption techniques to secure and encrypt data, which can only be decrypted by using special algorithm, logical key, formula or a combination of them[35]. This means if data falls into the hands of any third party, it will be unreadable and of no use, unless it is duly decrypted.

Commonly used secure protocols are Secure Sockets Layer (SSL), Secure File Transfer Protocol (SFTP) and Transport Layer Security (TLS).

SSL Protocol is designed to facilitate secure data transfer between a web browser and a web server, while guarding the confidentiality and authenticity of information. It is very popular as most web browsers support SSL protocol. It is found between the application layer and transport layer.

TLS Protocol generates a master key for encryption of data using a pseudo-random algorithm[36]. The encrypted data is then transmitted from the client to server, ensuring data protection. It encrypts communication between web browser and web server (for example- a web browser loading a website)[37].

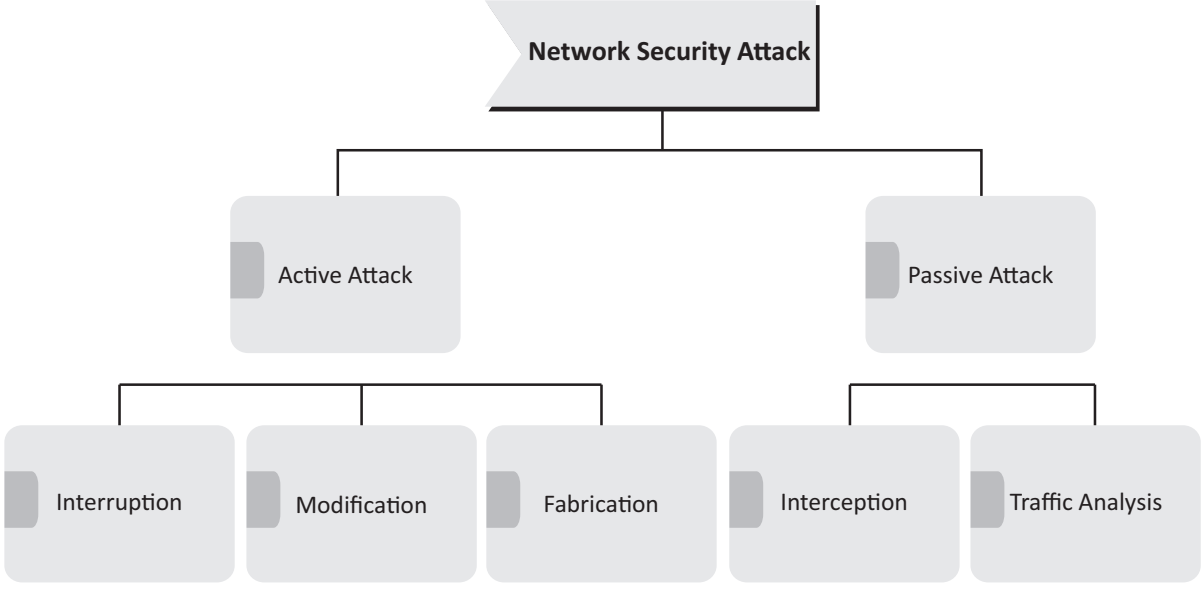
Other secure protocols are also used, apart from SSL and TLS. For example, FTPS which stands for File Transfer Protocol Secure helps in secure transmission of files over the internet.

Secure Protocols are essential to protect the safety and security of sensitive data which may be shared over the internet. Nowadays, increased number of transactions are conducted online, which involves sharing of OTPs (One-Time Passwords), debit and credit card details, UPI number, bank account details, etc. In order to safeguard such information and protect against falling prey to cybercrimes, secure protocols protect security and privacy of such sensitive data.

35 Margaret Rouse, Network Security Protocols, Available at: https://www.techopedia.com/definition/29036/network-security-protocols.
36 Types of Internet Security Protocols, GEEKS FOR GEEKS, (September 27, 2021), Available at: https://www.geeksforgeeks.org/types-of-internet-security-protocols/.
37 What is Transport Layer Security, CLOUDFLARE, Available at: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

COMMON NETWORK ATTACKS

Network security attacks can be classified under different heads as follows:



Passive Attack: It involves intrusion in the form of monitoring by an attacker, with the goal of "reading data on the network"[38]. Through this attack, an attempt is made by third party/attacker to obtain confidential information which is being transmitted. More often than not, neither the sender, nor the receiver is aware that the data security has been breached and data has been read by an attacker as such attacks do not involve any alteration of data.

Passive Attacks are of two types; Interception and Traffic Analysis. ***Interception*** involves reading of contents of any message, file, email, etc which may be sent across a network and extracting the information contained in the message. Interception may be avoided by having encryption protection in place. ***Traffic Analysis*** involves monitoring of traffic which is moving across a data network, which on careful analysis may reveal information like size, frequency and number of messages and the source and destination of such messages[39].

Active Attack: It involves active intrusion by an attacker, with the goal of "writing data onto the network"[40]. Attacker in such situations can seriously tamper with the data being transmitted across a communication network by:

a. Deleting the data sent;

38 Network Security Tutorial by APNIC, Available at: https://training.apnic.net/wp-content/uploads/sites/2/2016/12/TSEC01.pdf.
39 Available at : https://archive.mu.ac.in/myweb_test/MCA%20study%20material/M.C.A.(Sem%20-%20IV)%20Paper%20-%20III%20-%20%20Network%20Security.pdf.
40 Supra, Note 42.

b. Intercepting messages sent on the network and substituting the same with his own messages, where parties are fooled into believing that they are talking to each other when they are actually talking to the attacker (Man-in-the-middle);

c. Modification of data;

d. Playback of data from another connection[41].

Active attacks are of three types:

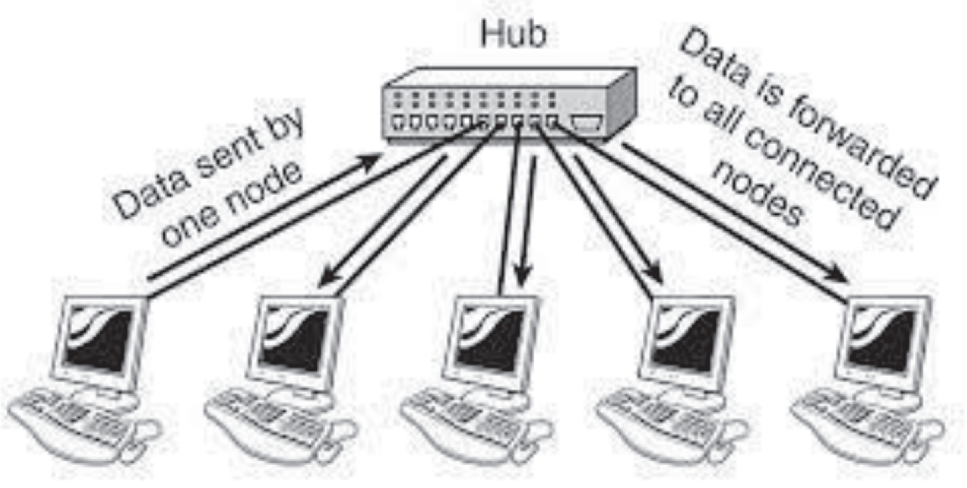
- ***Interruption:*** In this type of attack, the attacker masquerades as a different person and hamper with the communication network. For example, a hacker may impersonate himself as a Manager of a factory and send a message on his behalf to all the workers, frivolously announcing a ten-day paid holiday. Such type of security breaches will not only harm the reputation of the factory but also lead to business losses.
- ***Modification:*** In this attack, the original message is altered or modified by the attacker to produce an undesirable effect. For example, message to the effect that "Raju has been promoted" may be modified to mean "Raju has been demoted".
- ***Fabrication:*** The 'Denial of Service' attacks falls under this category, where an attacker attempts to affect the use of network facilities by seriously disrupting a network by disabling it or overloading it so as to degrade performance[42]. Timely detection is the key to prevent active attacks.

NETWORK DEVICES HUBS

Network devices are physical devices which allow communication between hardware on a computer network[43]. Examples of network devices include routers, gateways, bridge, switch, hubs, etc.

A hub refers to a networking device which is used for connection of multiple devices on a network[44]. Hubs are generally used in Local Area Networks (LAN). A hub consists of many ports, which are in turn connected to computer systems which are connected to the network.

41 Available at: https://archive.mu.ac.in/myweb_test/MCA%20study%20material/M.C.A.(Sem%20-%20IV)%20Paper%20-%20III%20-%20%20Network%20Security.pdf
42 Notes on Network Security, Available at: https://www.vssut.ac.in/lecture_notes/lecture1428550736.pdf.
43 Network Devices, February 21, 2023, Available at: https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/.
44 What are hub and switch in a computer network?, TUTORIALS POINT, Available at: https://www.tutorialspoint.com/what-are-hub-and-switch-in-computer-network.



Hubs are not able to differentiate between data packets. Therefore, any information or data which is shared with a hub through a port, is in turn transmitted to every other port connected to the hub. This means data is sent to all the connected devices on a network. A major limitation of a hub is that if data is received from two different devices at the same time, it may lead to a collision.

BRIDGES

A bridge can be defined as a device which connects smaller sub-networks in order to create a single, bigger network[45]. This function of a bridge of consolidating a single network from multiple sub-networks is called *'network bridging'*[46]. Bridges are used to create one extended LAN from multiple LANs. Bridges are found in the data link layer of the OSI model.

The following types of bridges are found in a computer network:

a. **Transparent Bridges:** Transparent bridges connect numerous network segments to other bridges in order to make routing choices[47].

b. **Translational Bridges:** When switching from one kind of networking system to another, translational links are employed. They can link various networks, including Ethernet and Token ring networks[48].

c. **Source Routing Bridges:** A source routing bridge chooses the best path between two server hosts[49].

SWITCH

A switch is a network device which is used to connect multiple computers or devices on a network. On receiving data, a switch identifies the destination from data packet and locates where exactly to send the packet. Unlike a hub, a switch sends data only to the designated nod and does not send the data to all devices on a network. A switch drops signals when it receives data which is corrupted in any manner. In such a case, a switch makes a request to the sender to resend the data packet. Switches are commonly used in homes and offices to create network connections to access the internet, smart TVs, etc.

45 Jaya Sharma, What is a Bridge in a computer network?, March 3, 2023, Available at: https://www.shiksha.com/online-courses/articles/bridge-in-computer-network/.
46 Ibid.
47 Jaya Sharma, What is a Bridge in a computer network?, March 3, 2023, Available at: https://www.shiksha.com/online-courses/articles/bridge-in-computer-network/.
48 Ibid.
49 Ibid.

Difference between a Switch and a Hub[50]:

Switch	*Hub*
Concerned with data link layer of OSI model.	Concerned with physical layer of OSI model.
Data is transmitted to only destination node.	Data is transmitted to all nodes.
Since they are associated with network software, they are 'active' devices.	Since they are not associated with any software, they are 'passive' devices.

SECURITY DEVICES

Network Security refers to the practice of safeguarding the network from any unauthorized access or external risks. The devices used by network administrators to safeguard their network are called network security devices.

Network Security devices are typically physical or virtualised hardware appliances, with vendor specific software installed. Seldom, organizations build their own network security device using custom software and commodity server hardware. For a specific type of equipment, one strategy may be more cost-effective than the other depending on your company's specific needs.[51]

With the spike in cloud computing, some devices that would be traditionally hosted on a local network, are instead provided by a third party. Businesses commonly host security applications used to protect web applications and email communications in the cloud, especially if the websites and email services themselves are cloud-hosted.

Types of Network Security Devices:

- ***Active Devices:*** Such devices block the surplus or unwanted traffic on a network. For example, firewalls, anti-virus scanning devices, content filtering devices, etc.
- ***Passive Devices:*** Such devices are concerned with identification and reporting of intrusion on a network. For example, intrusion detection devices.
- ***Preventive Devices:*** Such devices prevent potential security attacks by scanning, detecting and identifying breaches of security on a network.
- ***Unified Threat Management:*** These devices provide one-stop security solutions for all network problems. For example: Firewalls, web caching, etc.

Authentication Applications: These applications authenticate the identity of the sender of data to ensure that the communication has been sent by the intended sender and not an imposter/hacker, before providing access to a network. Data may be authenticated in the following manner:

- ***Peer Entity Authentication:*** It assures and reaffirms the identity of the entity involved in the communication.
- ***Data Origin Authentication:*** It verifies whether the source disclosed by the sender is the same as the actual source of data.

50 What are hub and switch in a computer network?, TUTORIALS POINT, Available at: https://www.tutorialspoint.com/what-are-hub-and-switch-in-computer-network.
51 Available at: https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/.

- ***Access Control:*** It prevents unauthorized use of data by controlling the access to the data by specifying under what conditions the data may be accessed, who may access the data, etc.
- ***Data Confidentiality:*** It assures that the privacy of the data has been protected against unauthorized access.
- ***Data Integrity:*** It assures that the data has not been tampered or compromised and its original form has not been altered.

Other security mechanisms:

- ***Encipherment:*** This technique is employed to hide the data in order to protect its authenticity and confidentiality. Data may be enciphered by both cryptography as well as encipherment.
- ***Digital Signature:*** Under this mechanism, the sender put his digital signature on the data which is then verified by the receiver. A digital signature authenticates that the data has originated from the sender.
- ***Traffic Padding:*** This mechanism inserts extra bits into the data stream which is being transmitted, so that any attempt to analyse the traffic is frustrated[52].
- ***Network Access Control:*** This technique controls the level of access granted to a network by placing password protections, firewalls, etc.
- ***Notarization:*** This mechanism involves the use of a trusted third party in the process of data exchange.

FIREWALL

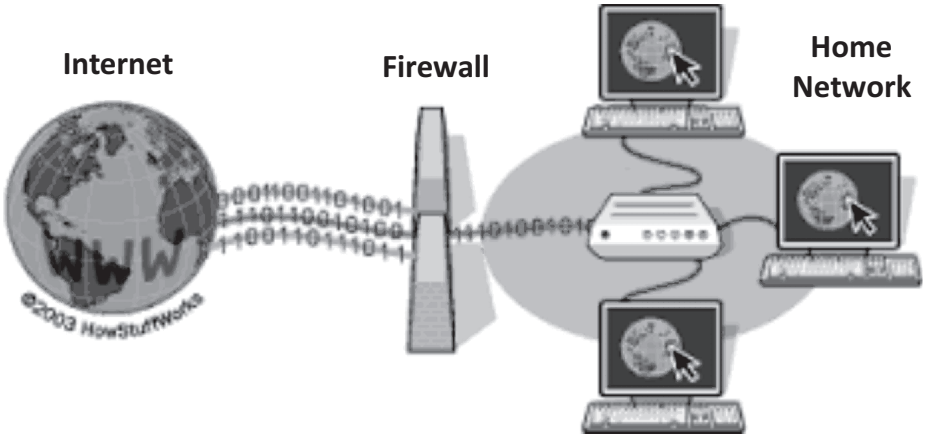
A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. Appositely, it is a barrier that stands between a private internal network and the open Internet at its most basic level. Firewalls exclude unwanted and undesirable network traffic from entering the organization's systems. Depending on the organization's firewall policy, the firewall may completely disallow some traffic or all traffic, or it may perform a verification on some or all of the traffic.[53]

Primarily, it is an essential component of any security design since it gives your network security device control over host level defences, eliminating the need for guesswork. With the help of an integrated intrusion prevention system (IPS), firewalls, and especially Next Generation Firewalls, concentrate on thwarting malware and application-layer attacks. These Next Generation Firewalls can react swiftly and seamlessly to detect and respond to external attacks across the entire network. They can implement policies to better protect your network and do speedy analyses to find intrusive or dubious activities, like malware, and stop it.

Firewalls can carry out fast assessments to detect intrusive or suspect behaviour, such as malware, and can be configured to act on previously specified policies to further safeguard a network. Network can be configured with precise policies to allow or prohibit incoming and outgoing traffic by using a firewall as security infrastructure.

52 Types of Security Mechanism, (September 10, 2020), GEEKS FOR GEEKS, Available at: https://www.geeksforgeeks.org/types-of-security-mechanism/.

53 Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.



The various types of Firewalls have been enlisted below:

- ***Packet Filtering***: A small amount of data is analysed and distributed according to the filter's standards.
- ***Proxy Service***: Network security system that protects while filtering messages at the application layer.
- ***Stateful Inspection****:* Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- ***Next Generation Firewall***: Deep packet inspection Firewall with application-level inspection.

LESSON ROUND-UP

- A network can be defined as a group of two or more computers or electronic devices which are connected together for the efficient exchange of information and resources.
- Computer networks are typically categorised as LAN (Local Area Network), MAN (Metro Area Network), and WAN (Wide Area Network) based on the geographic region covered and data transfer rate.
- Each device in a communication network that can receive, generate, store, or send data to network routes is referred to as a node.
- Network Security refers to the level of protective measures undertaken to secure data during transmission.
- Network security protects data to ensure its confidentiality, integrity and privacy.
- The unique number which identifies a computer or device or network on the internet is called Internet Protocol (IP) Address.
- Port is an address which is assigned to every application running on a computer which utilises the internet for communication.
- Secure Protocols usually make use of cryptography and encryption techniques to secure and encrypt data.
- Passive Attacks and Active Attacks are the common network attacks.
- The devices used by network administrators to safeguard their network are called network security devices. For example, Unified Threat Management, Encipherment, Digital Signature, etc.

GLOSSARY

Network: A network can be defined as a group of two or more computers or electronic devices which are connected together for the efficient exchange of information and resources.

Wired Network: It refers to a network where devices are connected through cables to switches, which are in turn connected to network router for accessing the internet.

Wireless Network: It refers to a network where devices are connected through radio waves to an access point, which is in turn connected to a router, for accessing the external network.

Security: In simple words, it refers to the state of being safe or free from danger. However, in terms of computer science, security refers to the level to which a program or device is safe from unauthorized use.

Computer Security: It refers to protection of computer systems through tools, measures and techniques, in order to protect data and evade hackers, data theft or unauthorized use.

Network Security: It refers to the level of protective measures undertaken to secure data during transmission.

Internet Security: It refers to the level of protective measures undertaken to secure activities conducted over the internet.

Network Protocol: Protocols enables transmission of data between various devices on the same network and allows internal devises on a network to communicate irrespective of differences in their internal configuration, structure or design.

IP Address: The unique number which identifies a computer or device or network on the internet is called Internet Protocol (IP) Address. When a computer connects to the internet through internet service provider (ISP), this IP address enables the identification and location of the computer device. IP address may affect the kind of information that you may receive over the internet.

Nodes and Hosts: A node is a term which is used to refer to any computer or device which is connected to a network. A host refers to any device having an IP address which requests or provides networking resources to other hosts or nodes connected to a network.

Protocols: Protocols enables transmission of data between various devices on the same network and allows internal devises on a network to communicate irrespective of differences in their internal configuration, structure or design.

Suppose, a computer which uses IP Protocol may not be able to communicate with a computer which does not use the same protocol. This is where standardized protocols help to establish communication by serving as a common language for computers.

Data Packets: Data which is transmitted through the internet is organised into smaller chunks, called data packets. The Computer/device is able to understand the final output of data sent via data packets, with help of protocols.

Domain Name: A domain name refers to the address of a website which a user types into the web browser. Domain name allows a user to connect to the server that hosts a website's data and services, in the absence of an IP address.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What is meant by network security? What are the goals of network security?
2. What is the difference between intranet and extranet?
3. Discuss the different types of active attacks.
4. Explain the Internet Suite Protocol.
5. Differentiate between a hub and a switch.
6. Write short notes on: (a) Firewalls, (b) Security Devices, (c) Internet and (d) Protocols.
7. What is the use of a bridge in a network connection?
8. Explain different types of network security devices.

LIST OF FURTHER READINGS

- Network Security Tutorial by APNIC, Available at: https://training.apnic.net/wpcontent/uploads/sites/2/2016/12/TSEC01.pdf
- William Stallings, "Cryptography and Network Security- Principles and Practice", Seventh Edition, Pearson, Delhi
- Cryptography and Network Security – by Atul Kahate – TMH
- Data Communications and Networking- by Behourz A Forouzan
- Cyber Security Operations Handbook – by J.W. Rittiaghouse and William M.Hancok – Elseviers.

Softwares and Software Security

Lesson 9

KEY CONCEPTS

■ Defects ■ Bugs ■ Failure ■ Flaws ■ Vulnerabilities ■ Software ■ System Software ■ Application Software ■ Utility Software ■ Software Security

Learning Objectives

To understand:

- The concept of software
- The Differentiate between different types of software
- And appreciate the concept and need of software security
- The software security mechanisms
- And learn how software security is perceived by the courts through various case laws
- Appreciate the legal and statutory compliances regarding software security.
- The get familiar with recent trends in software security
- The best practices of software security

Lesson Outline

- Introduction
- Software-Overview
- Characteristics of good software
- Software Classification
- Other types of software on the basis of availability and shareability
- Software Security
- Software security a proactive security
- Software security best practices
- What to Avoid in Software Security
- Software Security: Overview and Significance
- Case Study and Case Laws
- Analysis of Indian Law on Software Security
- SaaS; PaaS, IaaS and On Premise Software: Overview and Recent Trends
- Legal and Compliance Requirements of Software Security
- Lesson Round-Up
- Glossary
- Test Yourself
- List of Further Readings

INTRODUCTION

Security concerns in terms of software has become a pertinent issue in recent times and rightly so, because a weak software or complete lack of software can be a potential breeding ground for common security issues and malicious attacks.

In today's tech savvy world, software security cannot be ignored as we regularly interact with a multitude of software in our everyday life, right from home to office. Any kind of external intervention in software systems can seriously threaten the security of data and make it prone to unauthorized access. Therefore, it is important to take timely decisions for software security at all levels. An organization has to make decisions regarding investment in appropriate software security solutions to ensure company software systems are adequately protected. Software developers must design and develop security software mechanisms to safeguard against malware and other attacks. Individuals must regularly check and update their software security mechanisms to identify and guard against possible breaches.

In this chapter, we will understand about software, potential threats to software security and solutions to software security.

SOFTWARE-OVERVIEW

A computer system is composed of hardware and software components. Hardware is the external physical components of the computer which can be touched by users. Examples of hardware include desktop, printer, mouse, etc. On the other hand, software refers to set of instructions which enable the hardware components to perform[1]. Examples include Windows, Linux, MS Word, PowerPoint, MS Excel, etc. Software, thus, can be referred to as a "set of instructions" which direct the hardware to do a particular task and specifies the manner in which the said task must be accomplished[2].

The concept of software rests on the basic principle of:

The input fed into the computer through the hardware device is programmed by the software to produce the desired result or output.

The difference between software and hardware has been discussed in detail below:

Hardware	***Software***
It is the physical parts of the computer which process the data1.	It is the collection of instructions which directs the computer as to 'which' task to perform and 'how' to perform it.
Hardware is unable to perform any task without the support of software.	Software can only be run and executed in computer hardware.
It understands only machine-level language.	It accepts inputs by users, converts it into machine-level language which is then sent to Hardware for processing.
It can be seen, felt and touched.	It can only be seen and cannot be touched.
Examples: Monitor, Hard disk, CPU, Keyboard, Printer, Mouse, etc.	Examples: Windows, Linux, MS PowerPoint, MS Excel, etc.

1. Difference between Hardware and Software, BYJU'S, Available at: https://byjus.com/free-ias-prep/difference-between-hardware-and-software/#:~:text=A%20computer%20system%20is%20divided,a%20specific%20set%20of%20tasks.

2. Study material on Computing Basics, Available at: https://ftms.edu.my/v2/wp-content/uploads/2019/02/csca0101_ch07.pdf.

CHARACTERISTICS OF GOOD SOFTWARE

The desirable characteristics of a good software have been outlined below:

a) ***Security:*** A good software must have adequate security measures in place to safeguard against attacks.

b) ***Functionality:*** A software must be able to perform its intended function and fulfil the purpose for which it was designed[3].

c) ***Reliability:*** A software must be able to operate, without failure, over a specified period of time, under certain conditions.

d) ***Versatility:*** It refers to quality of the software of being able to perform as per the requirements of the user in varied conditions and environments.

e) ***Stability:*** A software must be stable enough to withstand changes made in its design and

f) ***Modifiability:*** A software must be capable of accepting modifications in its structure and design, necessitated by needs which may arise in due course.

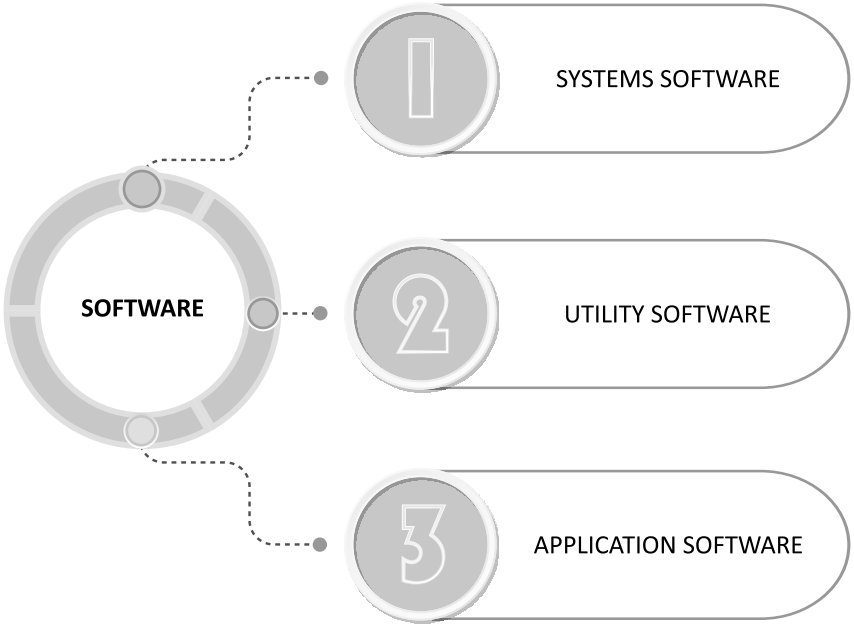
g) ***User-Friendliness:*** A software must be easy to understand and use.

h) ***Portability:*** It refers to the ease with which software can be ported from one platform to another without (or with minimal) changes, while obtaining similar results.

i) ***Maintainability:*** Software must be able to withstand changes made its code, so that the software can be altered or modified or new changes/features can be introduced as per requirements.

SOFTWARE CLASSIFICATION

Software can be classified into the following types:

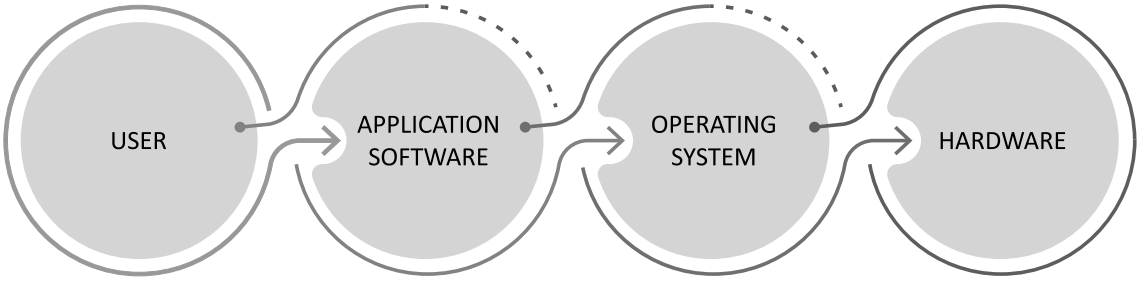


3. "Software Engineering", GEEKS FOR GEEKS, Available at: https://www.geeksforgeeks.org/software-engineering-characteristics-of-good-software/.

Systems Software: These software enables interaction of the user with hardware components of the computer and helps in running programs on the computer. System software serves as a point of interaction between the hardware components of computer and user applications. It is relevant to note that computer hardware only understands machine language (that runs into binary digits of 0s and 1s) whereas application function in human-readable language (for example: English). Therefore, a system software converts machine language to human readable language and vice versa to facilitate smooth functioning of the computer.

Types of system software

1. **Operating System:** It refers to the amalgamation of hardware configuration of a computer with a certain software package[4]. For example, Windows, DOS, MAC, Linux. Operating system is basic and essential to the functioning of a computer as all computer applications sit inside the operating system of a computer. The basic functions of storing data, retrieving files and scheduling of tasks are also managed by the operating system[5]. The software which is loaded just when the computer is turned on is the Operating System and this process is known as 'booting'.



Functions of an Operating System:

i. ***Performing Hardware Functions***: the operating system performs the important task of converting the simple instructions given by the user through application program into a set of elaborate and detailed instructions which are required by the hardware devices. It also informs the user about any error or malfunction which has occurred or if any of the input/output devices need attention[6].

ii. ***Interface***: The operating system provides an interface for the user to insert instructions and command the computer. Graphical User Interface, as the name suggests, provides graphics (in the forms of icons and menus on the screen) which are used by users to command the computer[7]. For example, Windows by Microsoft.

iii. ***File Management*:** Files are managed by the Operating System so that it can be made available to the CPU as and when required[8]. Operating System also ensures that the files are protected and kept secure from unauthorized access.

iv. ***Management of Processing Tasks*:** Operating System enables the user to run multiple programs at the same time or allow multi users to use the computer at the same time. This is made possible through the task processing feature of operating systems.

v. ***Memory Management*:** Operating systems manage the memory and storage of the computer so that data can be stored, retrieved and supplied to the application program so that instructions can be effectively executed.

4. Software Engineering, Available at: https://www.skylineuniversity.ac.ae/pdf/software-engineering/Software.pdf.

5. Basics of Computer Software, Available at: https://www.tutorialspoint.com/basics_of_computers/basics_of_computers_software_concepts.htm.

6. Study Material on Computer Software, Available at: https://egyankosh.ac.in/bitstream/123456789/7375/1/Unit-3.pdf.

7. Ibid.

8. Study Material on Computer Software, Available at: https://egyankosh.ac.in/bitstream/123456789/7375/1/Unit-3.pdf.

2. **Language Processor:** It performs the task of conversion of human readable language into machine language and vice versa[9]. The interactions between users and computer takes place in three languages namely:

   - **Machine Language:** This language consists of binary digits of O's and 1's, which is only understood by a machine. It can be called as a 'machine-friendly' language.
   - **Assembly Language:** This is the Low-Level Language (LLL) which uses "Mnemonics" or words and symbols in English language to represent long strings of binary digits (0's and 1's)[10]. For example: the mnemonic "READ" means that data has to be retrieved from the memory[11]. This language is dependent upon machines and varies according to the processor used[12].
   - **High Level Language:** This language consists of statements in English, which is readable and understandable to humans[13]. It can be called 'programmer friendly' language. For example: JAVA, C++, etc.

   Since the machine level language cannot be comprehended by users, HLL is commonly used for coding. The codes so developed (i.e. source codes) have to again be converted into machine language (i.e. machine/ object code) so that it can be understood by the computer to produce the desired output. This conversion is primarily the function of Language Processor.

   A language processor is typically made of three essential components:

   - ***Assembler:*** This component of language processor converts assembly language into high level language.
   - ***Compiler:*** This component of language processor converts high level language into machine language in one go.
   - ***Interpreter:*** This component of language processor is employed in line by line conversion of high-level language into machine language. The execution time of this processor is slow.

   The difference between Compiler and Interpreter has been outlined below:

COMPILER	***INTERPRETER***
It is concerned with simultaneous conversion of High Level Language into Machine Language, all at once.	It is concerned with line by line conversion of High Level Language into Machine Language.
Errors are reported after compilation.	Errors are reported line by line, as and when they occur.
Faster in comparison to an interpreter.	It is comparatively slower than a compiler.
It first scans the entire source code which is then converted to object/machine code, in one go.	It scans the source code line by line and converts one statement at a time.

9. Software and its Types, GEEKS FOR GEEKS, Available at: https://www.geeksforgeeks.org/software-and-its-types/.

10. Supra, Note 8.

11. Ibid.

12. Study Material on Types of Software, Available at: https://stlawrencehighschool.edu.in/uploads/onlineclass/364aecdbfc1a21ddc39606d5692ec3cf.pdf.

13. Ibid.

3. ***Device Driver:*** This software acts an interface between the user and the input-output devices of a computer[14].
4. ***BIOS:*** Basic Input Output System is responsible for controlling the input output devices of a computer. BIOS also initiates the booting process of a computer.

Application Software

These are software which are dedicated to the performance of a particular task or function.

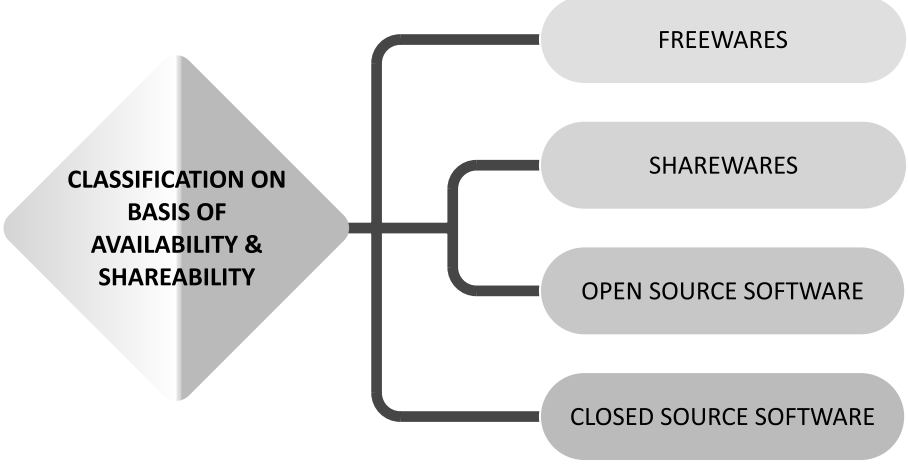
Application software are of the following two types:

- ***General Purpose Application Software:*** These are "ready to use" software, made for common use. For example, VLC Media Player is used to play audios and videos, MS PowerPoint is used to create presentations, etc.
- ***Specific Purpose Application Software:*** These types of software are customised for businesses or organisation. For example, a library may have a software that keeps a track of all the books, ticket reservation software, software used for management and allocation of rooms in a hotel, etc.

Utility Software

A utility software is a type of application which assists the system software in performing its work[15]. This software performs basic tasks, which are required daily. A computer may function without a utility software; however, it is found in most computers as it enhances the performance and output of a computer system. Examples of such software can be an anti-virus software which guards the computer against virus and malware attacks, Text Editors like Notepad which allows users to create text documents, Disk Defragmenter Tools which rearranges the files in proper order in a disk, etc.[16].

OTHER TYPES OF SOFTWARE ON THE BASIS OF AVAILABILITY AND SHAREABILITY



- **Freeware:** As the name suggests, freeware software are those which can be downloaded from the internet and used by the users free of cost. These are standardized software which cannot be tailored to suit individual needs. For example, Google Chrome, Mozilla Firefox, WPS, etc.

---

14. Study Material on Types of Software, Available at: https://stlawrencehighschool.edu.in/uploads/onlineclass/364aecdbfc1a21ddc39606d5692ec3cf.pdf.

15. Basics of Computer Software, TUTORIALSPOINT, Available at: https://www.tutorialspoint.com/basics_of_computers/basics_of_computers_software_concepts.htm#.

16. Supra, Note 14.

- **Sharewares:** These are made available to the users with a free trial for a limited time period during which the users can use the software and decide whether they want to purchase the software or not. Here, users are asked to pay in case they wish to use the software beyond the free trial period.
- **Open Source Software:** The peculiar feature of this software is that the source course is made available to the users along with the software and this source code can be modified by the users to suit their individual needs. This software is available for free or for charge on the internet. For example, Apache Web Server. Open Source Software offer varied benefits to the user like cost savings, customization and security.
- **Closed Source Software:** This type of software can be purchased by the users. However, the source code of such software is protected by intellectual property laws. Most of the commonly used software belong to this category. For example, Mac OS, Win RAR, etc.

SOFTWARE SECURITY

Software Security refers to the practice of developing and engineering the software in a manner which keeps it secure from external malicious attacks, while also ensuring that in case of any such attack, the software does not malfunction and continues to operate. It is essentially a preventive technique to manage and avoid security risks.

Since computers are heavily reliant upon software for their smooth functioning, it becomes important to secure software and protect them from undesirable viruses and attacks. Software attacks are increasingly common in mobile applications. Software developers need to be extra cautious while designing and developing a software as any loophole in the software can be exploited by hackers. The Developer should be aware about any possible vulnerability which may arise in respect of a particular software so that the source code can be written in a manner which guards against such a vulnerability.

Software Security: Overview and Significance

Systems are usually complex in nature and systems run by software are not only complex but also involve multiple risks. One such risk is that of protecting such complex systems as it is difficult to understand it, analyse and evaluate it to decide appropriate protection strategy. The complexity results in a situation where security risks are often identified at stages when most damage has already been done. Even simple systems might pose a challenge to secure when there are inherent flaws in the software design.

Hidden risks can affect any computing system. The software that is initially loaded on the device can be altered by malicious programmers[17].

Users may install a programme wrongly, introducing uninvited risk, or, worse, transmit a virus by installing new programmes or software updates. In a multiuser system, a malicious user may install a Trojan horse to steal the passwords of other users[18].

The significance of software security lies in the increased inter-connectivity of computers, mobiles and other electronic devices through the internet, which enables dissemination of information on the click of a button. Furthermore, people, organisations, and governments are becoming increasingly reliant on network-enabled communication tools like e-mail and websites offered by information systems. Unfortunately, because these systems are connected to the Internet, they are vulnerable to remote attacks. This interconnectivity not only increases possible areas of attacks but also enables attackers located in one corner of the world to target systems located in another part of the world. Resultantly, this means that an attacker does not need physical access to a system to trigger security issues.

17. Introduction to Software Security, Available at: https://img2.helpnetsecurity.com/dl/reviews/viegach1.pdf.

18. Supra, Note 20.

Software security also depends upon the degree of extensibility of systems. Systems are made "extensible" through updates/extensions which are made to improve the capabilities and functionality of the software, without re-writing the entire code. These updates must be designed with security of the software in mind.

These trends of extensive networking, increasing system complexity, and built-in extensibility, when combined, make software security more critical than ever[19].

SOFTWARE SECURITY: A PROACTIVE SECURITY

In the past, security issues in terms of systems, software, internet, etc. were only paid attention to when any breach or untoward attack came to light. However, one malicious attack has the potential to seriously disrupt any organization by leaking its data, hacking into its systems, accessing customer information, new product designs, etc., leading to loss of revenue, reputation and business of the organization. These kind of security solutions (which were conventionally used in the past) where actions are taken to remedy the breach only after the breach has occurred or damage has taken place, are called reactive security practices or solutions. The major task of reactive security is to identify the attacker, hacker or intruder, after discovery of breach.

Even though reactive security is not the suggested mode of security solution, it still has certain benefits which have been enumerated below:

- It scans and monitors any anomaly (for example, unusual traffic, authentication failures, etc.) through intrusion detection systems[20].
- It provides prompt incident response where every data breach incident is inquired and investigated to find out the root problem, which is then cured.
- Anti-malware and anti-spam applications are examples of reactive security. On detection of any spam or malware on computer, these applications immediately take steps to remove it.

Software security, on the other hand, is a type of proactive security. It is based on the principle "prevention is better than cure". Proactive security aims to prevent any data breach incident before any malware is able to access network server or before vulnerabilities in a software are exploited by hackers[21]. Proactive security typically necessitates additional software and hardware designed for spotting threats before they turn into serious incidents[22]. Giving administrators information on vulnerabilities so they may take the required steps to promptly fix them is another part of proactive security[23].

Some benefits of proactive security have been outlined below:

- It helps an organisation to save money and maintain its brand value by preventing attacks before they occur.
- It prevents breach of sensitive data and malicious attacks.
- It enables early identification of vulnerabilities before they are discovered by potential attackers.
- It enables organisations to stay complaint by constantly monitoring the data.
- It prevents potential crises and reduces the stress of facing any malicious attack so that management and employees can focus on growth and expansion.

19. Ibid.

20. Proactive v. Reactive Security, IMUNIFY SECURITY, Available at: https://blog.imunify360.com/proactive-vs.-reactive-security-5-tips-for-proactive-cyber-security.

21. Ibid.

22. Ibid.

23. Ibid.

Software Security Goals

Software security seeks to achieve the following goals:

- **Prevention of malicious attacks:** The main goal of software security is to prevent attacks in this age of Internet, where data breach spreads like wildfire.
- **Timely threat detection:** It aims to detect and prevent possible breach of security in time.
- **Effective Monitoring:** Real time monitoring is an effective tool to avoid attacks before they happen and prevent damage.
- **Privacy and Confidentiality**: Developers must address this issue effectively as software run on machine which has the ability to track or access information stored on the software. Therefore, a machine may be able to access information which the software may attempt to hide.
- **Anonymity:** This is an important concern which requires the developers to consider what may happen to any data which is collected by a program and whether the same has been adequately protected.
- **Authentication:** Most software require user to log into the system through Login ID and Password. It is essential for security as it is relevant to understand who can be trusted and who cannot be trusted[24].
- **Integrity:** Software should enable maintenance of integrity of data, i.e. the ability to remain the same, to ensure that data is not manipulated during transmission from sender to receiver.

SOFTWARE SECURITY: BEST PRACTICES

1. **Verification of Software:** Software Verification is the process of verifying whether a code corresponds to particular specifications. The security limitations are encoded and given as configuration to the verification process[25]. The process of verification ensures that a particular software conforms to the specifications, which in turn guarantees that security violations will not take place[26]. For example, CompCert is a formally verified compiler which ensures that conversions are always correct and no bug is introduced during compilation[27].
2. **Language Based Security:** A new area of research has emerged in the form of language-based security where security properties are implemented in the programming language[28]. This practice encourages development of programming languages in security specific manner and prevents the programmers from making mistakes[29]. For example, type safety and memory safety are enforced and implemented as part of programming language by Java (a widely used programming language).
3. **Software Testing:** It is the practice of finding flaws or possible vulnerabilities in software while executing a program[30]. However, it is important to note that security requirements cannot be tested easily as software testing only reveals and detects if the program is infused with bugs, but it cannot confirm absence of bugs[31].
4. **Training:** All users, be it employees, students, businessmen, should be trained to use the software in a proper manner and must be cautioned and informed about security risks and how to identify, avoid

24. Study Material, Available at: https://img2.helpnetsecurity.com/dl/reviews/viegach1.pdf.

25. Mathias Payer, "Software Security: Principles, Policies and Protection", July 2021, Available At: https://nebelwelt.net/SS3P/softsec.pdf.

26. Ibid.

27. Supra, Note 28.

28. Mathias Payer, "Software Security: Principles, Policies and Protection", July 2021, Available At: https://nebelwelt.net/SS3P/softsec.pdf.

29. Ibid.

30. Ibid.

31. Ibid.

and prevent them. Users must also be trained about remedial measures that must be taken as soon as a breach is detected.

5. **Data Encryption:** Data encryption converts data into an unreadable format which can only be deciphered with the help of a security key. It is a proven security technique which is widely used to protect against data breach.
6. **Patching Software:** It is always recommended to resolve and fix system vulnerabilities as and when they are detected. This is known as 'patching the software'.
7. **Use of Firewall:** Firewall act as a protective layer and barrier between the internal computer network and the internet. It allows or prohibits traffic from the internet as per the pre-established security rules and policies. Use of firewalls is thus recommended as a good security practice.
8. **Two factor authentication:** It is a security practice which allows access to a software or program only on providing credentials like login ID and password. Only a user who knows the login ID and password would be able to access the account.
9. **Penetration Testing:** This security practice involves hiring a testing team which attempts to penetrate into the system by using the same tools and in the same manner that a hacker would do, to identify and flag security issues in the software. It is recommended that penetration testing should be done periodically. Benefit of this practice is that existing issues or vulnerabilities in the software are quickly identified and resolved before they are discovered by hackers.
10. **Remain agile and proactive:** It is recommended that one must always be aware of current and emerging security trends and new security issues and constantly evolve and adapt to new, updated and emerging security practices, only after checking its viability.

Therefore, it can be concluded that software security is a continuous process which starts right at the design and developing stage and continues throughout as software is regularly patched and updated to resolve security issues.

WHAT TO AVOID IN SOFTWARE SECURITY?

Never misplace trust.

- Avoid storing sensitive client information except where it is necessary. If sensitive information has been stored, it must be ensured that it has been adequately protected at all levels, and cannot be compromised.
- Incoming data from untrusted sources should always be scrutinized and tested before allowing access to the system.
- Avoid sharing of passwords and resources like MAC address, etc.

Allow authorisation after authentication.

- Users should be allowed to access the system and perform tasks only after their identity has been verified and duly authenticated.
- Process of authentication may involve confirming identity of user through use of password or establishing identity through finger print, facial recognition sensors.
- Authorization may be granted to access the system, and depends on nature of request, time and location of request, etc.

- Sensitive transactions or high value transactions may be conducted only after double verification or by using higher level of authentication techniques.

Never mingle data and control functions.

- Lack of proper bifurcation and separation of data and control instructions can result in memory specific vulnerabilities.

Keep in mind the Users.

- Software must be developed keeping in mind the ultimate users and how they will operate the software. Keeping the background, biases, preferences of users in mind, security features must be built-in within the software.
- Moreover, security configurations must be easy to use and set up, so that users can make use of the same.
- Do not consider security as a feature, rather, built a foundation of the software on basis of security.

CASE STUDY AND CASE LAWS OF INDIAN LAW ON SOFTWARE SECURITY

CASE STUDY: MOBILE SECURITY

Smart phones, tablets, smart-watches, etc have become an indispensable part of our everyday lives. These devices run on mobile operating systems, which serves as a user interface and allows the user to download and run applications from the internet. Android is one such example of a mobile operating system which is widely used all over the world. One major issue for android is to accommodate devices made with different configurations, by different companies on one standard operating system framework.

Android is based on modified version of Linux kernel[32] Under android based system, applications are kept separate from each other and each application (be it downloaded from the internet or pre-installed) has its own individual user account, having its own login credentials. This means that multiple applications do not use the same user id. The interaction between the apps is minimised through an Application Programming Interface[33].

The applications used on smart phones and tablets can be downloaded from a central marketplace of apps like Google Play Store. Developers upload their apps on such marketplaces. Every developer has to pay a certain amount of entry fees to upload their apps to the marketplace. Moreover, automatic updates are instantly provided to existing users, who have already installed the application on their mobile phones and tablets.

Once downloaded, there are certain in-built security restrictions on the app. In order to function properly, every application would require some sort of permission access. For example, through Instagram, users upload their pictures and stories on social media. Therefore, in order for Instagram to properly function, it would require access to the phone's photos and photo gallery. Once this permission access is granted, applications perform their designated tasks. It must be noted that how much access and what areas of access to mobile device is provided to the application is in the hands of the user; who may decide to give or withhold such permission. In this manner, the ultimate security decisions lie in the hands of the user. However, to what extent the users are able to take informed decisions, depends upon the level of awareness and cautiousness exercised by them.

32. Android (Operating System), WIKIPEDIA, Available at: https://en.wikipedia.org/wiki/Android_(operating_system).

33. Mathias Payer, "Software Security: Principles, Policies and Protection", July 2021, Available At: https://nebelwelt.net/SS3P/softsec.pdf.

CASE STUDY: PUNE CITIBANK MPHASIS CALL CENTRE FRAUD (2005)

These were instances of source engineering in the United States of America. In 2005, $350,000 was illegally moved from four Citibank clients' bank accounts through the internet. By reassuring certain clients that they would find it simple to help them in difficult circumstances while they were far from the bank's branch, the bank personnel were able to gain their trust. The money was allegedly moved from the client's account with the bank to a phoney bank account in Pune, according to witnesses. There was no decoding of the encrypted software or breaking of firewalls; only the Mphasis system's weaknesses were found. The defendants in this case were former workers of the Mphasis call centre. Every time an employee entered or exited, they were scrutinized, and it was discovered that the employees were unable to write down the numbers and had to commit it to memory as this was the only option. Subsequently, money was transferred from a cybercafé.

The defendant was found guilty of utilizing unauthorized access to clients for criminal purposes, according to the court's observation. The defendant was found guilty of the crime by the court, and they were punished in accordance with sections 43(a) and 66 of the Information Technology Act as well as sections 420, 465.467, and 471 of the Indian Penal Code.

CASE LAWS ON SOFTWARE SECURITY

Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr. [Andhra High Court, reported as 2005 CriLJ 4314]

The present case concerned quashing of FIR registered against the Petitioners (who were staff members of TATA Indicom) under Sections 409, 420, 120B of the Indian Penal Code, 1860, Section 65 of the Information Technology Act, 2000 and Section 63 of the Copyright Act, 1957. In this case, a complaint was filed by Sales and Marketing Department of M/s Reliance Infocom Ltd. Hyderabad, who were offering Reliance India Mobile (RIM) services to telecom subscribers. Under the RIM scheme, a subscriber would get a mobile handset worth Rs. 10, 500/- along with service bundle for a period of three years. However, the handset offered was locked technologically, which meant that only Reliance services could be availed on the handset. One major drawback was that if a customer wanted to opt out of the service, it had to pay the original price of the handset along with others service charges.

The subscribers, after availing the said scheme, were not happy and were lured by better tariff plans offered by other telecom service providers, which also offered an option to switch the service provider. This scheme had a great influence on the market as the handset offered was a 3rd generation digital device and therefore, this scheme quickly garnered good market share. Resultantly, the other service providers in the market resorted to illegal tactics to divert and manipulate the customers. Employees of TATA Indicom started making calls to Reliance's customers, made a deal, where Reliance headsets were reprogrammed (by hacking the ESN i.e. Equipment Special Number) so that other service provider services could be used on it.

The Andhra High Court held that the definition of computer under S. 2(1)(i) of the Information Technology Act, 2000 includes within its ambit a mobile handset. The High Court while refusing to quash the offence under under Section 65 of the Information Technology Act, 2000, held that reprograming the handset by alteration of ESN by service providers like TATA Indicom, is an offence under the said section.

***Shreya Singhal* v. *Union of India* (AIR 2015 SC 1523)**

This case touched upon the subject of free expression on the internet and censorship and is often regarded as a milestone decision in the jurisprudence of information technology. This matter concerned two girls who were detained by police for posting remarks on Facebook criticizing the closure of Mumbai city following the death of a political leader. The matter was taken before the Supreme Court of India in 2013.

Any online communication that may be "offensive" or "menacing" was considered illegal under S. 66A of the Information Technology Act, 2000. The Supreme Court declared S.66A to be unconstitutional as it was ambiguous, overbroad, and unclear, thus infringing the fundamental right of free speech and expression guaranteed under Art. 19(1)(a) of the Constitution.

The case has received widespread praise as a victory for those who support free expression and has established a significant precedent for laws on free speech on the internet in India.

Avnish Bajaj v. State (NCT) of Delhi, (2008) 150 DLT 769

In the abovementioned case, the question of intermediaries' responsibility for user-generated content on their platforms was addressed. The conflict arose when the CEO of Baazee.com (now eBay India), an online marketplace, was detained for posting a listing of an offensive video.

According to the Information Technology Act of 2000, the court determined that Baazee.com was an intermediary and was not responsible for any information supplied by a user, provided that the intermediary was unaware of the content's illegality.

The court emphasized that while intermediaries are not obligated to actively track every piece of information posted on their platforms, they have a duty to promptly remove any illegal content after receiving notice from the authorities. The CEO was released from jail when the court ruled that his arrest was illegal. This case has clarified the issue of intermediaries' responsibility in India and established a significant precedent.

State of Tamil Nadu v. Suhas Kutti, CC No. 4680 of 2004

In this case, the question of cyberstalking and the application of the Indian Penal Code, 1860 (hereinafter referred to as 'IPC') to issue of online harassment were addressed.

The case included a man who had been texting, calling, and emailing a woman to harass her. The man was found to have engaged in cyberstalking, and the court ruled that these situations were within the provisions of IPC for criminal intimidation and stalking.

The decision made clear that harassment on the internet is a severe offence that may cause the victim great mental anguish and suffering, and that the law has to change to accommodate this new type of crime. The court also emphasized that the anonymity and seclusion offered by online communication might give offenders the confidence to act in ways they ordinarily wouldn't in face-to-face meetings.

The case has established a crucial precedent in India for the application of IPC provisions to cases of online harassment and has brought attention to the necessity for legislation and regulations to deal with the particular problems created by cybercrime.

MC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra, CM APPL. No. 33474 of 2016

This case addressed the subject of online libel and the responsibility of intermediaries for offensive material provided by their users.

The case concerned a complaint made by MC Pneumatics against Jogesh Kwatra, a former employee who was accused of posting false information about the business and its directors on social media channels. After concluding that the posts were defamatory and harmful to the company's reputation, the Court ordered Kwatra to delete the posts and stop publishing any further damaging claims.

The court further determined that the social media sites where the content was posted were intermediaries under the Information Technology Act of 2000 and weren't responsible for the material their users submitted, provided that they met the legal criteria for due diligence. The court emphasized that after obtaining notification from the person who is impacted or a court order, intermediaries must take immediate action to remove unlawful information.

The case has established a significant precedent for intermediaries' responsibility in cyberdefamation cases in India and has brought attention to the necessity for a balance between the protection of free expression and the protection of reputation and privacy.

CBI v. Arif Azim, (2008) 150 DLT 769

This case, also known as the Sony Sambandh case, is a well-known case in India, where the accused individual had stolen Barbara Campa's credit card information. He subsequently made purchases using the stolen card on a Sony India Private Limited website (sony-sambandh.com). Barbara protested the purchase, and the credit card company notified Sony of this. Sony, therefore, informed the CBI of the Internet fraud and cheating case.

In response, the CBI opened a probe under IPC sections 418, 419, and 420. The accused person was found guilty of the crime of cyber-fraud by the Delhi HighCourt under the aforementioned provisions of IPC. This case is specifically related to Section 66C of the IT Act, 2000, which addresses identity theft and the illegal and dishonest use of electronic passwords, signatures, and other personal identifying elements.

ANALYSIS OF INDIAN LAW ON SOFTWARE SECURITY

Various laws regulate cybercrime in India depending on the type of crime committed by the offenders, however the Indian Evidence Act of 1872, the Indian Penal Code of 1860 along with the Information Technology Act of 2000 are the most significant ones. The Indian Penal Code, 1860 (Hereinafter referred to as "IPC") and Information Technology Act, 2000 (Hereinafter referred to as "IT Act" both outline penalties and punishments related to numerous cybercrimes, and several provisions in both statutes have connections to one another. The IPC can be used to adequately prosecute cybercrimes that are not regulated under IT Act. However, it is important to note that both the IT Act and IPC penalize offences committed in the cyber space and internet.

I. The Information Technology Act (IT Act 2000)

In order to protect the leadership, finance, and retail sectors that are managed by people or organisations using the internet, the IT Act, 2000 was passed in India by the Parliament. The IT Act's purview has been expanded to include regulating internet-connected communication tools and offering remedies when a person's rights have been infringed. A number of cybercrimes are covered by the IT Act, and the act exhaustively makes an attempt to cover all cybercrimes. To draw attention to the crime and offer justice for the transgression committed, the IPC may have the last say in the situation. The IT Act has the following significant provisions that provide crimes and penalties for various types of cyber fraud.

1. **Section 43 of IT Act** – This section applies to anybody who intentionally damages another person's computer equipment without first letting the owner permit for the same. In such circumstances, the owner of the computer or electronic device is entitled to full recompense for the whole harm. This section empowers the victims with the ability to seek compensation for the violation of the rights guaranteed by the Act.
2. **Section 66 of IT Act** – This section is appropriate for injuries suffered by individuals as a result of dishonesty or deception on the part of the accused while committing any of the acts as described in Section 43. The offender will receive a punishment that may last up to three years in prison or a fine up to Rs. 5 lakhs.
3. **Section 66B of IT Act** – This section includes the penalties for obtaining a computer or other illegal communication equipment unlawfully. Depending on the seriousness of the violation, a three-year sentence can be coupled with one lakh rupees as fine.
4. **Section 66C of IT Act -** This section addresses crimes including impersonation in digital signatures, password hacking, and distinguishing identifying characteristics. If the accused is proven guilty, he/she might face up to 3 years in jail and an additional penalty of Rs. 1 lakh in addition to their sentence.

5. **Section 66 D of IT Act** – It was put into effect with an emphasis on punishing offenders who use computer resources to impersonate others. The penalty for the offence is a period of imprisonment that may last up to 3 years, as well as a fine that may amount to one lakh rupees.

II. The Indian Penal Code (IPC 1980)

The Information Technology Act of 2000 does not offer or include certain offences, which are covered under the IPC. Major crimes that can have a significant negative impact on society as a whole such as theft of identity and other related cyber scam offences can be penalized through IPC, in addition to the remedies provided by the Information Technology Act of 2000.

The key provisions of the IPC, 1860 that deal with crimes linked to cybercrimes and the associated penalties are as follows:

1. **Forgery (Section 464)**

   Forgery stipulates that an individual who commits the crime of forgery, i.e. creates a false document or a false electronic record with the intention to cause damage or injury to the public or any individual in general, will be penalized by imprisonment for a time that may not exceed two years, a fine, or a combination of the two.

2. **Forgery for purpose of Cheating (Section 468)**

   This section provides that an individual who forges a document or electronic record with the intention of using it to cheat others, is liable for this offence. If the suspect is proven to be at fault, he will be sentenced to a period of jail that may last up to seven years, along with payment of fine.

3. **Presenting a forged document as genuine (Section 471)**

   If any person, who knows that a document/electronic record is forged, uses it as genuine, he shall be punished in the same manner as if he had himself forged such document or electronic record.

4. **Forgery for harming reputation (Section 469)**

   This offence involves using a forged document or electronic record intending to use to harm person's reputation. The penalty prescribed will be 3 years in jail and a fine which will be imposed as punishment for the offender.

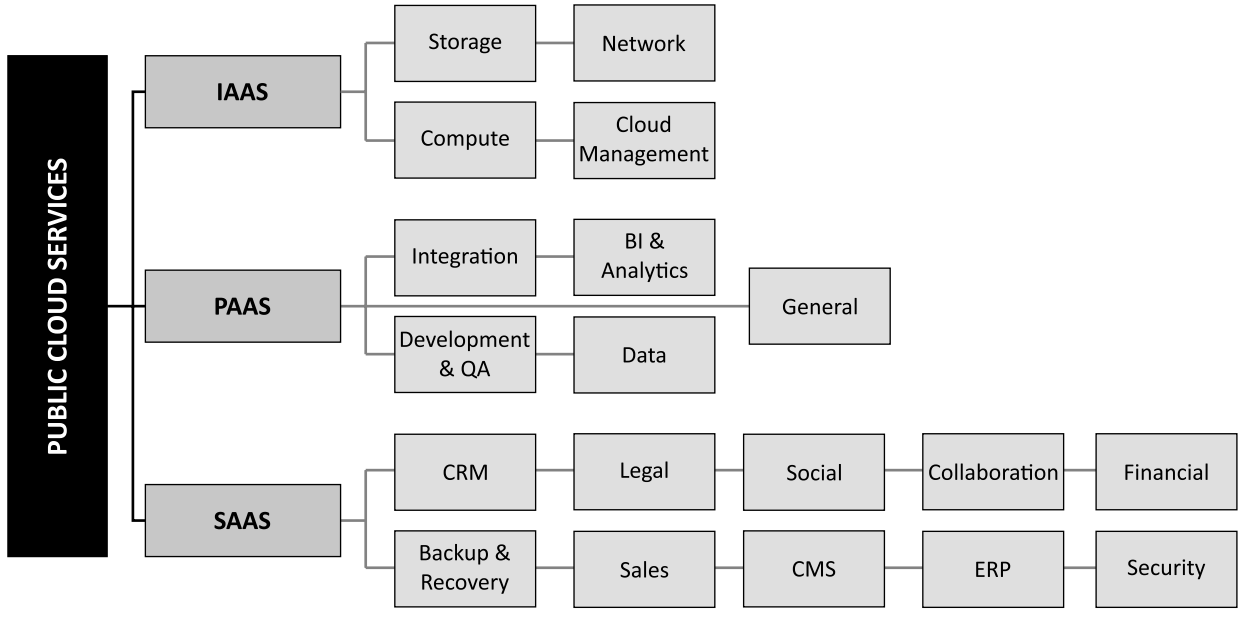
5. **Punishment for extortion (Section 384)**

   This offence involves putting the victim in a state of fear or inkjury so as to induce him to deliver to the offender any property, valuable security or anything that can be converted into a valuable security. The crime is punishable by a sentence of prison that may last up to 3 years, a fine, or both of them.

6. **Cheating and dishonestly inducing delivery of property (Section 420)**

   The perpetrator will get a penalty as well as a jail sentence that may last up to 7 years.

SAAS; PAAS, IAAS AND ON-PREMISE SOFTWARE: OVERVIEW AND RECENT TRENDS



IAAS Services

Infrastructure-as-a-Service, abbreviated as "IaaS," is a type of cloud computing where basic computing, networking, and storage resources are made available to users on demand through the internet and on a pay-as-you-go basis.

IaaS enables end users to increase and reduce resources as needed, lowering the need for expensive, upfront capital expenditures or needless "owned" infrastructure. IaaS offers the most fundamental level of control over cloud resources in contrast to PaaS and SaaS (even more modern computing paradigms like containers and serverless).

Early in the 2010s, IaaS began to gain popularity as a computing paradigm, and ever since then, it has evolved into the de facto abstraction model for many different kinds of workloads. IaaS remains fundamental but is more competitive than ever due to the emergence of new technologies like containers and serverless, as well as the introduction of the microservices application paradigm.

IAAS Platform and Architecture

IaaS is made up of a collection of physical and virtualized resources that provide consumers with the basic building blocks needed to run applications and workloads in the cloud.

- **Physical data centers:** IaaS providers manages large data centers that contain the physical machines required to power the various layers of abstraction on top of them and that are made available to end users over the web.
- **Compute:** IaaS is commonly understood as virtualized compute resources. Providers manage the hypervisors and end users can then programmatically provision virtual "instances" with desired amounts of compute and memory (and sometimes storage). Most providers offer both CPUs and GPUs for different types of workloads. Cloud compute also typically comes paired with supporting services like auto scaling and load balancing that provide the scale and performance characteristics that make cloud desirable in the first place.
- **Network:** Networking in the cloud is a form of Software Defined Networking in which traditional networking hardware, such as routers and switches, are made available programmatically. More

advanced networking use cases involve the construction of multi-zone regions and virtual private clouds.

- **Storage:** The three primary types of cloud storage are block storage, file storage and object storage. Block and file storage are common in traditional data centers but can often struggle with scale, performance and distributed characteristics of cloud. Thus, of the three, object storage has thus become the most common mode of storage in the cloud given that it is highly distributed, it leverages commodity hardware, data can be accessed easily over HTTP, and scale is not only essentially limitless but performance scales linearly as the cluster grows.

Pricing

IaaS prices are based on usage, so customers only pay for what they really use. There are now many different granularity levels included in the cloud infrastructure pricing models:

- **Subscriptions and reserved instances:** Many providers offer discounts off the sticker price for clients willing to commit to longer contract terms, typically around one to three years.
- **Monthly billing:** Monthly billing models are most common in the BMaaS market, where physical infrastructure typically implies steady state workloads without spiky characteristics.
- **By the hour/second:** The most common granularity for traditional cloud infrastructure, end users are charged only for what they use.
- **Transient/spot:** Some providers will offer up unused capacity at a discount via transient/spot instances, but those instances can be reclaimed if the capacity is needed.

Advantages

Several factors, when considered collectively, make cloud infrastructure seem like a good fit:

- **Pay-as-you-Go:** Unlike traditional IT, IaaS does not require any upfront, capital expenditures, and end users are only billed for what they use.
- **Speed:** With IaaS, users can provision small or vast amounts of resources in a matter of minutes, testing new ideas quickly or scaling proven ones even quicker.
- **Availability:** Through things like multizone regions, the availability and resiliency of cloud applications can exceed traditional approaches.
- **Scale:** With seemingly limitless capacity and the ability to scale resources either automatically or with some supervision, it's simple to go from one instance of an application or workload to many.
- **Latency and performance:** Given the broad geographic footprint of most IaaS providers, it's easy to put apps and services closers to your users, reducing latency and improving performance.

Typical use Cases

IaaS represents general purpose compute resources and is thus capable of supporting use cases of all types. IaaS is now mostly utilised for development and test environments, websites and web applications that are accessed by consumers, data storage, analytics, and data warehousing workloads, as well as backup and recovery, notably for on-premises workloads[34]. IaaS is also well suited for setting up and running popular commercial applications and software, such as SAP.

IaaS Services Infrastructure as a service helps companies to move their physical infrastructure to the cloud with

34. Available at: https://www.ibm.com/in-en/topics/iaas#:~:text=Infrastructure%2Das%2Da%2DService%2C%20commonly%20referred%20to%20as,as%2Dyou%2Dgo%20basis.

a level of control similar to what they would have in a traditional on-premise data center. As comparison to other service kinds, IaaS offers the most resemblance to the internal data centre. Storage, servers (or processing units), the network itself, and management tools for infrastructure upkeep and monitoring make up the core elements of a data center's infrastructure. Each of these elements has produced its own specific market niche.

IAAS: Storage

Companies can use storage services to store data on the storage equipment of third-party providers. Customers can access cloud storage online, which is displayed to them as a collection of storage pools or buckets, utilising sophisticated interfaces like command-line tools, web interfaces, or programming APIs[35]. Clients are unaware of the intricacy of the cloud storage architecture, although it is very sophisticated on the back end and often consists of distributed storage devices that are controlled by centralised software. Algorithms are used by sophisticated storage management software to manage data scattered across numerous storage devices.

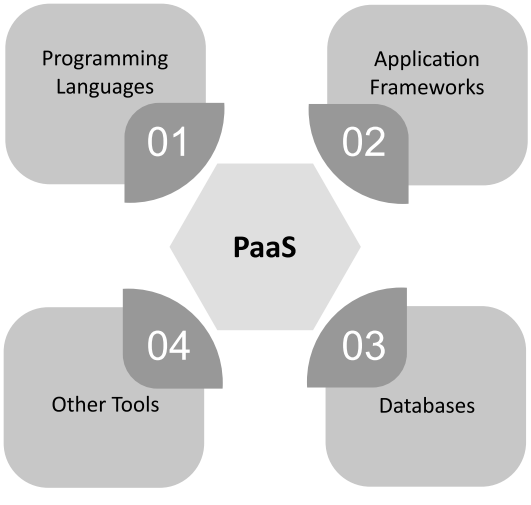
Network slowness, reliance on internet accessibility, security issues, and restricted control are all potential drawbacks. Due to the cloud provider's data center's distinct geographic location, network latency is greater than with internal storage. If a customer doesn't have a local copy of their data and instead saves it all in a public cloud, they are entirely dependent on internet connectivity. To prevent information loss or compromise, a cloud provider should provide high-level security, and data transit must be encrypted.

PAAS

Platform-as-a-Service, also known as PaaS, is a cloud computing model that offers customers a full cloud platform—including hardware, software, and infrastructure for creating, deploying, and managing applications without the expense, complexity, and rigidity that frequently accompany building and maintaining that platform on-premises. Without the hassles of updating the operating system, development tools, or hardware, PaaS offers everything developers require for application development. Instead, a third-party service provider uses the cloud to supply the whole PaaS environment or platform.

PaaS helps businesses avoid the hassle and cost of installing hardware or software to develop or host new custom applications. To build custom apps, development teams can easily obtain pay-as-you-go access to infrastructure, development tools, operating systems, and other resources. The result is simpler, faster, and secure app development that gives developers the freedom to focus on their application code.

PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle. **Example:** Google App Engine, Force.com, Joyent, Azure.



35. Available at: https://www.techtarget.com/searchcloudcomputing/definition/Infrastructure-as-a-Service-IaaS.

1. **Programming Languages**

   PaaS providers provide various programming languages for the developers to develop the applications. Some popular programming languages provided by PaaS providers are Java, PHP, Ruby, Perl, and Go.

2. **Application Frameworks**

   PaaS providers provide application frameworks to easily understand the application development. Some popular application frameworks provided by PaaS providers are Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.

3. **Databases**

   PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

4. **Other Tools**

   PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

Advantages of PAAS

The most commonly-cited benefits of PaaS, include**:**

1. **Simplified Development -** PaaS allows developers to focus on development and innovation without worrying about infrastructure management.
2. **Lower Risk -** No need for up-front investment in hardware and software. Developers only need a PC and an internet connection to start building applications.
3. **Prebuilt Business Functionality -** Some PaaS vendors also provide already defined business functionality so that users can avoid building everything from very scratch and hence can directly start the projects only.
4. **Instant Community** - PaaS vendors frequently provide online communities where the developer can get the ideas to share experiences and seek advice from others.
5. **Scalability** - Applications deployed can scale from one to thousands of users without any changes to the applications.

Disadvantages of PAAS

1. **Vendor Lock-in** - One has to write the applications according to the platform provided by the PaaS vendor, so the migration of an application to another PaaS vendor would be a problem.
2. **Data Privacy** - Corporate data, whether it can be critical or not, will be private, so if it is not located within the walls of the company, there can be a risk in terms of privacy of data.
3. **Integration with the rest of the systems applications** – It may happen that some applications are local, and some are in the cloud. Thus, there will be chances of increased complexity when we want to use data which in the cloud with the local data.

Use Cases for PAAS

By providing an integrated and ready-to-use platform and by enabling organizations to offload infrastructure management to the cloud provider and focus on building, deploying and managing applications, PaaS can ease or advance a number of IT initiatives, including:

- **API development and management:** Because of its built-in frameworks, PaaS makes it much simpler

for teams to develop, run, manage and secure APIs (application programming interfaces) for sharing data and functionality between applications.

- **Internet of Things (IoT):** Out of the box, PaaS can support a range of programming languages (Java, Python, Swift, etc.), tools and application environments used for IoT application development and real-time processing of data generated by IoT devices.
- **Agile development and DevOps:** PaaS can provide fully-configured environments for automating the software application lifecycle including integration, delivery, security, testing and deployment.
- **Cloud migration and cloud-native development:** With its ready-to-use tools and integration capabilities, PaaS can simplify migration of existing applications to the cloud particularly via *replatforming* (moving an application to the cloud with modifications that take better advantage of cloud scalability, load balancing and other capabilities) or *refactoring* (re-architecting some or all of an application using microservices, containers and cloud-native technologies).
- **Hybrid cloud strategy:** Hybrid cloud integrates public cloud services, private cloud services and on-premises infrastructure and provides orchestration, management and application portability across all three. The result is a unified and flexible distributed computing environment, where an organization can run and scale its traditional (legacy) or cloud-native workloads on the most appropriate computing model. The right PaaS solution allows developers to build once, then deploy and mange anywhere in a hybrid cloud environment.

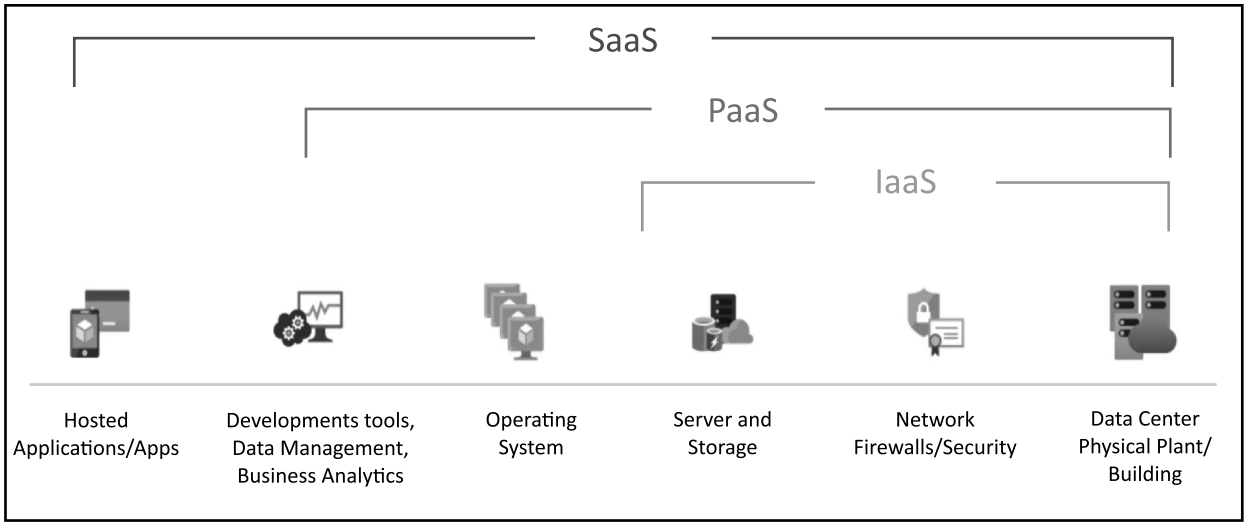
Purpose-Built PAAS Types

Many cloud, software and hardware vendors offer PaaS solutions for building specific types of applications, or applications that interacting with specific types of hardware, software or devices[36].

- **AIPaaS (PaaS for Artificial Intelligence)** lets development teams build artificial intelligence (AI) applications without the often prohibitive expense of purchasing, managing and maintaining the significant computing power, storage capabilities and networking capacity these applications require. AiPaaS typically includes pre-trained machine learning and deep learning models developers can use as-is or customize, and ready-made APIs for integrating specific AI capabilities, such as speech recognition or speech-to-text conversion, into existing or new applications.
- **iPaaS (integration platform as a service)** is a cloud-hosted solution for integrating applications. iPaaS provides organizations a standardized way to connect data, processes, and services across public cloud, private cloud and on-premises environments without having to purchase, install and manage their own backend integration hardware, middleware and software. (Note that Paas solutions often include some degree of integration capability API Management, for example – but iPaaS is more comprehensive.)
- **cPaaS (communications platform as a service)** is a PaaS that lets developers easily add voice (inbound and outbound calls), video (including teleconferencing) and messaging (text and social media) capabilities to applications, without investing in specialized communications hardware and software.
- **mPaaS (mobile platform as a service)** is a PaaS that simplifies application development for mobile devices. mPaaS typically provides low-code (even simple drag-and-drop) methods for accessing device-specific features including the phone's camera, microphone, motion sensor and geolocation (or GPS) capabilities.

36. Available at: https://www.techtarget.com/searchcloudcomputing/definition/Platform-as-a-Service-PaaS.

SAAS SERVICES



Software as a service (or SaaS) is a way of delivering applications over the Internet as a service. SaaS applications are also known as Web-based software, on-demand software, or hosted software. Common examples are email, calendaring, and office tools (such as Microsoft Office 365). It is a cloud-based software delivery model that allows SaaS applications to run on SaaS providers' servers instead of installing and maintaining software on-premises. The SaaS provider manages access to the application, including security, availability, and performance.

SaaS being a cloud based service where instead of downloading software your desktop PC or business network to run and update, you instead access an application via an internet browser. The software application could be anything from office software to unified communications among a wide range of other business apps that are available.

This offers a variety of advantages and disadvantages. Key advantages of SaaS includes accessibility, compatibility, and operational management. Additionally, SaaS models offer lower upfront costs than traditional software download and installation, making them more available to a wider range of businesses, making it easier for smaller companies to disrupt existing markets while empowering suppliers.

The major disadvantage of SaaS applications is that they ordinarily require an internet connection to function. However, the increasing wide availability of broadband deals and high-speed phone networks such as 5G makes this less of an issue. Additionally, some SaaS applications have an offline mode that allows basic functionality. Google Workspace, Trello, Zoom, DocuSign, Slack, Adobe Create Cloud, Mailchimp are some popular examples of SaaS products.

Characteristics of SAAS

1. **SaaS Multi-Tenant Architecture** - Multi-tenancy is an architecture where all SaaS vendor clients and applications share a single, common infrastructure and code base that is centrally maintained. This architecture allows vendors to innovate more quickly, saving development time previously spent on maintaining outdated code
2. **Easy Customisation with SaaS** - Users can easily customise applications to fit their business processes without affecting the shared infrastructure. A SaaS model supports each user and company's unique customisations changes and preserves them through regular upgrades. This means SaaS providers can make upgrades more often, with less customer risk and lower adoption costs.

3. **Better Access From Network Devices** - A SaaS model allows your business to remotely access data from any networked device, making it easy to manage privileges, monitor data use, and ensure many users can see the same information simultaneously.

4. **SaaS Harnesses the Consumer Web** – Anyone familiar with Amazon.com or My Yahoo! will be familiar with the Web interface of typical SaaS applications. With the SaaS model, you can customise with point-and-click ease, making the weeks or months it takes to update traditional business software seem hopelessly old-fashioned.

Advantages of SAAS

SaaS removes the need for organizations to install and run applications on their own computers or in their own data centers. This eliminates the expense of hardware acquisition, provisioning and maintenance, as well as software licensing, installation and support[37]. Due to the increased efficiency and cost-effectiveness of software as service applications, many businesses turn to cloud-based SaaS for solutions due to following reasons:

1. **Low Set Up and Infrastructure costs** - You only pay for what you need, so it is a very cost-effective solution for all-sized businesses.

2. **Scalability** - You can adapt your requirements to the number of people who need to use the system, the volume of data and the functionality required as your business grows.

3. **Accessible from Anywhere** - Just connect to the internet, and you can work from wherever you need to be via desktop, laptop, tablet or mobile or other networked devices.

4. **Automatic, frequent updates** - Providers offer timely improvements thanks to their scale and because they receive feedback about what their customers need. This frees up your IT department for other, more business-critical tasks.

5. **Security at the highest level required by any customer** - Because of the shared nature of the service, all users benefit from the security level set up for those with the highest need.

Future of SAAS

SaaS and cloud computing have come a long way in assisting businesses in creating comprehensive integrated solutions. Organizations are creating SaaS integration platforms (or SIPs) to build additional SaaS apps as knowledge and adoption of the model grow[38]. SaaS is one of many cloud computing remedies for enterprise IT problems. Other "as-a-Service" choices include:

- Infrastructure as a Service (IaaS) – the provider hosts hardware, software, storage and other infrastructure components.
- Platform as a Service (PaaS).
- Everything as a service (XaaS) – which is essentially all the "aaS" tools neatly packaged together.

The payment model for these kinds of services is typically a per-seat, per-month charge based on usage – so a business only has to pay for what they need, reducing upfront costs.

With companies adopting various "aaS" services, long-term relationships with service providers will grow, leading to innovation as customers' evolving needs are understood and provided for. SaaS may one day help address critical business challenges, such as predicting which customers will churn or which cross-selling practices work best.

37. Available at: https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-saas/.

38. Available at: https://www.techradar.com/news/what-is-saas

On Premise Software

On-premises software is a type of software delivery model that is installed and operated from a customer's in-house server and computing infrastructure. Also meaning, thereby that subsequent maintenance, repairs, safety, and further updates are all handled on-site. It just needs a licenced or purchased copy of software from an independent software provider and makes use of the natural computer resources of the company. Software installed on-site is also referred to as shrink wrap. After buying software, the company often installs it on its servers, connecting relevant database software and configuring operating systems accordingly. Since there is no involvement of any third-party, the company has full ownership and responsibility.

On-premises software is the most prevalent, traditional method of using enterprise and consumer applications. On-premises software typically requires a software license for each server and/or end user. The customer is responsible for the security, availability and overall management of on-premises software. However, the vendor also provides after sales integration and support services. Because it requires onsite server gear, capital expenditures for software licences, onsite IT support employees, and longer integration times, onsite software is more expensive than on-demand or cloud software. On-premises software, however, is regarded as being more secure because the full instance of the software stays on the organization's grounds

In the past, on-premise software was the only solution available to companies. Today, that's changing, as more and more off-site solutions become popular, and cloud computing becomes the standard. There is now agreement amongst IT professionals that companies can't solely rely on on-premise applications. In any case, a mixture of off-premise and on-premise solutions, also known as a hybrid IT environment, will be the way forward.

Pros and Cons of On-Premise Software

Features	*Pros*	*Cons*
Cost	Overall costs in the long-term are lower	Substantial upfront investment required
Security	Companies can deploy their own security protocols	Technical IT support is required, increasing costs
Control	Full control to the user	Trained IT Staff is required to provide support
User Access	Internet connectivity is often not required for in-house solutions	This also means access isn't available on-the-go
Future-Proofing	Additional software can be purchased at extra costs	No updates are provided and new features are costly to add

LEGAL AND COMPLIANCE REQUIREMENTS OF SOFTWARE SECURITY

Under the Information Technology Act, 2000, anyone who "controls, processes and handles" the data must have a lawful basis to do the same and the same must be done within applicable data retention requirements[39].

All body corporates are required to adhere to The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

39. Cybersecurity: Laws and Regulations, India, (November 14, 2022), ICGL, Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter referred to as 'IT Rules, 2011') defines 'cyber incidents' under Rule 2(d) in the following words: *"Cyber incidents means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation*[40]*"*

Rule 8 of the IT Rules 2011 talks about the Reasonable Security Practices and Procedures to be followed by body corporates and individuals. Rule 8[41] has been summarized herein below:

As per Rule 8(1) of IT Rules 2011, it is considered that Body Corporates and individuals have compiled with the reasonable security practices if they have such security practices and standards in place which corresponds with the information assets which are sought to be protected, keeping in mind the nature of the business[42]. It is obligatory to have a documented and elaborate information security programme and security policy containing *"managerial, technical, operational and physical security control measures"*[43].

It has been clarified in Rule 8(2) that an example of one such standard as referred to in sub-rule (1) of Rule 8 is the International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System – Requirements"[44]. Furthermore, if any association or entity follows practices for data protection other than the standard practices prescribed by IS/ISO/IEC, then it is mandatory to get its code of best practices approved and notified by Central Government[45]. The Rules also make it mandatory to get an audit of reasonable security practices and procedures conducted by an auditor every year or as and when there is significant upgradation of the processes and computer resources of a body corporate[46].

Moreover, the Data Security Council of India (DSCI) regularly publishes standards and best practices in cyber security, which can be kept in mind while developing security practices.

Reporting of Incidents:

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (for brevity, 'CERT-In Rules') prescribes the procedure of function of CERT-IN, which is the Computer Emergency Response Team, appointed by Central Government in accordance with Section 70B of the Information Technology Act, 2000. The CERT-In has been designated as the Nodal Agency for performing certain cyber security functions, some of which have been enumerated below:

- Handling cybersecurity incidents through emergency measures.
- Issuing guidelines, practices and advisories on cybersecurity and safe practices.
- Flagging, forecasting and alerting cybersecurity incidents, etc[47].

Rule 12 of the CERT-In Rules provides for a 24-hour Incident Response Helpdesk for reporting of cyber-security

40. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Available at: https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

41. Ibid.

42. Ibid.

43. Ibid.

44. Supra, Note 43.

45. Rule 8(3), Ibid.

46. Rule 8, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

47. The Information Technology Act, 2000 and The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

incidents[48]. Certain cybersecurity incidents have been identified in the annexure to the CERT In Rules and the same shall be mandatorily reported to the Incident Response Helpdesk as soon as possible[49].

Rule 12(a) reads as follows[50]:

"Reporting of incidents: Any individual, organisation or corporate entity affected by cyber security incidents may report the incident to CERT-In. The type of cyber security incidents as identified in Annexure shall be mandatorily reported to CERT-In as early as possible to leave scope for action. Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action"[51].

The Annexure to CERT-In Rules provides for mandatory reporting of the following incidents:

a. "Targeted scanning/ probing of critical networks/ systems;
b. Compromise of critical systems/ information;
c. Unauthorised access of IT systems/ data;
d. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.;
e. Malicious code attacks such as spreading of virus/ worm/ Trojan/ Botnets/ Spyware;
f. Attacks on servers such as Database, Mail and DNS and network devices such as Routers;
g. Identity Theft, spoofing and phishing attacks;
h. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks;
i. Attacks on Critical infrastructure, SCADA Systems and Wireless networks;
j. Attacks on Applications such as E-Governance, E-Commerce etc"[52].

The Ministry of Electronics and Information Technology has come out with directions regarding compliances and reporting obligations passed vide Notification No. 20(3)/2022-CERT-In dated 28.04.2022[53]. The notification has made it mandatory to report cyber incidents as listed above within a period of six hours of the incident coming into notice or being brought into the attention of the concerned person. This has been done to ensure prompt action to the cyber security incident and prevent delays in investigation and consequent action. The new 6 (six) hour deadline does not have retrospective effect and will apply only to cyber security incidents that take place on or after June 27, 2022[54].

48. Supra, Note 42.

49. Ibid.

50. CERT-IN'S SIX HOUR REPORTING RULE FOR CYBER SECURITY INCIDENTS- Statutory Interpretation and Analysis, Argus Partners, Available at: https://www.argus-p.com/uploads/blog_article/download/1664436637_Reporting_CyberSecurity_Incidents_in_India-_Statutory_Interpretation_and_Analysis.pdf.

51. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

52. Ibid.

53. CERT-IN'S SIX HOUR REPORTING RULE FOR CYBER SECURITY INCIDENTS- Statutory Interpretation and Analysis, Argus Partners, Available at: https://www.argus-p.com/uploads/blog_article/download/1664436637_Reporting_CyberSecurity_Incidents_in_India-_Statutory_Interpretation_and_Analysis.pdf.

54. Supra, Note 56.

LESSON ROUND-UP

- Any kind of external intervention in software systems can seriously threaten the security of data and make it prone to unauthorized access.
- Software refers to set of instructions which enable the hardware components to perform.
- System software serves as a point of interaction between the hardware components of computer and user applications.
- Operating system is basic and essential to the functioning of a computer as all computer applications sit inside the operating system of a computer.
- Application Software are dedicated to the performance of a particular task or function.
- Utility Software assists the system software in performing its work.
- Software Security refers to the practice of developing and engineering the software in a manner which keeps it secure from external malicious attacks, while also ensuring that in case of any such attack, the software does not malfunction and continues to operate.
- Proactive security aims to prevent any data breach incident before any malware is able to access network server or before vulnerabilities in a software are exploited by hackers.
- Infrastructure-as-a-Service, abbreviated as "IaaS," is a type of cloud computing where basic computing, networking, and storage resources are made available to users on demand through the internet and on a pay-as-you-go basis.
- Platform-as-a-Service, also known as PaaS, is a cloud computing model that offers customers a full cloud platform—including hardware, software, and infrastructure for creating, deploying, and managing applications without the expense, complexity, and rigidity that frequently accompany building and maintaining that platform on-premises.
- Software as a Service (or SaaS) is a way of delivering applications over the Internet as a service. SaaS applications are also known as Web-based software, on-demand software, or hosted software. Common examples are email, calendaring, and office tools (such as Microsoft Office 365).
- On-premises software is a type of software delivery model that is installed and operated from a customer's in-house server and computing infrastructure.

GLOSSARY

Defects: A defect refers to a mistake made by developer while developing the software which leads to differences in intended results and actual results.

Bugs: A bug is an error, problem or defect in the design or development of a software which hampers its ability to produce the desired result or results into producing invalid results.

Failure: It refers to the inability of a software to perform its designated.

Flaws: A flaw refers to a problem in the software code which makes the software prone to security risks. Software flaws can be rectified by updates formulated by software developer.

Vulnerabilities: It refers to exploitable points within the software which can be targets for potential attack by hackers.

Software: It is the collection of instructions which directs the computer as to 'which' task to perform and 'how' to perform it.

System Software: These software enables interaction of the user with hardware components of the computer and helps in running programs on the computer.

Application Software: These are software which are dedicated to the performance of a particular task or function.

Utility Software: A utility software is a type of application which assists the system software in performing its work.

Software Security: It refers to the practice of developing and engineering the software in a manner which keeps it secure from external malicious attacks, while also ensuring that in case of any such attack, the software does not malfunction and continues to operate.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. Differentiate between hardware and software.
2. What are the functions of an operating system?
3. Discuss the classification of software on the basis of availability and shareability.
4. Differentiate between a Compiler and Interpreter.
5. Discuss best practices in software security.
6. Enumerate software security goals.
7. Discuss about SaaS, PaaS and IaaS.
8. Write a short note on on-premise software.
9. Write a short note on legal and compliance requirement of software security.

LIST OF FURTHER READINGS

- Mathias Payer, "Software Security: Principles, Policies and Protection", July 2021, Available At: https://nebelwelt.net/SS3P/softsec.pdf
- LeBlanc, John Viega, 19 deadly sins of software security. McGraw-Hill, 2005.
- Gary McGraw, Software Security: Building Security In. Addison-Wesley Professional, 2006.

Database Management

Lesson 10

KEY CONCEPTS

■ Data Base ■ Data Structure ■ Data Base Management System ■ Data Mining ■ Data Warehousing

Learning Objectives

To understand:

- The concept of Database with basics of Data Structure
- Database Abstraction, Implementation and Creation
- DBMS- Users of DBMS and its applications
- The purpose of Data Warehousing and Data Mining
- The usefulness of Data warehousing and Data mining in context to a large retail firm

Lesson Outline

- Data Base Concepts
- Data Structure
- Data Base Management System
- Data Base Files
- Data Mining and Warehousing
- Lesson Round-Up
- Test Yourself

DATABASE CONCEPTS

Database concepts are vital to understand how databases function, and databases are a crucial element in modern computer systems. The aim of databases, data abstraction, data models, database management systems, data integrity, data security, and the benefits and drawbacks of databases are just a few of the topics that we'll cover in this chapter.

Purpose of Database

A database's goal is to have a collection of data serve as many applications as it can. As a result, a database is frequently considered to be a collection of data required to carry out specific tasks inside a business or organisation. It would enable not just data retrieval but also on going data alteration, which is necessary for operation control. You might be able to search the database to get answers to your inquiries or details for planning.

Database Abstraction

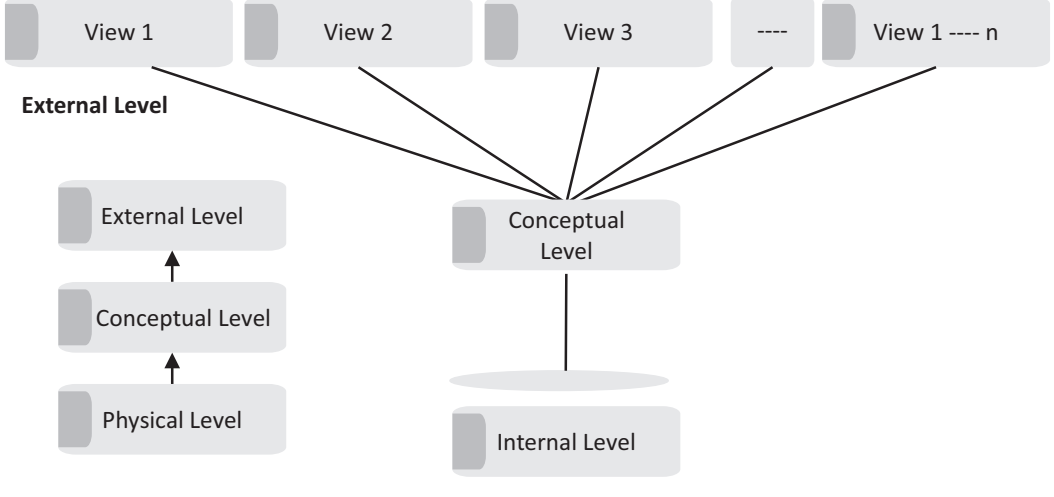
Providing the user with only the information they need is one of a database's main goals. This indicates that the system hides some information about how the data is maintained and kept rather than disclosing all the information about the data. They are shielded from the complexity of databases, which, if necessary, are arranged across a number of layers of abstraction to ease their engagement with the system. Three layers are used to implement the various database levels:

Physical Level (Internal Level): Internal level, the lowest level of abstraction, is most analogous to physical storage. It explains the specifics of how the data is kept on the storage media.

Conceptual Level: The data that is specifically saved in the database is described at this level of abstraction. Moreover, it describes the connections between the data. At this level, databases are logically explained using straightforward data structures. Users at this level are not concerned with the actual implementation of these logical data structures.

View Level (External Level): It relates to how specific users see the data and is the level that is closest to the users.

Each modification at one level can have an impact on plans at other levels since a database can be seen through three different levels of abstraction. Databases may occasionally undergo numerous modifications as they continue to expand. The database shouldn't need to be redesigned and implemented as a result of this. The idea of data independence is useful in this situation.



Data Models: A database's data and connections are conceptually represented by a data model. It offers a blueprint that details how information is set up, kept, and used in a database. Hierarchical, network, and relational models are the three basic types of data models.

Hierarchical Model: The hierarchical approach organises data in a tree-like form, with a parent-child connection between each item. No of how many kids a parent has, each child can only have one parent. Organizational charts and other types of data with a natural hierarchical structure are best suited for the hierarchical approach.

Network Model: As an extension of the hierarchical model, the network model enables records to have numerous parent-child connections. It is helpful for modelling data when a record may include several parent and child connections since it may express complicated relationships.

Relational Model: The model that is being utilised the most is the relational model. Data is arranged in tables with rows and columns, where each row denotes a distinct record and each column denotes a field or attribute. A large variety of data kinds and connections may be handled by the relational model, which is adaptable.

Database Management System (DBMS): Software that enables users to build, edit, and administer databases is known as a Database Management System (DBMS). To manage the storing, retrieval, and modification of data in a database, it offers a variety of features and capabilities.

Data Definition Language (DDL) is used to create and edit database schema. Data Manipulation Language (DML) is used to query and modify data. Transaction Control Language (TCL) is used to govern how transactions are handled.

Data Integrity: Any database must maintain data integrity. It speaks of the precision, thoroughness, and consistency of information in a database. By imposing restrictions and guidelines on the data in a database, a DBMS protects data integrity.

Constraints: The structure and connections between tables are established by constraints, which are rules. They make sure that linkages between tables are upheld and that data is not duplicated. Each row in a table is guaranteed to be unique by the primary key constraint, and each record in one table is guaranteed to have a matching record in another table by the foreign key constraint.

Rules: Data values must fall inside particular ranges or satisfy certain requirements, which is why rules like check constraints are used. A check constraint, for instance, can make sure that a person's birthdate is not later than the present day.

Data Security: A crucial idea in databases is data security. It speaks of safeguarding data from unlawful access, usage, disclosure, or obliteration. To guarantee data security, a DBMS offers a variety of security capabilities, including authentication, authorisation, and encryption.

Authentication: It includes confirming the user's identity, usually using a username and password.

Authorization: It regulates each user's degree of access. It entails allowing or refusing access to particular database sections.

Encryption: Data is protected by encryption by being transformed into a secret code that can only be cracked with a special key. It guarantees that the data cannot be read even if an unauthorised person obtains access to the database.

Advantages of Database

Let's look at some of the advantages offered by database systems and how they solve the issues described above: -

- Significantly reduces database redundancy.
- The database has strong control over inconsistent data.
- Data exchange is made easier by the database.
- Databases impose rules.
- Data security may be ensured via the database.
- Databases may be used to ensure integrity.

Database systems are therefore recommended for systems with superior performance and efficiency.

Disadvantages of Database

There may be various issues that arise as a result of the database system's need to do sophisticated tasks; these issues can be referred to as the database system's drawbacks. They include:

- Without effective controls, security might be jeopardised.
- Without effective controls, integrity might be jeopardised.
- Further hardware could be needed.
- Possible performance overhead is considerable.

The mechanism is probably complicated.

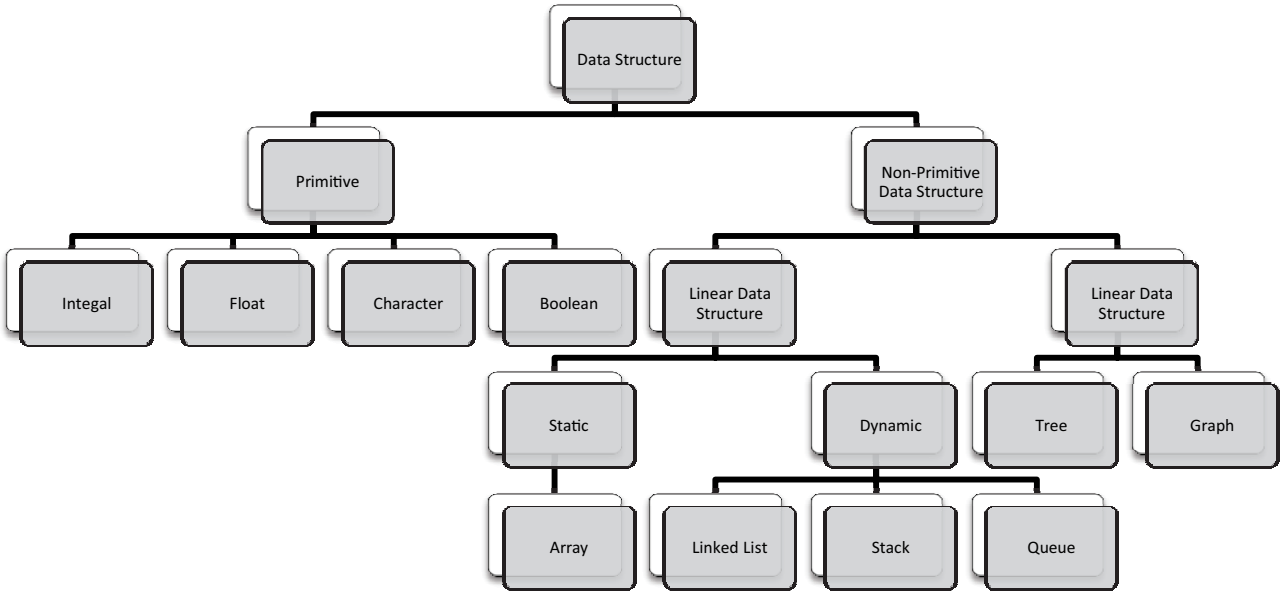
Therefore, understanding database principles is essential to comprehending how databases operate. Anybody dealing with databases has to understand key concepts including data models, DBMS, data integrity, and data security. To guarantee efficient and successful data administration, it is crucial to keep current with the most recent database ideas and technology. Databases may offer a strong foundation for organising and analysing massive volumes of data if the correct skills and resources are applied.

DATA STRUCTURE

A fundamental idea in computer science, data structures are crucial for effective programming. It is a method of setting up and keeping track of data in a computer so that it may be easily retrieved and used. We will explore the numerous facets of data structures in this chapter, including their types, operations, and implementation.

Types of Data Structures

The two types of data structures are Primitive and Non-Primitive data structures.



Primitive Data Structures

Primitive data structures are the character and number-based data structures that are pre-built into programmes.

Machine-level instructions might directly alter or use these data structures.

Primitive Data Structures include fundamental data types including Integer, Float, Character, and Boolean.

Due to the fact that they include characters that cannot be further subdivided, these data types are also known as simple data types.

Non-Primitive Data Structures

Data structures that are descended from primitive data structures are known as non-primitive data structures.

Machine-level instructions cannot directly alter or use these data structures.

These data structures' main goal is to create a collection of data pieces that are either homogenous (all of the same kind) or heterogeneous (different data types).

These data structures may be divided into two sub-categories: linear data structures and non-linear data structures, based on the organisation and structure of the data.

Linear Data Structures: Each component in a linear data structure is related to the element before it and the element after it in a consecutive way. The most popular linear data structure types are queues, stacks, linked lists, and arrays.

Arrays: A distinct index is given to each element, starting at 0. Although they can't be resized in-place, arrays are fixed in size and offer quick access to their elements.

Linked Lists: A linked list is made up of a group of objects called nodes, each of which has a reference to the

node after it as well as data. Linked lists make it simple to add and remove components and can be used to construct dynamic data structures.

Stacks: It only permits adding and deleting pieces from the top of the stack, which is one end.

Queues: The First-In-First-Out (FIFO) principle governs the operation of queues, which are a type of data structure. It enables the addition of elements at the back and the removal of parts from the front.

Non-Linear Data Structures: The organisation of data in non-linear data structures is not sequential. Instead, they show intricate connections between different data points. The most popular non-linear data structure types are heaps, trees, and graphs.

Tress: Trees are hierarchical data structures in which each node contains zero to more than one offspring and at most one parent. In hierarchical data representations like file systems, organisational charts, and database indexes, trees are employed.

Graphs: Graphs are collections of nodes connected by connecting edges. Graphs are used to describe intricate connections between data items, including those seen in social, transportation, and communication networks.

Heaps: A unique kind of binary tree that meets the heap condition is called a heap. The element with the greatest (or lowest) priority will always be at the bottom of the heap according to the heap attribute.

Key Features of Data Structures

Here are some of the Important Characteristics of these Data Structures:

Robustness: In theory, all computer programmers strive to create software that produces accurate results for all conceivable inputs and performs effectively across all hardware architectures. Both legitimate and erroneous inputs must be managed by this powerful programme.

Adaptability: The development of large-scale software systems is necessary for many years in order for programmes like web browsers, word processors, and internet search engines to function correctly and efficiently. Software also changes as a result of new technology or dynamic market situations.

Reusability: Adaptability and Reusability are complementary qualities. It is common knowledge that a programmer need several resources to create any software, making it an expensive endeavour. Yet, if the software is created in a way that makes it adaptive and reusable, it can be used in the majority of future applications. Consequently, it is feasible to create reusable software that looks to be both time and cost-effective by using excellent data structures.

Operations on Data Structures: Data structures support a number of operations, including insertion, deletion, traversal, and searching. A data structure gets a new element by insertion.

Deletion: Deletion involves removing a data structure piece. A data structure is traversed by going through each element in turn. A data structure element is located using search.

Implementation of Data Structures

The use of arrays, linked lists, and pointers can be used to build data structures. While they have a fixed size, arrays are the most straightforward data structure to build. Linked lists provide dynamic data structures but demand more memory for pointer storage. Although pointers are an effective tool for building data structures, they need for a deep understanding of memory management.

Therefore, it can be concluded that a fundamental idea in computer science, data structures are crucial for effective programming. Data structures may be divided into two categories: linear and non-linear. Although non-linear data structures show intricate interactions between data pieces, linear data structures arrange data in a

sequential manner. The numerous operations supported by data structures include insertion, deletion, traversal, and searching. These can be put into practise utilising pointers, linked lists, and arrays. Data structures may offer a potent platform for data organisation and manipulation with the correct skills and resources.

DATABASE MANAGEMENT SYSTEM

A Database Management System (DBMS) is a piece of software that controls how data is stored, organised, and retrieved from databases. It is a crucial tool for successfully and efficiently handling massive amounts of data. We shall talk about a DBMS's architecture, parts, and features in this chapter, among other things.

DBMS Architecture

There are three levels of a DBMS structure: external, conceptual and internal.

External Level: It specifies the actions that may be carried out on the data as well as how the data is displayed to the user. The application software that accesses the database is of interest at the external level.

Conceptual Level: The database is logically represented at the conceptual level. It describes the connections between the various data pieces as well as the general structure of the database. The conceptual level is unrelated to how the data is physically stored.

Internal Level: The database's physical representation is at the internal level. It specifies how information is kept and retrieved on the actual storage hardware.

DBMS Components

Data Definition Language (DDL), Data Manipulation Language (DML), query language, and data dictionary are the four parts of a Database Management System (DBMS).

Data Definition Language (DDL): DDL, or Data Definition Language, is used to specify the database's structure, including the tables, columns, and connections between them. Also, it outlines the restrictions that apply to database data storage.

Data Manipulation Language (DML): The database's data can be changed using the Data Manipulation Language (DML). Operations like insertion, deletion, modification, and retrieval of data are included.

Query Language: Data is collected from the database using query language. The database library standard language, SQL (Structured Query Language), is included.

Data Dictionary: A database that contains metadata about the data in the database is called a data dictionary. It contains details about data kinds, connections between data items, and access rights.

DBMS Features: A DBMS has a number of capabilities that make it an indispensable tool for handling massive amounts of data. The following are some of a DBMS's important characteristics:

Data Security: To prevent unauthorised access to data, a DBMS offers a variety of security options. Access control, authentication, and encryption are all part of it.

Data Integrity: By imposing constraints like uniqueness, referential integrity, and domain integrity, a DBMS protects the accuracy of the data.

Concurrency Control: Concurrency control is a feature of DBMSs that permits concurrent entry to the database without compromising with other users' operations.

Backup and Recovery: In the case of a system breakdown, a DBMS offers backup and recovery options to avoid losing data. It has capabilities like recovery and transaction recording.

Scalability: A DBMS offers scalability characteristics to meet an organization's expanding data demands. It has capabilities like replication and segmentation.

DBMS Users

Users with varying access and permissions use a typical DBMS for a variety of objectives. Some people back up their data while others retrieve it. A DBMS's users may be roughly divided into three groups: administrators, designers and end users.

Administrator: Administrators are in charge of managing the database and maintaining the DBMS. They are in charge of monitoring how it should be utilised and by whom. In order to enforce security and preserve isolation, they construct access profiles for users and set restrictions. Moreover, administrators take care of DBMS resources including system licences, necessary equipment, and other upkeep-related software and hardware.

Designers: A company's DBA staff includes database designers. The individuals who really work on the designing portion of the database are known as designers. They are in charge of comprehending end customers' database requirements. They closely monitor what information needs to be stored and in what format. The whole collection of entities, relations, constraints, and views are identified and designed by them.

End Users: End users are the ones who genuinely profit from a DBMS. End users might be as basic as viewers who focus on the logs or market prices or as complex as business analysts. They can also be knowledgeable experts who access data by directly querying the database using a DBMS's query interface. Those that need to use data from a database to power sophisticated applications like knowledge bases, decision systems, intelligent systems, data analytics, or the storage and administration of big data might be considered to be another group of end users.

Advantages of DBMS

Controls database redundancy: Because it keeps all the data in a single database file and stores the recorded data in the database, it is able to manage data redundancy.

Data sharing: A DBMS enables an organization's authorised users to distribute data across several users.

Easy Maintenance: Because the database system is centralised, it may be simple to maintain.

Time savings: It lessens the requirement for maintenance and development time.

Backup: It has subsystems for backup and recovery that automatically back up data in the event of hardware or software problems and restore the data as needed.

Multiple User Interface: It offers a variety of user interfaces, including graphical user interfaces and application programme interfaces.

Disadvantages of DBMS

Cost of Hardware and Software: To operate DBMS software, a fast data processor and plenty of memory are needed.

Size: To operate them effectively, it takes up a lot of memory and storage space.

Complexity: The database system adds more requirements and complexity.

Higher Impact of Failure: Failure has a greater impact on databases since, in the majority of organisations, all data is kept in a single database. If the database is destroyed due to an electrical failure or database corruption, all data may be permanently lost.

DATABASE FILES

Data is kept in files in a Database Management System (DBMS). A database file is a group of connected records, each of which has one or more data fields.

The capacity to organise data consistently and logically is one of the main benefits of utilising database files. Intuitive and effective data access and manipulation are made possible for users as a result. In a Relational Database Management System (RDBMS), for instance, data is arranged into tables with columns and rows, making it simple to query for and retrieve certain bits of data. Contrarily, document-oriented databases arrange data as documents with nested fields and arrays, which makes it simpler to manage unstructured, complicated data.

The capacity to maintain data consistency is a key benefit of database files. Database files avoid data duplication or discrepancies by specifying a set of guidelines for how data should be kept and arranged. By ensuring that data is correct and current, this lowers mistakes and enhances the ability to make decisions.

Database files offer better data security in addition to organised data management and data consistency enforcement. Since databases allow for restricted access to data, managers can limit user access to sensitive data. They also provide user authentication and data encryption services to stop unwanted access and security breaches.

Despite the many benefits of database files, there are a few drawbacks to take into account. The expense of developing and maintaining a database is one of the biggest obstacles. Database systems may be pricey, especially for individuals or small organisations. However, setting up and managing databases requires specific technical skills, which can be difficult for someone without a background in database administration.

The systems' intricacy is another possible issue with database files. The setup and configuration of databases may be difficult and time-consuming, requiring extensive planning and design effort. Moreover, they are prone to data corruption and system failures, both of which can result in the loss of crucial information. We will go through the different kinds of database files, how they are organised, and how to access and edit them in this chapter.

Types of Database Files

Database files come in a variety of forms, each having unique properties and applications. Database files often come in one of these formats:

Relational Data: Data is stored in tables with rows and columns in relational files. Each column denotes a field of data, and each row denotes a single record. The relationships between the tables are used to arrange the relational file.

Hierarchal Files: A tree-like structure is used to arrange data in hierarchical files. One or more parent records and one or more child records are connected to each record. The relationships between the records are used to structure the records in the hierarchical structure.

Network Files: A record may have more than one parent using network files, which are equivalent to hierarchical files. This makes it possible for records to have more intricate associations.

Object-Oriental Files: Files that store data as objects with attributes and methods are said to be object-oriented files. The properties of each object stand in for a single record, and the fields of data they represent.

Organization of Database Files:

To speed up access times and maximise storage space, database files are structured into a variety of forms. These are the most typical database file organisation structures:

Sequential Files: Records are kept in a sequential file in a certain order. Data are appended to the file's end and accessed one at a time starting at the starting.

Indexed Files: An index is made in an indexed file that associates each entry with a different identifier. This makes it possible to quickly retrieve particular files' records.

Hashed Files: Datasets are assigned to specific positions in a hashed file according to a hashing algorithm. This enables quick access to particular records using a search key.

Access and Manipulation of Database Files

The DBMS offers a number of procedures to access and work with the database files. The most frequent operations include:

Insert: New records are added to the database file using the insert procedure.

Delete: Remove records from the database file using the delete procedure.

Update: Modify existing records in the database file using the update operation.

Retrieve: To obtain records from the database file, utilise the retrieve procedure.

Search: Using a search key, the search method locates particular records in the database file.

Therefore, it can be concluded that any database management system must include database files. They do it in a way that makes it easy to access and manipulate the data they hold. There are several database file formats and organisational patterns, each with certain benefits and drawbacks. Insert, delete, update, retrieve, and search are just a few of the operations that may be used to access and manipulate database files. Organizations may handle their data efficiently and base judgements on the data by comprehending the various database file formats and their organisational structures.

DATA MINING AND WAREHOUSING

Organizations acquire enormous volumes of data daily in today's data-driven environment. Yet, this information is meaningless without a thorough study. Organizations may gain useful insights from their data using two methods: data mining and data warehousing. The ideas of data mining and data warehousing, their distinctions, and their applications in businesses will all be covered below.

Data Mining

The procedure of extracting patterns, trends, and insights from huge databases is known as data mining. By seeing patterns and connections between the data, it includes drawing information from the data. To glean insights from data, data mining employs a variety of methods including machine learning, artificial intelligence, and statistical analysis. Finding hidden patterns and insights that may be utilised to make wise judgements is the main objective of data mining.

Some key characteristics of data mining include

Large datasets: Large datasets with potentially millions or billions of records are frequently analysed using data mining techniques. To manage the data's complexity and volume, specialist tools and approaches are needed.

Complex data structures: Data mining frequently works with non-tabular data types including text, photos, and audio. Techniques for assessing unstructured and semi-structured data are necessary for this.

Multidimensional analysis: Analyzing data across several dimensions, such as time, place, and client demographics, is known as data mining. As a result, patterns and insights that might not be seen from a single-dimensional perspective of the data might be found.

Machine learning: Machine learning techniques are frequently used in data mining to find patterns in the data. These algorithms are capable of automatically learning from the data and progressively improving.

Predictive modeling: Building predictive models that may foretell future trends and behaviours through data mining is feasible. These models may be applied to improve corporate operations and make well-informed judgements.

Data visualization: Data visualisation methods are frequently used in data mining to portray the data in a form that is simple to grasp and analyse. This makes it simpler for analysts to find patterns and connections in the data.

Iterative process: Data processing, model development, and assessment are all steps in the iterative process of data mining. Once the desired outcomes are obtained, this procedure may be repeated several times.

Data Warehousing

The procedure of gathering, arranging, and storing data from numerous sources in a main repository is known as data warehousing. A data warehouse's organisation of the data makes for effective querying and analysis. Data extraction from diverse sources, including databases, applications, and external sources, is followed by data transformation into a standard format and transferring into a data warehouse.

Some key characteristics of data modelling include:

Abstraction: In order to make data simpler to comprehend and handle, data modelling entails building a simplified representation of the real world. This entails defining and portraying the essential entities, connections, and features of the system being represented in a form that is simple to understand.

Structure: The categories of data, the connections between them, and the limitations that apply to them are all defined by data modelling, which also identifies the structure of data in a system. With the help of this structure, data may be stored, organised, queried, and subjected to analysis.

Flexibility: A reliable data model is adaptable enough to take into account system changes. This indicates that the model should have the flexibility to adapt as the needs of the system do.

Clarity: To ensure that the data modelling simple for others to comprehend and utilise, it should be clear and unambiguous. To do this, it is necessary to define the connections and constraints of the data being represented in detail as well as to use standardised notations and language.

Data integrity: Data consistency, accuracy, and completeness should be ensured by data modelling. To do this, it is necessary to specify the guidelines and limitations that apply to the data and to apply them by utilizing data validation and error-checking.

Scalability: Efficient data modelling will be able to handle massive amounts of data and allow sophisticated searches and analyses. This necessitates building the system to handle massive datasets and performance-enhancing data structure and indexing.

Iterative process: As new information becomes available, data modelling is an iterative process that involves adjusting and rewriting the model. To make sure that the model effectively reflects the demands of the system, collaboration is required amongst stakeholders, including developers, analysts, and end users.

Differences between Data Mining and Data Warehousing

Focus is the main distinction between data mining and data warehousing. Data warehousing focuses on storing and organising data in a way that makes efficient querying and analysis possible whereas data mining focuses on analysing data to find patterns and insights.

Data is analysed using data mining to find hidden patterns and insights that may be utilised to guide decisions. Data warehousing, on the other hand, is a method for storing data in a form that makes efficient querying and analysis possible.

Whereas data warehousing is a systematic process that involves gathering, organising, and storing data, data mining is an exploratory process that involves finding patterns and insights in data.

Uses of Data Mining and Data Warehousing:

Several businesses employ data mining and data warehousing to glean insightful information from the data. Data warehousing and mining are frequently used for the following purposes:

Marketing: To find trends and insights in consumer data, data mining is utilised in marketing. With this data, tailored marketing efforts with a higher chance of success may be created.

Healthcare: In the healthcare industry, data mining is used to examine patient data and spot trends that may be utilised to better patient outcomes.

Retail: Data collection from several sources, including point-of-sale systems, inventory management systems, and customer loyalty programmes, is done in the retail industry by means of data warehousing. With this information, personalised marketing campaigns are created as well as inventory management and pricing optimisation.

Finance: Finance uses data mining and data warehousing to examine market data, spot patterns, and make wise investment decisions.

Data warehousing and data mining are crucial methods that let businesses get the most out of their data. Data warehousing is gathering, organising, and storing data in a way that makes efficient querying and analysis possible. Data mining entails analysing data to find patterns and insights. These methods are applied across a range of sectors to enhance decision-making, streamline operations, and create focused marketing efforts. Organizations may efficiently manage their data and make choices based on the insights gleaned from their data by comprehending the principles of data mining and data warehousing.

LESSON ROUND-UP

- Any collection of facts, numbers, or statistics that are gathered and examined with a specific goal is data. Data comes in a variety of forms, including semi-structured, unstructured, and structured data. Unstructured data does not adhere to a set format, whereas structured data does. Both structured and unstructured data components can be found in semi-structured data.

- Data structures describe how information is arranged and kept in computer systems. Arrays, linked lists, stacks, queues, and trees are the most popular types of data structures. The type of data and the operations that must be carried out on it determine which data structure should be used.
- A database management system, or DBMS, is a piece of software that controls how data is stored, retrieved, and modified. The DBMS conducts functions like data backup, recovery, and security while also giving users a way to interact with the database through an interface. MySQL, Oracle, SQL Server, and PostgreSQL are a few popular database management system.
- The data kept in a database is physically represented by database files. These documents are arranged in tables with rows and columns. Each column is a data element, and each row denotes a distinct record. The files may be kept on a hard drive or other types of storage.
- The method of obtaining valuable information from huge databases is known as data mining. To find patterns, correlations, and trends in the data, statistical and machine learning approaches are used. Data mining findings may be applied to forecasting, predictions, and decision-making.
- The procedure of gathering, storing, and managing data from many sources in a single repository is known as data warehousing. The relationships across various data pieces are reflected in the schema that was used to arrange the data. Organizations can rapidly and effectively access and analyse vast volumes of data thanks to data warehousing. Business intelligence, reporting, and analytics frequently use it.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What is a database? Explain the different levels of database.
2. What are some common data structures used in computer systems?
3. What is a Database Management System (DBMS)? What are the different categories of Database Management Users?
4. What is a database file? How is data organized within a database file?
5. What is data mining? How can it be used in decision-making?
6. What is data warehousing? What are the characteristics of data warehousing?
7. What is the difference between:
    a) Data Mining and Data Warehousing
    b) Administrator versus End User in a Database Management System.
8. How can data warehousing be used for different purposes?

Data Analytics

Lesson 11

KEY CONCEPTS

■ Data ■ Data Recovery Tools ■ Evidence ■ Internet ■ Data Protection ■ Swap Files ■ Temporary Files ■ Cache Files

Learning Objectives

To understand:

- The procedure and ethical norms associated with data recovery in the overall perspective of Data Analytics
- Function of computer forensics tools for the different file systems
- Different nuances of identification, preservation, and analysis of evidence related to Data Analytics

Lesson Outline

- Data Recovery Tools
- Data Recovery Procedures and Ethics
- Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility
- Document a Chain of Custody and its importance
- Complete time line analysis of computer files based on file creation, file modification and file access
- Recover Internet Usage Data
- Data Protection and Privacy
- Recover Swap Files/Temporary Files/Cache Files
- Introduction to Encase Forensic Edition, Forensic Toolkit
- Use computer forensics software tools to cross validate findings in computer evidence-related cases
- Lesson Round-Up
- Test Yourself
- List of Further Readings

INTRODUCTION TO DATA ANALYTICS

Data Analytics is the science of analyzing raw datasets in order to derive a conclusion regarding the information they hold. It enables us to discover patterns in the raw data and draw valuable information from them. Data analytics processes and techniques may use applications incorporating machine learning algorithms, simulation, and automated systems. The systems and algorithms work on unstructured data for human use. These findings are interpreted and used to help organizations understand their clients better, analyze their promotional campaigns, customize content, create content strategies, and develop products. Data analytics help organizations to maximize market efficiency and improve their earnings.

Process of Data Analytics

Below are the common steps involved in the data analytics method:

Step 1: Determine the criteria for grouping the data

Data can be divided by a range of different criteria such as age, population, income, or sex. The values of the data can be numerical or categorical data.

Step 2: Collecting the data

Data can be collected through several sources, including online sources, computers, personnel, and sources from the community.

Step 3: Organizing the data

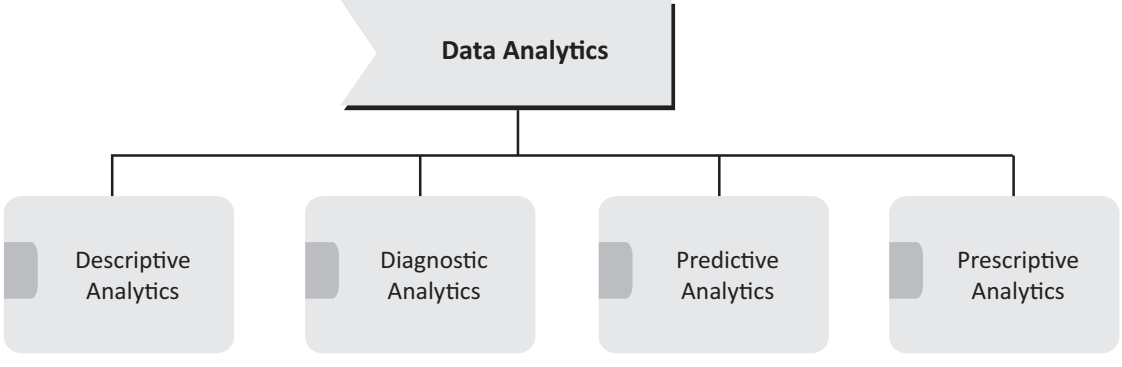
The data must be organized after it is collected so that it can be examined. Data organization can take place on a spreadsheet or other type of software that is capable of taking statistical data.

Step 4: Cleaning the data

The data is first cleaned up to ensure that there is no overlap or mistake. Then, it is reviewed to make sure that it is not incomplete. Cleaning the data helps to fix or eliminate any mistakes before the data goes to a data analyst for analysis.

Data Analytics Types

The following are the four fundamental types of data analytics:



1. **Descriptive Analytics** describes the happenings over time, such as whether the number of views increased or decreased and whether the current month's sales are better than the last one.
2. **Diagnostic Analytics** focuses on the reason for the occurrence of any event. It requires hypothesizing and involves a much more diverse dataset. It examines data to answer questions, such as "Did the weather impact the selling of beer?" or "Did the new ad strategy affect sales?"

3. **Predictive Analytics** focuses on the events that are expected to occur in the immediate future. Predictive analytics tries to find answers to questions like, what happened to the sales in the last hot summer season? How many weather forecasts expect for this year's hot summer?
4. **Prescriptive Analytics** indicates a plan of action. If the chance of a hot summer calculated as the average of the five weather models is above 58%, an evening shift can be added to the brewery, and an additional tank can be rented to maximize production.

Benefits of Data Analytics

1. **Decision-making improves**

   Companies may use the information they obtain from data analytics to guide their decisions, leading to improved results. Data analytics removes a lot of guesswork from preparing marketing plans, deciding what material to make, creating goods, and more. With advanced data analytics technologies, new data can be constantly gathered and analyzed to enhance your understanding of changing circumstances.

2. **Marketing becomes more effective**

   When businesses understand their customers better, they will be able to sell to them more efficiently. Data analytics also gives businesses invaluable insights into how their marketing campaigns work so that they can fine-tune them for better results.

3. **Customer service improves**

   Data analytics provides businesses with deeper insight into their clients, helping them to customize customer experience to their needs, offer more customization, and create better relationships with them.

4. **The efficiency of operations increases**

   Data analytics will help businesses streamline their operations, save resources, and improve the bottom line. When businesses obtain a better idea of what the audience needs, they spend less time producing advertisements that do not meet the desires of the audience.

DATA RECOVERY TOOLS

Data recovery is the process of retrieving data from a storage medium that, for some reason, cannot be accessed normally. This process may be used to recover data from a variety of storage media, such as: hard disk drives, solid-state drives, other flash storage (such as USB drives, and SD cards), or other disk storage (such as CDs, and DVDs). The damage that causes data to be lost typically falls into one of two categories: physical damage (where the hardware is damaged or is malfunctioning), or logical damage (where part of the software and/or file system prevents the data from being accessed by the host operating system.) We'll discuss these different types of storage damage in greater depth a bit later. The term "data recovery" can also be organized into two different contexts: personal data recovery, and forensic data recovery. Personal data recovery is what we normally associate with this topic. It simply refers to the retrieval of data that has been involuntarily lost or made inaccessible due to, for example, damaged storage media. By contrast, forensic data recovery often deals with retrieving data that has been purposely encrypted or hidden to prevent others (such as forensic investigators) from accessing the data.

Data recovery software is a type of software that enables the recovery of corrupted, deleted, or inaccessible data from a storage device. This software reviews, scans, identifies, extracts, and copies data from deleted, corrupted, and formatted sectors or in a user-defined location within the storage device. Data recovery software is primarily used by IT support staff and service providers. Data recovery software generally has access to the core architecture of a hard disk. It can extract data from corrupt storage devices or deleted files/folders by

referring to and accessing the file structure records/entries. Having access and control over file systems and structure, it can also un-format and repair hard drive partitions.

It can be used for both recovering user-stored and system-created data, files, and folders. It can recover data from virtually any storage device including hard disks, flash drives, external storage cards, tape drives, and more. Most data recovery software can perform data recovery on common file systems. Machine learning, also known as artificial intelligence (AI), is gaining traction when it comes to anything related to technology. AI technology is essential to any organization that regularly deals with large data sets, and high-performing companies are always searching for a way to make operations more efficient. Eventually, AI's ability to streamline the processing of large data sets through machine learning and software as a service (SaaS) will replace traditional data centers. Data recovery tools are software applications designed to retrieve data that has been lost, damaged, or corrupted. These tools can be used to recover data from a variety of sources, such as hard drives, USB drives, memory cards, and mobile devices. Data loss can occur due to a variety of reasons, such as hardware failure, human error, malware, or natural disasters. When data is lost, it can be a major setback for individuals and businesses, leading to lost productivity, revenue, and valuable information. Data recovery tools can help mitigate the effects of data loss by providing a way to recover lost data.

There are two main types of data recovery tools: free and paid. Free data recovery tools are typically limited in their functionality and may not be able to recover all types of data. These tools are often useful for simple data recovery tasks, such as retrieving accidentally deleted files. Paid data recovery tools offer more advanced functionality and can often recover data from more complex situations, such as damaged or corrupted files. These tools are typically more expensive than free tools, but they offer a higher success rate for data recovery. There are many data recovery tools available on the market, each with its own set of features and capabilities.

Here are some of the most commonly used data recovery tools:

1. **EaseUS Data Recovery Wizard:** EaseUS Data Recovery Wizard is a popular data recovery tool that can recover data from a variety of sources, including hard drives, memory cards, and USB drives. It offers both free and paid versions, with the paid version offering more advanced features such as deep scanning and advanced filtering.
2. **Recuva:** Recuva is a free data recovery tool that can recover data from hard drives, USB drives, and memory cards. It offers a user-friendly interface and the ability to preview recovered files before they are restored.
3. **Stellar Data Recovery:** Stellar Data Recovery is a paid data recovery tool that can recover data from a variety of sources, including hard drives, SSDs, and mobile devices. It offers advanced features such as disk imaging, which allows users to create a backup of their hard drives before attempting recovery.
4. **Disk Drill:** Disk Drill is a data recovery tool that can recover data from a variety of sources, including hard drives, USB drives, and memory cards. It offers both free and paid versions, with the paid version offering more advanced features such as data protection and a duplicate finder.
5. **R-Studio:** R-Studio is a paid data recovery tool that can recover data from a variety of sources, including hard drives, SSDs, and RAID systems. It offers advanced features such as disk imaging, remote data recovery, and support for virtual machines.

When using data recovery tools, it is important to follow best practices to maximize the chances of successful data recovery. Here are some tips for using data recovery tools effectively:

1. **Stop using the device:** When data is lost, it is important to stop using the device immediately to avoid overwriting the lost data. Continuing to use the device can cause further damage and decrease the chances of successful data recovery.

2. **Identify the cause of data loss:** Before attempting data recovery, it is important to identify the cause of data loss. This can help determine the best approach for data recovery and prevent further data loss.
3. **Use the appropriate data recovery tool:** Different data recovery tools are designed to handle different types of data loss. It is important to choose a data recovery tool that is appropriate for the specific type of data loss being experienced.
4. **Read user reviews:** Before using a data recovery tool, it is important to read user reviews and check the tool's reputation. This can help identify potential issues and ensure that the tool is effective for the specific type of data loss being experienced.
5. **Back up recovered data:** After data has been successfully recovered, it is important to back up the recovered data to prevent future data loss. This can be done by creating a backup on an external hard drive or cloud storage.
6. **Consider professional data recovery services:** In some cases, data recovery tools may not be able to recover lost data. In these situations, it may be necessary to seek professional data recovery services. These services are typically more expensive than using data recovery tools, but they offer a higher success rate for data recovery.

In conclusion, data recovery tools are essential tools for individuals and businesses to recover lost or damaged data. When using these tools, it is important to follow best practices to maximize the chances of successful data recovery. Whether using a free or paid data recovery tool, it is important to choose a tool that is appropriate for the specific type of data loss being experienced and to back up recovered data to prevent future data loss.

There are seven data analysis tools mentioned below in terms of learning, and performance:-

i. **Tableau Public**

It is a free data visualization application that links to any data source you can think of whether it's a corporate Data Warehouse, Microsoft Excel, or web-based information. It also generates data visualizations, maps, dashboards, and so on, all with real-time changes that are shown on the web. These may also be shared on social media or with your customer, and you can download the files in several formats. However, it truly shines when you have an excellent data source. That's when you realize Tableau's ultimate potential. Tableau's Big Data features make it indispensable. Its approach to data analysis and visualization is considerably better than that of any other data visualization software on the market.

ii. **R Programming**

Well, R is the industry's premier analytics tool, and it's extensively used for statistics and data modeling. It can readily alter data and show it in a variety of formats. It has outperformed SAS in several aspects, including data capacity, performance, and results. R may be compiled and run on a broad range of systems, including Windows, UNIX, and macOS. It offers 11,556 packages and lets you explore them by category. Also, R has tools for installing all packages automatically based on user needs, which may be used with Big Data.

iii. **Python**

It's a scripting language that is simple to understand, write, as well as maintain. Furthermore, it's a free open-source tool. Guido van Rossum developed it in the late 1980s and it supports both structured and functional programming methodologies. Python is simple to learn since it is related to Ruby, JavaScript, and PHP. Python also contains excellent machine-learning packages such as Tensorflow, Theano, Scikitlearn, and Keras. Another useful characteristic of Python is that it can be built on any platform, such as a MongoDB database, SQL browser, or JSON. It also excels at handling text data.

iv. Apache Spark

Apache was created in 2009 by the AMP Lab at the University of California, Berkeley. Apache Spark is a large-scale data processing engine that performs applications hundred times quicker when it comes to memory and 10 times faster on disk in Hadoop clusters. It is based on data science, and its design makes data science simple. Spark is also popular for developing data pipelines and machine learning models. Spark also contains the MLlib package, which provides a progressive collection of machine algorithms for recurring data science procedures like classification, collaborative filtering, regression, clustering, and so on.

v. SAS

SAS is basically a data manipulation programming ecosystem and language that is a market leader in analytics. The SAS Institute created it in 1966, and it was expanded upon in the 1980s as well as the 1990s. It is simple to use and administer, and it can analyze data from any source. In 2011, SAS released a significant collection of solutions for customer intelligence, as well as numerous SAS modules for social media, online, and marketing analytics. These are now often used to profile clients and prospects. It can also forecast their actions and manage and improve communications.

vi. Excel

Excel is a popular, basic, and frequently leveraged analytical tool in practically all industries. Whether you are a Sas, R, or Tableau specialist, you will still need to utilize Excel. When analytics on the client's internal data is required, Excel comes in handy. It analyzes the hard work of summarizing the data with a preview of pivot tables, which aids in filtering the data according to the client's needs. Excel includes a sophisticated business analytics feature that aids in modeling skills. It has prebuilt tools such as automated relationship recognition, DAX measure generation, and time grouping.

vii. RapidMiner

It is an extremely capable comprehensive data analysis tool. It's created by the same house that does predictive analysis as well as other advanced analytics such as machine learning, text analysis, visual analytics, and data mining without the use of programming. RapidMiner supports all data source types, including Microsoft SQL, Excel, Access, Oracle, Teradata, Dbase, IBM SPSS, MySQL, Ingres, IBM DB2, Sybase, and others. This tool is quite powerful, as it can provide analytics based on real-world data transformation settings, allowing you to customize the data sets and formats for predictive analysis.

DATA RECOVERY PROCEDURES AND ETHICS

The digital revolution has made our life a lot easier. Digital technology has evolved to become an indispensable part of our daily lives and businesses. Today, in this digital era, information is more accessible to people than ever before. However, despite plenteous benefits, now corporate entities and individual consumers have started recognizing the risks inherent in digital services. The digital economy collects, combine and share data which has come with challenges like loss of the control to personal privacy, compromised data and other cyberspace crimes. Thus, in the digital age, the risk of unethical or even illegal use of consumers' data without their consent can permanently damage consumers' trust in a brand. Therefore, it has become crucial that the digital economy addresses these issues, along with cyber-security threats. Ethics is the key to preventing these types of internal, as well as, external threats.

Digital Ethics

Digital ethics is defined as the field of study concerned with the manner in which digital technology is shaping our political, social ,and moral well-being. In a broader sense, this field deals with the impact of digital Information and Communication Technologies (ICT) on our societies and the environment.

Role of Digital Ethics in Data Storage

The digital advancements have undoubtedly enhanced the business opportunities for companies by enabling them to compete and thrive. However, they must realize and strive toward transparent operations, ethical practices, and protection of privacy. Similar to any other field of work like medicine or accounts, the IT sector also needs a strict set of codes and ethics. The strict guidelines will ensure more stringent legal requirements. Presently, in IT the codes of ethics are not as standard as in other professional careers which makes it difficult to regulate them. CRM tools and other software are immensely useful to collect volumes of data from clients. This has made it necessary to implement ethical guidelines to decide what to do with that data. Companies need to draw a line between what information is ethical to collect and what violates the privacy of clients.

Data Recovery Ethics

When dealing with a massive amount of data, often companies suffer data loss which needs to get recovered. For the purpose of data recovery, companies mostly depend on third parties. Whenever it happens, the data of clients are put at risk if the third-party data recovery service doesn't take the security of clients' data seriously. To make sure that the files are kept safe and confidential during the recovery process, the ethical data recovery company follows ethical safeguard rules and practices, such as secure servers, reliable access protocols, and smart data return policies, etc. Therefore, with great benefits comes great responsibility. It is necessary to establish guidelines and uphold ethical digital practices to build digital trust while reaping the benefits of this revolutionary technology.

There are some common scenarios where data recovery procedures would be necessary:

1. There has been an operating system failure or some critical operating system files have been damaged, causing the device to not be able to boot up properly. In this case, a simple solution would be to use a Live USB to boot up from another operating system so that you can access the data from the storage medium.
2. There has been a hard disk failure and there is physical damage to the storage medium. In this case, you may be able to repair the hardware, but the storage medium is often beyond repair and the focus is more on a one-time recovery in an attempt to salvage any data you can. This will often require the services of a specialized data recovery company.
3. Files have been deleted from a storage medium. As we will discuss later in the presentation, when an operating system "deletes" files, oftentimes the data is not immediately removed from the drive. This allows tools such as file carvers to recover this data.

There are three research methods of data recovery namely, Direct-to-cloud backup, cloud-to-cloud backup, and SaaS backup. With direct-to-cloud, offsite file backups are copied directly to the cloud, bypassing the need for a local device. Cloud-to-cloud backup is the process of copying data from one cloud to another cloud. SaaS backup refers to backing up data created in SaaS applications such as Microsoft 365 or Google G Suite.

Types of Data Recovery

Not all data loss scenarios are the same, so it is important to choose a backup solution that addresses a wide range of restore and recovery needs and reduces data recovery steps:

- **File Restore:** A file restore is exactly what it sounds like—the process of replacing a lost file or files from a backup to its primary location. With SIRIS, an administrator can mount a recovery point, view the protected system's file structure, locate the necessary files, and restore them back to the primary system. If you only need to retrieve a file or a small number of files, this is the ideal restore type.

- **Volume Restore:** When you perform a volume restore on SIRIS, the contents of the chosen recovery point are shared as an iSCSI target. This restore type retrieves files and folders with permissions intact and is used to restore large numbers of files when a bare metal restore is not necessary (i.e., the physical server is intact and operating correctly).
- **Bare metal restores:** This is the process of restoring an entire system image (the protected machine's data, applications, settings, and operating system) from a backup to a new physical server. "Bare metal" refers to the new system's unused, unconfirmed hardware. Bare metal restore is used when a primary server fails, is damaged, or is otherwise rendered inoperable.
- **Local virtualization:** Local virtualization is a feature of BCDR solutions that offers fast recovery of business operations. Local virtualization uses hypervisor technology to boot a virtual server from a snapshot on the backup device. This enables businesses to continue normal business operations while the primary server is restored (using one of the methods above). Local virtualization nearly eliminates costly business downtime. Sometimes, this functionality is known as Instant Virtualization.
- **Cloud virtualization:** Cloud virtualization refers to the process outlined above, but in the cloud rather than on a local backup device. Some BCDR solutions can create a tertiary cloud copy of backup server images. In the event that both the primary and backup servers are inoperable, say because of a fire or flood, business operations can be continued on the cloud backup server image.

Business continuity/disaster recovery (BCDR)

BCDR solutions are designed to enable fast restores that minimize business downtime. To do so, these solutions use snapshot and virtualization technologies to create and store bootable virtual server images on a backup device or in the cloud. In the event of a primary server failure or other outage, business operations are "failed over" to the backup device or cloud while the primary server is being restored, repaired, or replaced. Once the primary server is back up and running, operations are "failed back" to the primary device. BCDR recovery times are typically measured in minutes rather than the hours or even days required of traditional backup tools. BCDR solutions have become popular with businesses of all sizes, but are probably most beneficial for small to medium businesses (SMBs).

GATHERING EVIDENCE- PRECAUTIONS, PRESERVING AND SAFELY HANDLING ORIGINAL MEDIA FOR ITS ADMISSIBILITY

Digital forensics is a process of identifying, preserving, analyzing, and documenting digital evidence; it helps in presenting evidence in a court of law when required. It is to be systematic in a very specific way, that is:

Identification: It is a process to identify where the attacker has stored the data or evidence.

Preservation: The data and evidence are kept secured and preserved; so that they cannot tamper with.

Analysis: This is the process of recreating fragments of data and drawing conclusions based on the evidence found therein.

Documentation: It includes the creation of records of the data, for the recreation of the crime scene.

Presentation: The last step includes summaries and drawing a conclusion based on the data collected.

When collecting digital evidence investigators should maintain a proper and well-documented chain of custody to ensure any evidence collected does not lose its integrity. Different devices should be handled in a specific manner depending on how data is stored on the device.

If mobile devices must be submitted to a lab they should be turned off in order to preserve the cell tower location. This step not only prevents the phone from being used but also prevents remote destruction commands. The

device should be put in a Faraday bag to prevent network interaction from potentially altering data on the device.

Devices that cannot be turned off can instead be placed on airplane mode or disable any Wi-Fi or Bluetooth capabilities. If it is necessary to keep the device powered on, connect it to an external power source such as a portable battery pack. Devices that are found turned off should be left off and their model number, carrier, and unique identifiers should be documented.

Forensic investigators who encounter computers at a scene should prevent any alteration of evidence during collection. They should first document any activity on the computer, components, or devices by screenshotting and recording any information on the screen. If any destructive software is running on the computer, the power must be immediately disconnected to preserve the evidence.

Investigators that have been appropriately trained can also collect digital evidence at the scene. By using tools that help them identify which electronic devices contain evidence related to their case. The ability to preview digital evidence at the scene can save investigators time and resources. Investigators must make duplicate copies of the content contained on devices to maintain the integrity of the primary source of evidence. The data obtained should not be altered or modified.

The simple reasons for collecting evidence are:

- *Future Prevention*: Without knowing what happened, you have no hope of ever being able to stop someone else from doing it again.
- *Responsibility:* The attacker is responsible for the damage done, and the only way to bring him to justice is with adequate evidence to prove his actions. The victim has a responsibility to the community. Information gathered after a compromise can be examined and used by others to prevent further attacks.

Collection Options

Once a compromise has been detected, you have two options:

- Pull the system off the network and begin collecting evidence: In this case, you may find that you have insufficient evidence or, worse, that the attacker left a dead man's switch which destroys any evidence once the system detects that it's offline.
- Leave it online and attempt to monitor the intruder: you may accidentally alert the intruder while monitoring and cause him to wipe his tracks in any way necessary, destroying evidence as he goes.

Obstacles

- Computer transactions are fast, they can be conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsibly.
- Any paper trail of computer records they may leave can be easily modified or destroyed or maybe only temporarily.
- Auditing programs may automatically destroy the records left when computer transactions are finished with them.
- Investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously.
- The best we can do is follow the rules of evidence collection and be as assiduous as possible.

Volatile Evidence

The field of computer Forensics Analysis involves identifying, extracting, documenting, and preserving information that is stored or transmitted in an electronic or magnetic form (that is, digital evidence). The volatile data that is held in temporary storage in the system's memory (including random access memory, cache memory, and the onboard memory of system peripherals such as the video card or NIC) is called volatile data because the memory is dependent on electric power to hold its contents. Volatile data is the data that is usually stored in cache memory or RAM. This volatile data is not permanent this is temporary and this data can be lost if the power is lost i.e., when computer loses its connection. During any cyber crime attack, investigation process is held in this process data collection plays an important role but if the data is volatile then such type of data should be collected immediately. Volatile information can be collected remotely or onsite. If there are many numbers of systems to be collected then remotely is preferred rather than onsite. It is very important for the forensic investigation that immediate state of the computer is recorded so that the data does not lose as the volatile data will be lost quickly. If the volatile data is lost on the suspects computer if the power is shut down, Volatile information is not crucial but it leads to the investigation for the future purpose. To avoid this problem of storing volatile data on a computer we need to charge continuously so that the data isn't lost. So that computer doesn't lose data and forensic expert can check this data sometimes cache contains Web mail. This volatile data may contain crucial information.so this data is to be collected as soon as possible. This process is known "Live Forensics".

The final step in evidence assessment specifically deals with the evidence itself. You should identify the stability of the evidence, and collect the most volatile evidence first before moving to nonvolatile evidence. In doing so, you should prioritize the collection and acquisition of evidence so that the evidence that is most likely to contain what you're searching for is examined first. There are different examples of an order of volatility like Registers and cache, Routing tables, Arp cache, Process table, Kernel statistics and modules, Main memory, Temporary file systems, Secondary memory, Router configuration & Network topology.

Methods of Collection

There are two basic forms of collection: freezing the scene and honey potting.

Freezing the Scene

- It involves taking a snapshot of the system in its compromised state. You should then start to collect whatever data is important onto removable non-volatile media in a standard format.
- All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.

Honey Potting

- It is the process of creating a replica system and luring the attacker into it for further monitoring.
- The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.

Artifacts

- There is almost always something left behind by the attacker be it code fragments, trojan programs, running processes, or sniffer log files. These are known as artifacts.
- Never attempt to analyze an artifact on the compromised system.
- Artifacts are capable of anything, and we want to make sure their effects are controlled.

Collection Steps

1. Find the Evidence: Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.
2. Find the Relevant Data: Once you've found the evidence, you must figure out what part of it is relevant to the case.
3. Create an Order of Volatility: The order of volatility for your system is a good guide and ensures that you minimize the loss of uncorrupted evidence.
4. Remove external avenues of change: It is essential that you avoid alterations to the original data.
5. Collect the Evidence: Collect the evidence using the appropriate tools for the job.
6. Document everything: Collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important.

Controlling Contamination: The Chain of Custody

Once the data has been collected, it must be protected from contamination. Originals should never be used in the forensic examination; verified duplicates should be used. A good way of ensuring that data remains uncorrupted is to keep a chain of custody. This is a detailed list of what was done with the original copies once they were collected. Analysis

- Once the data has been successfully collected, it must be analyzed to extract the evidence you wish to present and to rebuild what actually happened.

Time

- To reconstruct the events that led to your system being corrupted, you must be able to create a timeline.
- Never, ever change the clock on an affected system. Forensic Analysis of Back-ups When we analyze back-ups, it is best to have a dedicated host for the job. We need a dedicated host which is secure, clean, and isolated from any network for analyzing backups.
- Document everything you do. Ensure that what you do is repeatable and capable of always giving the same results.

Reconstructing the Attack

After collecting the data, we can attempt to reconstruct the chain of events leading to and following the attacker's break-in. We must correlate all the evidence we have gathered. Include all of the evidence we've found when reconstructing the attack---no matter how small it is.

Searching and Seizing

There is no one methodology for performing a computer forensic investigation and analysis. There are too many variables for it to be just one way. Some of the typical variables that come to mind include operating systems; software applications; cryptographic algorithms and applications; and hardware platforms. But moving beyond these obvious variables spring other equally challenging variables: law, international boundaries, publicity, and methodology.

There are a few widely accepted guidelines for computer forensic analysis:

- A computer forensic examiner is impartial. Our job is to analyze the media and report our findings with no presumption of guilt or innocence.

- The media used in computer forensic examinations must be sterilized before each use.
- A true image (bit stream) of the original media must be made and used for the analysis.
- The integrity of the original media must be maintained throughout the entire investigation.

Before the Investigation

- For the sake of the first argument, you must have skilled technicians in-house and a top-notch lab with the right equipment, the right computer forensic tools, and so on.
- District attorneys may require more documentation on the chain of evidence handling.
- When you have a case arise, you know what is required and can work the case from the inception in support of these requirements.

Methodology Development

- Define your methodology, and work according to this methodology.
- Here methodology defines a method, a set of rules: guidelines that are employed by a discipline.

The chain of evidence is so important in computer forensic investigations. If resources allow, have two computer forensic personnel assigned to each case every step of the way. Important in the documentation are the times that dates steps were taken; the names of those involved; and under whose authority were the steps taken.

Evidence Search and Seizure

Prior to search and seizure, you already have the proper documents filled as well as permission from the authority to search and seize the suspect's machine.

Step 1: Preparation

You should check all media that is to be used in the examination process. Document the wiping and scanning process. Check to make sure that all computer forensic tools are licensed for use and that all lab equipment is in working order.

Step 2: Snapshot

We should photograph the scene, whether it is a room in a home or in a business. You should also note the scene. Take advantage of your investigative skills here. Note pictures, personal items, and the like. Photograph the actual Evidence. For example, the evidence is a PC in a home office. Take a photograph of the monitor. Remove the case cover carefully and photograph the internals.

Step 3: Transport

If you have the legal authority to transport the evidence to your lab, you should pack the evidence securely. Photograph/videotape and document the handling of evidence leaving the scene to the transport vehicle and from the transport vehicle to the lab examination facility.

Step 4: Examination

You should prepare the acquired evidence for examination in your lab. There are many options to on what tool to use to image the drive. You could use EnCase, the Unix command DD, ByetBack, or also SafeBack. It is wise to have a variety of tools in your lab. Each of these tools has its respective strengths. The important note to remember here is: Turn off virus-scanning software. We must record the time and date of the COMS. Do not boot the suspect machine. When making the image, make sure that the tool you use does not access the file system of the target evidence media. After making the image, seal the original media in an electrostatic-safe container, catalogue it, and initial the container. Finally, the examination of the acquired image begins.

DUPLICATION AND PRESERVATION OF DIGITAL EVIDENCE

Preserving the Digital Crime Scene

- After securing the computer, we should make a complete bitstream backup of all computer data before it is reviewed or processed.
- Bit stream backups are much more thorough than standard backups.
- They involve copying of every bit of data on a storage device, and it is recommended that two such copies be made of the original when hard disk drives are involved.
- Any processing should be performed on one of the backup copies.
- IMDUMP was the first software for taking bit stream back-ups developed by Michael White.

SafeBack

- SafeBack has become a law enforcement standard and is used by numerous government intelligence agencies, military agencies, and law enforcement agencies worldwide.
- SafeBack program copies and preserves all data contained on the hard disk. Even it goes so far as to circumvent attempts made to hide data in bad clusters and even sectors with invalid CRCs.

SnapBack

- Another bit steam backup program, called SnapBack, is also available and is used by some law enforcement agencies primarily because of its ease of use.
- Its prices are several hundred dollars higher than SafeBack.
- It has error-checking built into every phase of the evidence backup and restoration process.
- The hard disk drive should be imaged using specialized bit stream backup software.
- The floppy diskettes can be imaged using the standard DOS DISKCOPY program.
- When DOS DISKCOPY is used, it is recommended that the MS-DOS Version 6.22 be used and the (data verification) switch should be invoked from the command line.
- Know and practice using all of your forensic software tools before you use them in the processing of computer evidence.
- We may only get one chance to do it right.

Computer Evidence Processing Steps

There really are no strict rules that must be followed regarding the processing of computer evidence. The following are general computer evidence processing steps:

1. **Shut down the computer**

   Depending on the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved. Generally, time is of the essence, and the computer system should be shut down as quickly as possible.

2. **Document the hardware configuration of the system**

   Before dismantling the computer, it is important that pictures are taken of the computer from all angles

to document the system hardware components and how they are connected. Labeling each wire is also important so that it can easily be reconnected when the system configuration is restored to its original condition at a secure location.

3. Transport the computer system to a secure location. A seized computer left unattended can easily be compromised. Don't leave the computer unattended unless it is locked up in a secure location.
4. Make bit stream backups of hard disks and floppy disks. All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. Bit stream backups are much like an insurance policy and are essential for any serious computer evidence processing.
5. Mathematically authenticate data on all storage devices. You want to be able to prove that you did not alter any of the evidence after the computer came into your possession. Since 1989, law enforcement and military agencies have used a32- bit mathematical process to do the authentication process.
6. Document the system date and time: If the system clock is one hour slow because of daylight-saving time, then file timestamps will also reflect the wrong time. To adjust for these inaccuracies, documenting the system date and time settings at the time the computer is taken into evidence is essential.
7. Make a list of key search words. It is all but impossible for a computer specialist to manually view and evaluate every file on a computer hard disk drive. Gathering information from individuals familiar with the case to help compile a list of relevant keywords is important. Such keywords can be used in the search of all computer hard disk drives and floppy diskettes using automated software.
8. Evaluate the Windows swap file. The Windows swap file is a potentially valuable source of evidence and leads. When the computer is turned off, the swap file is erased. But the content of the swap file can easily be captured and evaluated.
9. Evaluate file slack: It is a source of significant security leakage and consists of raw memory dumps that occur during the work session as files are closed. File slack should be evaluated for relevant keywords to supplement the keywords identified in the previous steps. File slack is typically a good source of Internet leads. Tests suggest that file slack provides approximately 80 times more Internet leads than the Windows swap file.
10. Evaluate unallocated space (erased files). Unallocated space should be evaluated for relevant keywords to supplement the keywords identified in the previous steps.
11. Search files, file slack, and unallocated space for keywords. The list of relevant keywords identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes. It is important to review the output of the text search utility and equally important to document relevant findings.
12. Document file names, dates, and times. From an evidence standpoint, file names, creation dates, and last modified dates and times can be relevant. The output should be in the form of a word-processing-compatible file that can be used to help document computer evidence issues tied to specific files.
13. Identify file, program, and storage anomalies. Encrypted, compressed, and graphic files store data in binary format. As a result, text data stored in these file formats cannot be identified by a text search program. Manual evaluation of these files is required. Depending on the type of file involved, the contents should be viewed and evaluated for their potential as evidence.
14. Evaluate program functionality. Depending on the application software involved, running programs to learn their purpose may be necessary. When destructive processes that are tied to relevant evidence are discovered, this can be used to prove wilfulness.

15. Document your findings. It is important to document your findings as issues are identified and as evidence is found. Documenting all of the software used in your forensic evaluation of the evidence, including the version numbers of the programs used, is also important. Be sure you are legally licensed to USE the forensic software. Screen prints of the operating software also help document the version of the software and how it was used to find or process the evidence.

16. Retain copies of the software used. As part of your documentation process, it is recommended that a copy of the software used to be included with the output of the forensic tool involved. Duplication of results can be difficult or impossible to achieve if the software has been upgraded and the original version used was not retained.

LEGAL ASPECTS OF COLLECTING AND PRESERVING COMPUTER

Forensic Evidence

Definition

- A chain of custody is a roadmap that shows how evidence was collected, analyzed, and preserved in order to be presented as evidence in court.
- Preserving a chain of custody for electronic evidence requires proving that:
  - No information has been added or changed.
  - A complete copy was made.
  - A reliable copying process was used.
  - All media was secured.

Legal Requirements

- When evidence is collected, certain legal requirements must be met. These legal requirements are vast, and complex, and vary from country to country.
- CERT Advisory CA-1992-19 suggests the following text be tailored to a corporation's specific needs under the guidance of legal counsel:
- This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
- In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
- Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.
- The legality of workplace monitoring depends primarily on whether employment policies exist that authorize monitoring and whether that policy has been clearly communicated to employees.
- To prove that the policy has been communicated, employees should sign a statement indicating that they have read, understood, and agreed to comply with corporate policy and consent to system monitoring.

Evidence Collection Procedure

When the time arrives to begin collecting evidence, the first rule that must be followed is Do not rush.

- The investigation team will need a copy of their incident-handling procedure, an evidence collection notebook, and evidence identification tags.
- They may also need to bring tools to produce reliable copies of electronic evidence, including media to use in the copying process.
- In some cases, legal counsel will want photographs of the system prior to search and seizure. Then include a Polaroid camera in the list of tools.

The Incident Coordinator

Policy and procedure should indicate who is to act as incident coordinator.

The Incident Coordinator

- will contact the other members of the response team as outlined in the Incident Response Policy, when an incident is reported.
- will be responsible for ensuring that every detail of the incident-handling procedure is followed, upon arrival at the incident site.
- will assign team members the various tasks outlined in the incident-handling procedure.
- serve as the liaison to the legal team, law enforcement officials, management, and public relations personnel.

Ultimate responsibility for ensuring that evidence is properly collected and preserved and that the chain of custody is properly maintained, belongs to the incident coordinator.

The Evidence Notebook

- One team member will be assigned the task of maintaining the evidence notebook.
- This person will record who, what, where, when, and how of the investigation process. At a minimum, items to be recorded in the notebook include the following task.
    a) Who initially reported the suspected incident along with the time, date, and circumstances surrounding the suspected incident?
    b) Details of the initial assessment leading to the formal investigation.
    c) Names of all persons conducting the investigation.
    d) The case number of the incident.
    e) Reasons for the investigation.
    f) A list of all computer systems included in the investigation, along with complete system specifications. Also include identification tag numbers assigned to the systems or individual parts of the system.
    g) Network diagrams.
    h) Applications running on the computer systems previously listed.
    i) A copy of the policy or policies that relate to accessing and using the systems previously listed.

j) A list of administrators responsible for the routine maintenance of the system.

k) A detailed list of steps used in collecting and analyzing evidence. Specifically, this list needs to identify the date and time each task was performed, a description of the task, who performed the task, where the task was performed, and the results of the analysis.

l) An access control list of who had access to the collected evidence at what date and time.

- A separate notebook should be used for each investigation. It should be bound in such a way that it is obvious if a page or pages have been removed.
- This notebook is a crucial element in maintaining the chain of custody. Therefore, it must be as detailed as possible to assist in maintaining this chain.

Evidence Collection

- Another team member (or members) will be assigned the task of evidence collection.
- To avoid confusion, the number of people assigned to this task should be kept to a minimum.
- This member (or members) should also be highly proficient with copying and analysis tools.
- This person will tag all evidence and work with the person responsible for the evidence notebook to ensure that this information is properly recorded.
- Next, the person will also be responsible for making a reliable copy of all data to be used as evidence.
- The data will include complete copies of drives on compromised or suspect systems, as well as all relevant log files.
- This can be done on-site or the entire system can be moved to a forensics lab, as needs dictate.
- A binary copy of the data is the proper way to preserve evidence.
- A reliable copy process has three critical characteristics.
- The process must meet industry standards for quality and reliability.
- The copies must be capable of independent verification.
- The copies must be tamperproof.
- Once all evidence is collected and logged, it can be securely transported to the forensics lab.
- A detailed description of how data was transported and who was responsible for the transport, along with the date, time, and route, should be included in the log. Storage and Analysis of Data.
- The lab must provide some form of access control; a log should be kept detailing the entrance and exit times of all individuals.
- It is important that evidence never be left in an unsecured area.
- If a defense lawyer can show that unauthorized persons had access to the evidence, it could easily be declared inadmissible.

As analysis of evidence is performed, investigators must log the details of their actions in the evidence notebook. The following should be included at a minimum:

- The date and time of analysis.
- Tools used in performing the analysis.

- Detailed methodology of the analysis.
- Results of the analysis.
- Finally, once all evidence has been analyzed and all results have been recorded in the evidence notebook, a copy of the notebook should be made and given to the legal team.
- If the legal team finds that sufficient evidence exists to take legal action, it will be important to maintain the chain of custody until the evidence is handed over to the proper legal authorities.
- Legal officials should provide a receipt detailing all of the items received for entry into evidence.

COMPUTER IMAGE VERIFICATION AND AUTHENTICATION

Special Needs of Evidential Authentication

- During an investigation, it is decided that evidence may reside on a computer system.
- It may be possible to seize or impound the computer system, but this risks violating the basic principle of innocent until proven guilty, by depriving an innocent party of the use of his or her system.
- It should be perfectly possible to copy all the information from the computer system ina manner that leaves the original system untouched and yet makes all contents available for forensic analysis.
- The courts may rightly insist that the copied evidence is protected from either accidental or deliberate modification and that the investigating authority should prove that this has been done. Thus, it is not the content that needs protection, but its integrity.
- A secure method of determining that the data has not been altered by even a single bit since the copy was taken.
- A secure method of determining that the copy is genuinely the one taken at the time and on the computer in question.
- These elements are collectively referred to as the Digital Image Verification and Authentication Protocol.

DIGITAL IDS AND AUTHENTICATION TECHNOLOGY

- Without an assurance of the software's integrity, and without knowing who published the software, it's difficult for customers to know how much to trust the software. It's difficult to make the choice of downloading the software from the Internet.
- For example (when using Microsoft Authenticode coupled with Digital IDs™ fromVeriSign®), through the use of digital signatures, software developers are able to include information about themselves and their code with their programs.
- When customers download software signed with Authenticode and verified byVeriSign, they should be assured of the content source, indicating that the software really comes from the publisher who signed it, and content integrity, indicating that the software has not been altered or corrupted since it was signed.

Authenticode

- Microsoft Authenticode allows developers to include information about themselves and their code with their programs through the use of digital signatures.
- Through Authenticode, the user is informed

- Of the true identity of the publisher
- Of a place to find out more about the control
- The authenticity of the preceding information
- Users can choose to trust all subsequent downloads of software from the same publisher and all software published by commercial publishers that have been verified by VeriSign.

Public Key Cryptography

- In public key cryptographic systems, every entity has two complementary keys (a public key and a private key) that function only when they are held together.
- Public keys are widely distributed to users, whereas private keys are kept safe and only used by their owners.
- Any code digitally signed with the publisher's private key can only be successfully verified using the complementary public key.
- Code that was successfully verified using the publisher's public key, could only have been digitally signed using the publisher's private key and has not been tampered with.

Certificate Authorities (CA)

- Certification Authorities such as VeriSign are organizations that issue digital certificates to applicants whose identity, they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it.

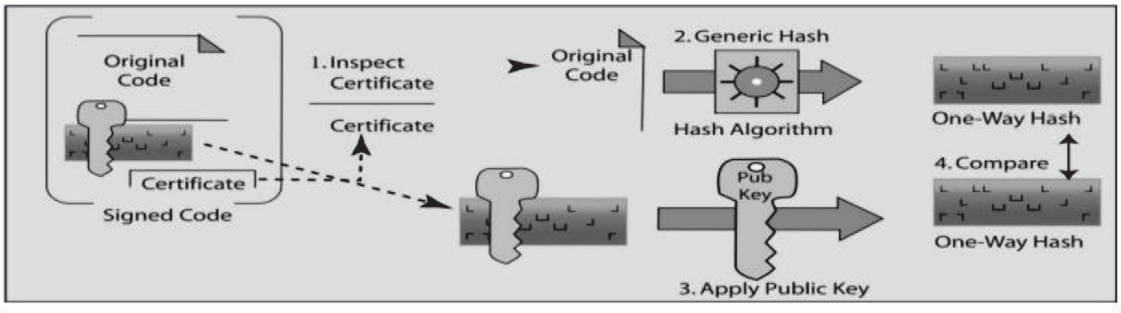
VeriSign has the following responsibilities:

1. Publishing the criteria for granting, revoking, and managing certificates;
2. Granting certificates to applications who meet the published criteria;
3. Managing certificates;
4. Storing VeriSign's root keys in an exceptionally secure manner;
5. Verifying evidence submitted by applicants;
6. Providing tools for enrolment;
7. Accepting the liability associated with these responsibilities;
8. Time-stamping digital signatures.

Digital ID

- A Digital ID/Certificate is a form of electronic credentials for the Internet.
- A Digital ID is issued by a trusted third party to establish the identity of the ID holder.
- The third party who issues certificates is known as a Certificate Authority (CA).
- Digital ID technology is based on the theory of public key cryptography.
- The purpose of a Digital ID is to reliably link a public/private key pair with its owner.
- When a CA such as VeriSign issues a Digital ID, it verifies that the owner is not claiming a false identity.
- When a CA issues you a digital certificate, it puts its name behind the statement that you are the rightful owner of your public/private key pair.

How Authenticode works with VeriSign Digital IDs?



Authenticode: Verisign Digital ID Process

1. Publisher obtains a Software Developer Digital ID from VeriSign.
2. Publisher creates code.
3. Using the SIGNCODE.EXE utility, the publisher.
4. The end user encounters the package.
5. The end user's browser examines the publisher's Digital ID. Using the VeriSign root Public Key, which is already embedded in Authenticode-enabled applications, the end user browser verifies the authenticity of Software Developer Digital ID (which is itself signed by the VeriSign root Private Key).
6. Using the publisher's public key contained within the publisher's Digital ID, the end user browser decrypts the signed hash.
7. The end browser runs the code through the same hashing algorithm as the publisher, creating a new hash.
8. The end user browser compares the two hashes. If they are identical, the browser messages that the content has been verified by VeriSign, and the end user has the confidence that the code was signed by the publisher identified in the Digital ID, and the code hasn't been altered since it was signed.

Time Stamping: Because key pairs are based on mathematical relationships that can theoretically be "cracked" with a great deal of time and effort, it is a well-established security principle that digital certificates should expire.

DOCUMENT A CHAIN OF CUSTODY AND ITS IMPORTANCE

Evidence Collection

The Investigator needs to make sure that evidence must be collected in a systematic and careful manner. The process of evidence collection begins with the preliminary crime scene survey/walk-through, followed by a determination of the evidence collection sequence to be used. There are various methods that can be adopted for evidence collection based on the type of crime scene. The evidence collection sequence may be based on the following information:

- *The scene location:* whether the crime has occurred inside premises or within a vehicle or it is an exterior one.
- *The condition of the evidence:* the condition of evidence (Whether the evidence is fragile or stable) plays an important role in choosing which evidence collection method is to be used.

- Weather conditions which might affect the scene or evidence within.
- Scene management considerations that may alter or contaminate the evidence.

Investigators should use the appropriate equipment when collecting evidence. Equipment that is required for the collection of evidence must be sterile so as to avoid contamination of evidence. Various equipment is used to collect evidence. A few of them are named below:

1. Latex gloves/nitrile gloves (N-DEX, non-latex): - helps in preventing contamination as well as any kind of hazardous exposure to the hands of personnel collecting evidence.
2. Forceps- Forceps and similar tools may have to be used to pick up small items.
3. Tweezers
4. Scalpels
5. Swabs
6. Paper bags
7. Plastic bags
8. Cardboard boxes
9. Wrapping paper
10. Hand tools
11. Thermometer

Evidence Marking and Packaging

Evidence collected from the scene of a crime or received during the investigation of crime scene should be cataloged and packaged before leaving the scene to prevent loss or cross-contamination. Mark the item of evidence when possible. Evidence which cannot be marked, such as soil, hair, and stains, should be placed in an appropriate container or envelope. An important point that is to be kept in mind is that the evidence marked directly might result in interference with the forensic analysis and hence marking should always be done on the outer packaging. When marking evidence directly, include the following:

- Case number
- Item number
- Date recovered or received
- Investigator's initials

Evidence that has been inventoried, marked, and prepared for submittal (or to be returned to the investigating agency) is packaged in an appropriate container and labeled per agency protocol. A trained investigator or evidence collector arrives at the crime scene with all types of packaging materials and tools ready to encounter any type of situation. In order to prevent any change in evidence, the evidence must be packaged carefully. The type of packaging depends on the type of evidence. The evidence must be properly packaged, properly labeled, and sealed with appropriate initials to maintain the chain of custody. The evidence must be packaged in its original condition as it is found at the crime scene. The objects with the trace evidence must be sent as a whole unless it is not possible to transport the whole item such as a wall. As sometimes it takes a long time for a crime lab to process the evidence so it is necessary that the evidence must be packaged in such a manner that the conditions such as evaporation, breakage, etc. should not change its condition. While packaging the chances of cross-contamination must be ended. Each item must be packaged in a separate container. Every

package must be labeled with all the essential details such as Case FIR No., Item No., Type of Evidence (fragile/ stable), etc. After labeling the package must be sealed with evidence tape. Take the entire piece of evidence as it is found on the crime scene, if possible. New and unused packaging materials should be used. Evidence must be sealed using proper methods which prevent tampering. For powders such as drugs or others, ordinary mailing envelopes should not be used because powders will leak out of their corners.

1. Unbreakable Plastic pill bottles with pressure lids or in Manila envelopes, screwcap glass vials, or cardboard pillboxes- Used to store trace evidence such as hair glass fiber, etc.
2. Paper bags and boxes- Used to package larger and/or heavier pieces of evidence.
3. Clean Paint Cans- Used to store Arson evidence.
4. Paper bags or Manila envelopes- Used to store Blood-stained materials/clothing after air drying.
5. Air-tight containers- used to store.

CHAIN OF CUSTODY

After careful collection of the evidence, the next step of the investigator is to submit evidence in the laboratory for examination. In the whole process, the maintenance of the chain of custody is very important. The transfer of property or evidence from a crime scene investigator to any other individual, agency, or location is documented by having a chain of custody. The list of information that is to be included in the chain of custody:

- List of evidence: the item number and a brief description.
- All transfers must include the date and time of the transfer.
- The signature of the individual releasing the evidence to another individual or location.
- The signature of the individual transporting the evidence.
- The signature of the individual receiving the evidence from another individual or location.
- Reason for the transfer as needed.

After all the collected evidence have been packaged properly they should be properly labeled. After labeling the next step is to transport all the packed evidence to the crime lab for forensic analysis or for further evaluation. The chain of custody is a tracking document beginning with detailed scene notes that document where the evidence was received from or collected. The chain of custody is initially established when an investigator takes custody of evidence at a crime scene, or when evidence is received from an officer or detective at, or from, the crime scene. In order to maintain all items, a complete and correct chain of custody must be maintained for all items.

Notes should be prepared which comprise of documentation of recovery location, the date and time of recovery, and also the description of items, condition, and whether any unusual markings or alterations to the item were present during recovery. This is not necessary that the evidence collector only will transport the evidence to the laboratory. Often some other officer transports the evidence to the lab. That's why maintenance of chain of custody log must be maintained indicating the transfer of custody to and from every individual who is involved in transporting or storing the evidence until it gets to the crime lab.

These include:

a) The collecting officer (who collects the evidence from the crime scene),

b) The transportation officer (who transports the collected & packaged evidence from the Crime scene to the laboratory),

c) Any evidence storage officer if the evidence is stored prior to taking it to the lab,

d) Any further transportation officer,

e) Anyone who gets into the evidence for any reason,

f) The laboratory evidence collection person(s),

g) Any other person involved in the whole process,

h) Send all evidence (to the crime lab) by registered or certified mail, return receipt requested, to maintain the chain of custody.

Transfer of Evidence to Property Room

On many occasions, the agencies transfer the evidence to a property room aforementioned to its submission in a crime lab. Property room documentation or secure electronic transfer is used when the investigator submits evidence to the property room. The associated information may include the following:

- Agency case number;
- Type of evidence;
- Officer responsible for the investigation: the name, rank, and identification number of the officer for whom the evidence was recovered. The official laboratory report is addressed to this officer;
- Transporting officer: the name, rank, identification number, and assignment of the investigator;
- Signature or another identifier of responsible officer and date prepared; the date the evidence is submitted to the property room;
- Comment: the address where the incident was located, or where the evidence was recovered.

The list of the evidence/property may include:

- Number each evidence item sequentially;
- Quantity of items included, e.g., 10 spent shell casings;
- Sera ial number of the item, e.g., VCR, handgun;
- Item description;
- Status: e.g., submit for analysis, Hold, or RTC (releasable, return to claimant or owner).

A file system in a computer is the manner in which files are named and logically placed for storage and retrieval. It can be considered as a database or index that contains the physical location of every single piece of data on the respective storage device, such as a hard disk, CD, DVD, or flash drive. This data is organized in folders, which are called directories. These directories further contain folders and files.

For storing and retrieving files, file systems make use of metadata, which includes the date the file was created, date modified, file size, and so on. They can also restrict users from accessing a particular file by using encryption or a password.

Files are stored on a storage media in “sectors”. Unused sectors can be utilized for storing data, typically done in sector groups known as blocks. The file system identifies the file size and position and the sectors that are available for storage. If a structure for organizing files wouldn’t exist, it would not be possible to delete or retrieve files, or to keep two files with the same name since all the files would exist in the same folder. For example, it is because of folders that we are able to name two different image files with the same name, as both exist in two different folders. But if two files are in the same directory, they cannot have the same name.

Most of the applications need a file system to work, hence every partition needs to have one. Programs are also dependent on file systems, which means that if a program is built to be used in Mac OS, it will not run on Windows.

Some commonly used file systems

FAT File System

FAT or File Allocation Table is a file system used by operating systems for locating files on a disk. Due to fragmentation, files may be scattered around and divided into sections. The FAT system keeps a track of all parts of the file. FAT has existed as a file system since the advent of personal computers.

Features

- File Name
  - FAT system in MS-DOS allows file names of 8 characters only
  - FAT file system in Windows supports long file names, with full file path being as long as 255 characters
  - File name should start with alphanumeric characters
  - File names can have any character except "/ = [],? ^""
  - File names can have more than one period and spaces. Characters that come after the last period in the full file name are considered as the file extension.
- FAT file system does not support folder and local security. This means users logged into a computer locally will gain complete access to folders and files that lie in FAT partitions.
- It provides fast access to files. The rate depends upon the size of the partition, file size, type of file, and number of files in the folder.

FAT 32 File System

This is an advanced version of the FAT File system and can be used on drives ranging from 512 MB to 2 TB.

Features

- It is more storage-efficient and supports up to 2TB of size
- Provides a better usage of disk space
- Easier access of files in partitions less than 500 MB or greater than 2GB in size

The figure below shows the partitioning layout in FAT and FAT 32 file systems:

FAT File System

FAT 32 File System

NTFS File System

The NTFS File System stands for New Technology File System.

Features

- Naming
  - File name can be as long as 255 characters
  - File names can have any character other than / " :*
  - They are not case sensitive
- It provides folder and file security. This is done by passing on NTFS permission to files and folders. Security works at the local as well as network levels. Every file and folder in the list has an Access Control List that includes the users, security identifiers, and the access privileges that are granted to the users.
- Files and partition sizes are larger in NTFS than those in FAT. An NTFS partition can be of a size as large as 16 Exabytes, but practically it is limited to 2TB. File size can range from 4 GB to 64 GB.
- It provides up to 50% file compression.
- It is a reliable and recoverable file system that makes use of transaction logs for updating files and folders automatically.
- It provides bad-cluster mapping. This means that it can detect bad clusters or erroneous space in the disk, retrieve the data in those clusters, and then store it in another space. To avoid further data storage in those areas, bad clusters are marked for errors.

NTFS File System

EXT File Systems

Extended file system (EXT), Second Extended file system (EXT2), and Third Extended file system (EXT3) are designed and implemented on Linux. The EXT is an old file system that was used in pioneer Linux systems. EXT2 is probably one of the most widely used Linux file systems. EXT3 also includes the same features as EXT2 but also includes journaling. Here we will talk about the most commonly used EXT2. With the optimizations in kernel code, it provides robustness along with good performance whilst providing standard and advanced Unix file features.

Features

- Supports standard file types in Unix i.e. regular files, device special files, directories, symbolic links
- Can manage file systems created on huge partitions. Originally, file system size was restricted to 2 GB, but with recent work in the VFS layer, this limit has now increased to 4 TB.
- Reserves about 5 percent of blocks for administrator usage, thus allowing the admins to recover from situations of overfilled processes.
- Allows for secure deletion of files. Once data is deleted, the space is overwritten with random data to prevent malicious users from gaining access to the previous data.

What is a file format?

A file format is a layout and organization of data within the file. If a file is to be used by a program, it must be able to recognize and have access to the data in the file. For instance, a text document can be recognized by a program such as Microsoft that is designed to run text files but not by a program that is designed to run audio or video files.

A file format is indicated along with the file name in the form of a file extension. The extension contains three or four letters identifying the format and is separated from the file name by a period.

Steps in the file system forensics process

Carrying out a forensic analysis of file systems is a tedious task and requires expertise every step of the way. Following are the steps that can help analyze a file system for data that may provide evidence in a forensic investigation.

Acquisition

The system should be secured to ensure that all data and equipment stay safe. In other words, all media required for forensic analysis should be acquired and kept safe from any unauthorized access. Find out all files on the computer system including encrypted, password-protected, hidden, and deleted (but not overwritten) files. These files must be acquired from all storage media that include hard drives and portable media. Once acquired, forensic investigators have to make a copy of them so that the original files are kept intact without the risk of alteration.

This can be done in four ways:

- *Disk-to-Image*: This is the most common method as it provides more flexibility and allows to creation of multiple copies.
- *Disk-to-Disk*: Used where disk-to-image is not possible.
- *Logical*: it captures only the files that are of interest to the case. Used when time is limited.
- *Sparse*: It gathers fragments of deleted or unallocated data.

Validation and discrimination

Before you analyze an image, you need to validate it to ensure the integrity of the data.

Hashing algorithms help forensic investigators determine whether a forensic image is an exact copy of the original volume or disk. This validates the integrity of evidence and conforms to its admissibility in the court.

Extraction

Data extraction, which involves the retrieving of unstructured or deleted data and needs to be processed for forensic investigation. Many computer users think that a file, once deleted, will disappear forever from the hard disk. However, this is not true. Deleting files only removes it from the disc contents table. In FAT systems it is called the File Allocation Table, while in NTFS it is called the Master File Table. Data is stored in clusters on the hard disc and consists of a certain number of bits. Parts of files are mostly scattered throughout the disc, and deleting the files makes it difficult to reconstruct them, but not impossible. With increased disk capacity, it now takes longer for all fragments of a file to be overwritten.

In many cases, the criminals may have hidden the data that can turn out to be useful for forensic investigation. Criminals with basic technical knowledge have many options available for hiding data such as disk editor, encryption, steganography, and so on. Recovering and reconstructing this data can be time-consuming, but generally, it produces fruitful evidence.

Extracting data from unallocated space is file carving. It is a helpful technique in digital forensics that finds deleted or hidden files from the media. A hidden file can lie in any area such as slack space, unallocated clusters, or lost clusters of the digital media or disk. For using file carving, a file should have a header that can be located by performing a search that continues till the file footer is located. Data that lies between these two points is extracted and then analyzed for file validation.

Reconstruction

Extracted data can be reconstructed using a variety of available software tools that are based on various reconstruction algorithms such as bottom-up tree reconstruction and inference of partition geometry. Reconstructed data is thoroughly analyzed for further evidence and put forth in the form of a report.

Reporting

In order to keep a track record of every step of the investigation, document every procedural step. Evidence presented without proper documentation may not be admissible in court. This documentation should not only include the recovered files and data but also the physical layout of the system along with any encrypted or reconstructed data. Forensic analysis of time-based metadata can help investigators correlate distinct information quickly and to find notable times and dates of activities related to improper computer usage, spoliation, and misappropriation.

Recovery of Internet Usage Data

Data recovery can be defined as a process of obtaining the information located on a storage device that cannot be accessed by standard means due to its previous deletion or certain damage to the digital medium. Different approaches are used to regain the missing files, yet, only on the condition that their content *is present somewhere within the storage*. For instance, data recovery doesn't cover the situations when a file has never been written to persistent storage, like documents that were created but could not be eventually saved to the hard disk drive due to a power failure. Also, none of the existing restore methods can cope with the cases of permanent erasure which occurs when some other information occupies its storage space – under such circumstances, the lost files can only be retrieved from an external backup.

In general, data recovery techniques are divided into two types: software-based and ones involving the repair or replacement of damaged hardware components in a laboratory setting. A software-based approach is employed in the majority of cases and involves the use of specialized utilities able to interpret the logical structure of the problem storage, read out the required data, and deliver it to the user in a usable form for further copying. Physical repairs are conducted by specialists in the most severe instances, for example, when some mechanical or electrical parts of the drive no longer work properly – in this case, all the measures are directed towards a one-time extraction of the critical content, without the possibility of continued usage of the affected device.

The information remaining on an intact storage can usually be recovered without professional help by means of data-specialized software. However, it is important to keep in mind that *no information is recoverable after being overwritten*. For this reason, nothing should be written to the storage until the last file from it is rescued.

Most data recovery utilities operate using the algorithms of metadata analysis, the method of raw recovery based on the known content of files, or a combination of the two approaches.

Metadata is hidden service information contained within the file system. Its analysis allows the software to locate the principal structures on the storage that keep a record of the placement of files' content, their properties, and directory hierarchy. After that, this information is processed and used to restore the damaged file system. This method is preferred over raw recovery as it allows obtaining files with their original names, folders, dates, and time stamps. If the metadata wasn't seriously corrupted, it may be possible to reconstruct the entire folder structure, depending on the specifics of the mechanisms employed by the file system to get rid of "unnecessary"

items. Yet, such analysis cannot be performed successfully when the crucial parts of metadata are missing. That is why it is extremely important to refrain from using file system repair tools or initiating operations that may result in its modification until the data is restored completely.

As a rule, when the desired result wasn't achieved with the help of metadata analysis, the search for files by their known content it performed. In this case, the "known content" doesn't imply the entire raw content of a file, only particular patterns that are typical for the files of the given format and may indicate the beginning or the end of the file. These patterns are referred to as "file signatures" and can be used to determine whether a piece of data on the storage belongs to a file of a recognized type. Files recovered with this method receive an extension based on the found signature, and new names and get assigned to new folders, usually created for files of different types. The main limitation of this approach is that some files may lack identifiable signatures or have only a signature denoting the start of a file, making it hard to predict where it ends, especially when its parts are not stored consequently.

To get the lost files back with maximum efficiency, data recovery software may use the described techniques concurrently during a single scan launched on storage.

Remote data recovery is performed through a modem or Internet connection by engineers using technology to achieve the same results as if the hard drive had been sent to a lab, yet in a more convenient manner for the customer. Assuming the hard drive is still functioning, remote recovery can be achieved for a single file or for huge volumes of data.

However, many users don't consider remote recovery to be as reliable as sending damaged drives to a lab. They believe recovery can be achieved only by engineers with highly specialized tools in state-of-the-art clean rooms. Users also are concerned about the security of having their computer systems, and their valuable data, connected to a third-party system and any vulnerability that might create.

Depending on the scenario, remote recovery offers the same advantages as in-lab service, with the added benefit of faster recovery times -- often as short as one hour. The initial goal is to either make the original volume mountable -- meaning that the operating system can read and write data to that drive -- or restore the data to its previous location. If this isn't possible, the engineer copies the data to a different location on the customer's system. With no need to dismantle and ship the drive or hardware for service, many concerns about a traditional recovery are eliminated. Security isn't an issue, since each recovery is performed through a connection secured with proprietary communication protocols and encrypted packets.

Remote recovery can solve many data-loss problems because it works for all types of recoveries, including servers, desktops, and laptops, across a wide variety of media, platforms and operating systems. In addition, the pricing structure is similar to traditional in-lab work. With remote recovery, you're not paying more, but you're potentially getting your data back faster.

Requirements of remote recovery

The major requirement of remote service is that the hardware must be working for lost data to be recovered. In these cases, where there is physical damage, the hard drive needs to go into a recovery lab so engineers can use special tools to get the drive running again for long enough to copy the data.

There are other hurdles with remote service for customers already shaken by their data-loss experience. Remote service requires some assistance from the customer so the engineer can connect with the system and produce a file listing. This process might be too intimidating for the less technically inclined user, as many people are afraid to even touch their computers after a data-loss situation out of fear that they might cause more damage.

Another requirement is the need for available staff to work with the remote-recovery engineers. If the circumstances surrounding the data loss are too hectic, sending the drive into a reliable data recovery lab might be a better option.

Remote service requires a stable connection, which can be a challenge in a high-security environment. Many organizations have strict proxy server or firewall policies and may not be able to connect with outside systems. Working with large amounts of data can also be a problem. Although remote recovery is capable of recovering huge volumes of data, sometimes the customer doesn't have the space available for the copied data. For example, working with some Unix or Macintosh systems requires special copy-out destinations to maintain data integrity.

Finally, the unique nature of the service can be a roadblock to using remote data recovery. Since it's a fairly new technology, many users feel that remote recovery is too good to be true and don't believe that it can deliver on the promises it makes. As the following examples show, however, remote data recovery is an option that every data-loss sufferer should always consider.

Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior. Just as someone may wish to exclude people from a private conversation, many online users want to control or prevent certain types of personal data collection.

As Internet usage has increased over the years, so has the importance of data privacy. Websites, applications, and social media platforms often need to collect and store personal data about users in order to provide services. However, some applications and platforms may exceed users' expectations for data collection and usage, leaving users with less privacy than they realized. Other apps and platforms may not place adequate safeguards around the data they collect, which can result in a data breach that compromises user privacy.

Why is data privacy important?

In many jurisdictions, privacy is considered a fundamental human right, and data protection laws exist to guard that right. Data privacy is also important because in order for individuals to be willing to engage online, they have to trust that their personal data will be handled with care. Organizations use data protection practices to demonstrate to their customers and users that they can be trusted with their personal data.

Personal data can be misused in a number of ways if it is not kept private or if people don't have the ability to control how their information is used:

- Criminals can use personal data to defraud or harass users.
- Entities may sell personal data to advertisers or other outside parties without user consent, which can result in users receiving unwanted marketing or advertising.
- When a person's activities are tracked and monitored, this may restrict their ability to express themselves freely, especially under repressive governments.

For individuals, any of these outcomes can be harmful. For a business, these outcomes can irreparably harm its reputation, as well as result in fines, sanctions, and other legal consequences. In addition to the real-world implications of privacy infringements, many people and countries hold that privacy has intrinsic value: that privacy is a human right fundamental to a free society, like the right to free speech.

What are some of the challenges users face when protecting their online privacy?

Online tracking: User behavior is regularly tracked online. Cookies often record a user's activities, and while most countries require websites to alert users of cookie usage, users may not be aware of to what degree cookies are recording their activities.

Losing control of data: With so many online services in common use, individuals may not be aware of how their data is being shared beyond the websites with which they interact online, and they may not have a say over what happens to their data.

Lack of transparency: To use web applications, users often have to provide personal data like their name, email, phone number, or location; meanwhile, the privacy policies associated with those applications may be dense and difficult to understand.

Social media: It is easier than ever to find someone online using social media platforms, and social media posts may reveal more personal information than users realize. In addition, social media platforms often collect more data than users are aware of.

Cybercrime: Many attackers try to steal user data in order to commit fraud, compromise secure systems, or sell it on underground markets to parties who will use the data for malicious purposes. Some attackers use phishing attacks to try to trick users into revealing personal information; others attempt to compromise companies' internal systems that contain personal data.

What are some of the challenges businesses face when protecting user privacy?

Communication: Organizations sometimes struggle to communicate clearly to their users what personal data they are collecting and how they use it.

Cybercrime: Attackers target both individual users and organizations that collect and store data about those users. In addition, as more aspects of a business become Internet-connected, the attack surface increases.

Data breaches: A data breach can lead to a massive violation of user privacy if personal details are leaked, and attackers continue to refine the techniques they use to cause these breaches.

Insider threats: Internal employees or contractors might inappropriately access data if it is not adequately protected.

Recover Swap Files/Temporary Files/Cache Files

The biggest problem with data is that once you store it on any form of magnetic media, it stays there forever. When you delete a file, your computer takes a shortcut. Instead of physically destroying the file, the computer simply pretends that the file no longer exists by replacing the first letter of the file name with a special character (hex byte code E5h), which leaves the contents of the file intact.

This process is like taking your name off an apartment building directory to make it look like you no longer live there, but stay in the apartment until someone else moves in. Only when the computer needs the space taken up by the deleted file will it actually overwrite the old file with new data? If your disk has plenty of extra space available, you could go weeks, months, or even years without ever overwriting previously deleted files. (Although, when you defragment your hard disk, your computer will likely overwrite many of these "deleted" files.)

Temp files are the temporary files that store the content of an unsaved in-editing document every minute on Windows for backup purposes. These files are helpful to combat situations of data loss when the system gets crashed, halted, or shut down abruptly, as users can restore content from the temporary files. The Temp folder has two locations on the system hard drive.

- *C:\Username\AppData\Local\Temp*
- *C:\Documents and Settings\ \Application Data\Microsoft (for Windows 7 and XP, when saved on the network drive)*

System users can change or modify this default location of the Temporary files by clicking on the Environment Variables properties of your system or running sysdm.cpl in the Windows Run box.

Ways to Recover Deleted Temp Files

If we talk about any manual way to recover deleted Temp files, then if these are deleted using the simple delete process, the recovery is possible by restoring files through the Recycle Bin. But if it is cleared from the Recycle Bin or Shift+Del action is taken to delete the Temp files, the manual recovery of files is not possible.

However, you can prevent this unpleasant situation by adopting some crucial measures given below.

- Create regular backups of Windows drive, creating a fresh restore point on its storage
- Never save the backup of the Temp files on the same drive/folder
- Avoid using a corrupted hard drive on which the files are lost
- Select a reliable, professional Windows Data Recovery tool for Temp file recovery.

Retrieving deleted files

When a file is deleted, the file system removes the file logically. That is, it removes all the metadata and stamps related to the file. However, the file still resides in the disk as a physical entity until it is overwritten. These physical areas can be very easily explored and read and converted to a readable file using a forensic application. It is observed that data resides on a computer for a very long time and are retrieved to a good extent.

Retrieving cached files

One can find the webpage visited by the suspect or the victim by looking into the cache. The cache file of an application can be spread across the system storage. We can confine only search by using typical keywords related to the case or probable websites.

Retrieving files in unallocated space

In general, a deleted file can be searched sequentially or structurally by looking for file headers or extensions. However, certain tools help us to scan and look for broken headers and use supplementary headers to retrieve data or at least retrieve blocks of a lost file for unallocated space. These retrieved blocks can later be studied and reformed using other tools to retrieve lost files to a great extent. This is also called file carving.

Forensic Toolkit (FTK) is computer forensics software, created by AccessData. It is a court-accepted, digital investigations software that includes many features and capabilities such as full-disk forensic images, decrypting files and cracking passwords, parsing registry files, collecting, process and analyzing datasets, and advanced volatile memory analysis. FTK is recognized as the standard toolkit for cyber defense forensic analysts, incident responders, and other professionals working or collecting forensic evidence. This path will cover the basic tools within the FTK suite - FTK Imager, Registry Viewer, and Password Recovery Toolkit (PRTK.) Then dive into use cases and analysis with FTK Suite.

OpenText™ EnCase™ Forensic is recognized globally as the standard for digital forensics and is a court-proven solution built for deep-level digital forensic investigation, powerful processing, and integrated investigation workflows with flexible reporting options. It is built with a deep understanding of the digital investigation lifecycle and the importance of maintaining evidence integrity. EnCase Forensic empowers any examiner to seamlessly complete any investigation, including investigations of mobile devices. For digital investigations, examiners need to be able to prioritize, collect, and decrypt evidence from a wide variety of devices while maintaining its integrity. The process needs to be quick, efficient, repeatable, and defensible, with the ability to

create intuitive reports. With EnCase Forensic, examiners can be confident the integrity of the evidence will not be compromised. All evidence captured with EnCase Forensic is stored in the court-accepted EnCase evidence file formats.

EnCase Forensic has been used in thousands of court cases and is known for its ability to uncover evidence that may go unnoticed if analyzed with other solutions. Police agencies, federal agencies, and companies across the globe depend on EnCase Forensic for its functionality, flexibility, and track record of court acceptance. New customer-driven enhancements further differentiate EnCase Forensic from all other forensic tools on the market.

FTK can perform forensics analysis on the following file systems: • Microsoft FAT12, FAT16, and FAT32Microsoft NTFS (for Windows NT, 2000, XP, and Vista) • Linux Ext2fs and Ext3fs.

FTK can analyze data from several sources, including image files from other vendors. It can also read entire evidence drives or subsets of data, allowing you to consolidate large volumes of data from many sources when conducting a computer forensics analysis. With FTK, you can store everything from image files to recovered server folders on one investigation drive. FTK also produces a case log file, where you can maintain a detailed record of all activities during your examination, such as keyword searches and data extractions. This log is also handy for reporting errors to Access Data.

At times, however, you might not want the log feature turned on. If you're following a hunch, for example, but aren't sure the evidence you recover is applicable to the investigation, you might not want opposing counsel to see a record of this information because he or she could use it to question your methods and perhaps discredit your testimony. (Chapter 15 covers testimony issues in more detail.) Look through the evidence first before enabling the log feature to record searches. This approach isn't meant to conceal evidence; it's a precaution to ensure that your testimony can be used in court. FTK has two options for searching for keywords. One option is an indexed search, which catalogs all words on the evidence drive so that FTK can find them quickly. This option returns search results quickly, although it does have some shortcomings. For example, you can't search for hexadecimal string values, and depending on how data is stored on the eve-dense drive, indexing might not catalog every word. If you do use this feature, keep in mind that indexing an image file can take several hours, so it's best to run this process overnight. The other option is a live search, which can locate items such as text hidden in unallocated space that might not turn up in an indexed search. You can also search for alphanumeric and hexadecimal values on the evidence drive and search for specific items, such as phone numbers, credit card numbers, and Social Security numbers.

Usage of computer forensics software tools to cross-validate findings in computer evidence-related cases

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Computer forensics -- which is sometimes referred to as *computer forensic science* -- essentially is data recovery with legal compliance guidelines to make the information admissible in legal proceedings. The terms *digital forensics* and *cyber forensics* are often used as synonyms for computer forensics.

Digital forensics starts with the collection of information in a way that maintains its integrity. Investigators then analyze the data or system to determine if it was changed, how it was changed, and who made the changes. The use of computer forensics isn't always tied to a crime. The forensic process is also used as part of data recovery processes to gather data from a crashed server, failed drive, reformatted operating system (OS), or other situation where a system has unexpectedly stopped working.

Why is computer forensics important?

In the civil and criminal justice systems, computer forensics helps ensure the integrity of digital evidence presented in court cases. As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence -- and the forensic process used to collect, preserve and investigate it -- has become more important in solving crimes and other legal issues.

The average person never sees much of the information modern devices collect. For instance, the computers in cars continually collect information on when a driver brakes, shifts and changes speed without the driver being aware. However, this information can prove critical in solving a legal matter or a crime, and computer forensics often plays a role in identifying and preserving that information.

Digital evidence isn't just useful in solving digital-world crimes, such as data theft, network breaches, and illicit online transactions. It's also used to solve physical-world crimes, such as burglary, assault, hit-and-run accidents, and murder.

Businesses often use a multilayered data management, data governance, and network security strategy to keep proprietary information secure. Having data that's well managed and safe can help streamline the forensic process should that data ever come under investigation.

Businesses also use computer forensics to track information related to a system or network compromise, which can be used to identify and prosecute cyber attackers. Businesses can also use digital forensic experts and processes to help them with data recovery in the event of a system or network failure caused by a natural disaster.

As the world becomes more reliant on digital technology for the core functions of life, cybercrime is rising. As such, computer forensic specialists no longer have a monopoly on the field. See how the police in the U.K. are adopting computer forensic techniques to keep up with increasing rates of cybercrime.

Types of computer forensics

There are various types of computer forensic examinations. Each deals with a specific aspect of information technology. Some of the main types include the following:

- **Database forensics.** The examination of information contained in databases, both data and related metadata.
- **Email forensics.** The recovery and analysis of emails and other information contained in email platforms, such as schedules and contacts.
- **Malware forensics.** Sifting through code to identify possible malicious programs and analyzing their payload. Such programs may include Trojan horses, ransomware or various viruses.
- **Memory forensics.** Collecting information stored in a computer's random access memory (RAM) and cache.
- **Mobile forensics.** The examination of mobile devices to retrieve and analyze the information they contain, including contacts, incoming and outgoing text messages, pictures and video files.
- **Network forensics.** Looking for evidence by monitoring network traffic, using tools such as a firewall or intrusion detection system.

How does computer forensics work?

Forensic investigators typically follow standard procedures, which vary depending on the context of the forensic investigation, the device being investigated or the information investigators are looking for. In general, these procedures include the following three steps:

1. **Data collection.** Electronically stored information must be collected in a way that maintains its

integrity. This often involves physically isolating the device under investigation to ensure it cannot be accidentally contaminated or tampered with. Examiners make a digital copy, also called a *forensic image*, of the device's storage media, and then they lock the original device in a safe or other secure facility to maintain its pristine condition. The investigation is conducted on the digital copy. In other cases, publicly available information may be used for forensic purposes, such as Facebook posts or public Venmo charges for purchasing illegal products or services displayed on the Vicemo website.

2. **Analysis.** Investigators analyze digital copies of storage media in a sterile environment to gather the information for a case. Various tools are used to assist in this process, including Basis Technology's Autopsy for hard drive investigations and the Wireshark network protocol analyzer. A mouse jiggler is useful when examining a computer to keep it from falling asleep and losing volatile memory data that is lost when the computer goes to sleep or loses power.

3. **Presentation.** Forensic investigators present their findings in a legal proceeding, where a judge or jury uses them to help determine the result of a lawsuit. In a data recovery situation, forensic investigators present what they were able to recover from a compromised system.

One of the most critical aspects of computer forensics is validating digital evidence because ensuring the integrity of the data you collect is essential for presenting evidence in court. Most computer forensic tools such as ProDiscover, X-Ways Forensics, FTK, and Encase provide automated hashing of image files. For example, when ProDiscover loads an image file, it runs a hash and compares that value to the original hash calculated when the image was first acquired. You might remember seeing this feature when the Auto Image Checksum Verification message box opens after you load an image file in ProDiscover. Computer forensics tools have some limitations in performing hashing, however, so learning how to use advanced hexadecimal editors is necessary to ensure data integrity.

Validating with Hexadecimal Editors Advanced hexadecimal editors offer many features not available in computer forensics tools, such as hashing specific files or sectors. Learning how to use these tools is important, especially when you need to find a particular file—for example, a known contraband image. With the hash value in hand, you can use a computer forensics tool to search for a suspicious file that might have had its name changed to look like an innocuous file. (Recall that two files with exactly the same content have the same hash value, even if they have different names.) Getting a hash value with a full-featured hexadecimal editor is much faster and easier than with a computer forensics tool.

A Computer Forensic Investigation generally investigates the data which could be taken from computer hard disks or any other storage devices with adherence to standard policies and procedures to determine if those devices have been compromised by unauthorized access or not. Computer Forensics Investigators work as a team to investigate the incident and conduct the forensic analysis by using various methodologies (e.g. Static and Dynamic) and tools (e.g. ProDiscover or Encase) to ensure the computer network system is secure in an organization. A successful Computer Forensic Investigator must be familiar with various laws and regulations related to computer crimes in their country (e.g. Computer Misuse Act 1990, the UK) and various computer operating systems (e.g. Windows, Linux) and network operating systems (e.g. Win NT). According to Nelson, B., et al., (2008), Public Investigations and Private or Corporate Investigations are the two distinct categories that fall under Computer Forensics Investigations. Public investigations will be conducted by government agencies, and private investigations will be conducted by a private computer forensic team. This report will be focused on private investigations since an incident occurred at a new start-up SME based in Luton.

LESSON ROUND-UP

- Data recovery tools are an essential tool for individuals to recover lost or damaged data. Such tools perform differently in case of personal data recovery and forensic data recovery.
- Data privacy is also important because in order for individuals to be willing to engage online, they have to trust that their personal data will be handled with care. Organizations use data protection practices to demonstrate to their customers and users that they can be trusted with their personal data.
- Forensic data recovery is the extraction of data from damaged evidence sources in a forensically sound manner. This method of recovering data means that any evidence resulting from it can later be relied on in a court of law.
- Digital forensics tools are either hardware or software designed to aid in the recovery of digital evidence of cyber-attack, and preservation of data or critical systems.
- The chain-of-custody form is critical in evidence gathering, and it comes into play as soon as you arrive at the scene of the incident. Every report, disk, screenshot, and printout is considered evidence; the chain of custody will begin as soon as the evidence is placed in an evidence bag or is tagged as evidence.
- Evidence gathering focuses on collecting all potential evidence, such as might be present in computer/ network logs, on defaced websites, on social media sites, or forensically from a computer hard drive.
- Digital Evidence is any information that is stored or transmitted in the digital form that a party at court can use at the time of trial. Digital evidence can be Audio files, and voice recordings, Address books and contact lists, Backups to various programs, including backups to mobile devices, Browser history, Cookies, Database, Compressed archives (ZIP, RAR, etc.) including encrypted archives, etc.
- Files that are deleted, lost, cached or unallocated can be retrieved using various methods and tools.

GLOSSARY

Data Analytics - Data Analytics is the science of analyzing raw datasets in order to derive a conclusion regarding the information they hold. It enables us to discover patterns in the raw data and draw valuable information from them. Data analytics processes and techniques may use applications incorporating machine learning algorithms, simulation, and automated systems.

Data Recovery - Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible.

Chain of Custody - Chain of Custody form the Chain of Custody form (CCF or CoC) is used to record all changes in the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.

Swap File - A swap file is a system file that creates temporary storage space on a solid-state drive or hard disk when the system runs low on memory. The file swaps a section of RAM storage from an idle program and frees up memory for other programs.

Computer forensics – Computer forensics which is sometimes referred to as computer forensic science -- essentially is data recovery with legal compliance guidelines to make the information admissible in legal proceedings. The terms digital forensics and cyber forensics are often used as synonyms for computer forensics.

Data Privacy- Data privacy is the branch of data management that deals with handling personal data in compliance with data protection laws, regulations, and general privacy best practices.

TEST YOURSELF

(These are meant for recapitulation only. Answers to these questions are not to be submitted for evaluation)

1. What is the standard procedure and practice followed for the recovery of data and what ethical norms to be followed in such cases?
2. What are the precautions need to be followed in identification, preservation, analysis and presentation of evidence?
3. Why the issue of data privacy is significant in contemporary world today and what are the challenges faced in protection of such data?
4. Forensic Toolkit can perform forensics analysis on many file systems with different strategies. Discuss.

LIST OF FURTHER READINGS

- Anil Maheshwari, Data Analytics, McGraw Hill Education, First Edition, July 2017
- Jay Liebowitz, Data Analytics and AI, Taylor & Francis, First Edition, August, 2020
- Samaddar, Auerbach P, Data Analytics, Taylor & Francis, First Edition, February, 2019
- Joao Moereira, Andre Carvalho, Tom Horvath, A General Introduction to Data Analytics, Wiley Interscience, 1st Edition, August, 2020
- Goldenfein, J,Images and Biometrics – Privacy and Stigmatisation. In *Monitoring Laws: Profiling and Identity in the World State* (pp. 42-63). Cambridge: Cambridge University Press. doi:10.1017/9781108637657.003,2019
- Van Alsenoy, B., Introduction. In *Data Protection Law in the EU: Roles, Responsibilities and Liability* (pp. 343-346). Intersentia. doi:10.1017/9781780688459.023,2019
- Culnan, M., & Bruening, P., Privacy Notices: Limitations, Challenges, and Opportunities*. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (Cambridge Law Handbooks, pp. 524-545). Cambridge: Cambridge University Press. doi:10.1017/9781316831960.029,2018

Information Systems

Lesson 12

KEY CONCEPTS

■ Information System ■ Hardware ■ Software ■ Data ■ Telecommunications ■ Information Systems ■ Decision Support System ■ Management Information System ■ Office Automation Systems

Learning Objectives

To understand:

- The meaning Information System
- Uses of Information System
- Types of Information System
- Information System and Cyber Security
- Information System and Its Application in Different Spheres of Business

Lesson Outline

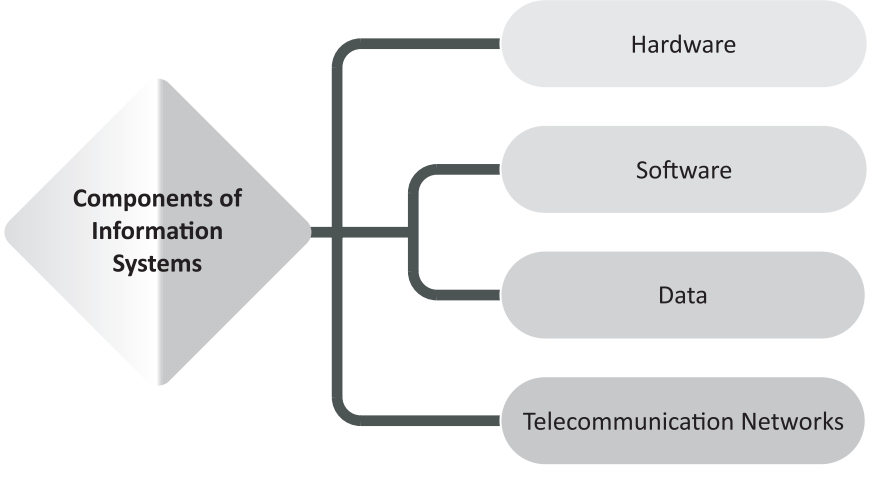
- What is Information System?
- How Information System is Useful for Business?
- Types of Information System
- Application of Information System
- Information System and Security
- Lesson Round-Up
- Glossary
- Test Yourself

WHAT IS INFORMATION SYSTEM

Information systems encapsulates the tools that organizations use to collect, manage, and analyze data. Decision making process in the organization is getting improved by enhancing decision making capacity and efficiency of operations as whole, which in turns result in improved profitability.

In today's scenario, be it human resource management, financial management, or customer support activities, or supply chain of operations, data is core of every business activity and information system become inevitable part of all such data-driven activities.

Information system does not merely mean the usage of software for the purpose of processing data and sharing information based on such processing, in real sense it is more than that and encapsulates various components such as hardware, software and telecommunication networks to collect useful data, especially in an organization.



Components of Information System

a. **Hardware** – This is the physical component of the technology. It includes computers, hard disks, keyboards, iPads, etc. The hardware cost has decreased rapidly while its speed and storage capacity has increased significantly. However, the impact of the use of hardware on the environment is a huge concern today. Nowadays, storage services are offered from the cloud, which can be accessed from telecommunications networks.

b. **Software** – Software can be of two types, system software and application software. The system software is an operating system that manages the hardware, program files, and other resources while offering the user to control the PC using GUI. Application software is designed to manage tasks by the users. In short, system software makes the hardware usable while application software handles specific tasks.

An example of system software is Microsoft windows, and an example of application software is Microsoft Excel.

Large companies may use licensed applications which are developed and managed by software development companies to handle their specific needs. The software can be proprietary and open source, available on the web for free use.

c. **Data** – Data is a collection of facts and is useless by themselves, but when collected and organised together, it can be very powerful for business operations. Businesses collect all the data and use it to make decisions that can be analysed for the effectiveness of the business operations.

d. Telecommunications – Telecommunication is used to connect with the computer system or other devices to disseminate information. The network can be established using wired or wireless modes. Wired technologies include fiber optic and coaxial cable, while wireless technologies include radio waves and microwaves.

Elements of complete Information System implementation

a. Development of computer applications for business transactions, such as production, marketing, selling, etc.

b. Development of management information systems for effective business control.

c. Planned introduction and use of computers and telecommunications.

d. Creation of an overall systems and standards architecture for technology, applications and data.

e. Development of information systems for business planning.

f. Improved productivity in information systems and computing.

g. Development of appropriate staff resources.

h. Development of internal support systems (payroll, personnel, pensions, etc.).

Implementation Plans of Information System

Three general tactical implementation plans of implementing Information System are there. The process of putting the new information system online and retiring the old system is known as system changeover. There are four changeover methods which are:

Changeover Method	*Particular*
Direct Cutover	The direct cutover approach causes the changeover from the old system to the new system to occur immediately when the new system becomes operational. It is the least expensive but involves more risks than other changeover methods.
Parallel Operation	The parallel operation changeover method requires that both the old and the new information systems operate fully for a specified period. Data is input to both systems and output generated by the new system is compared with the equivalent output from the old system. When users, management, and IT group are satisfied that the new system operates correctly then the old system is terminated. It is the costliest changeover method and involves lower risks.
Pilot Operation	The pilot changeover method involves implementing the completely new system at a selected location of a company. Direct cutover method and operating both systems for only the pilot site. The group that uses the new system first is called the pilot site. By restricting the implementation to a pilot site reduces the risk of system failure as compared with is less expensive than a parallel system.
Phased operation	The phased operation changeover method involves implementing the new system in stages, or modules. We can implement each subsystem by using any of the other three changeover methods. In this approach risk of errors or failures is limited to the implemented module only as well as it is less expensive than the full parallel operation.

HOW INFORMATION SYSTEM IS USEFUL FOR BUSINESS

Business Information Systems may be boundary-spanning field of ponder relating to how Information and Communication Technologies (ICT) can be deployed to enhance business processes and upgrade the organization's value chain systems, which firms utilize to obtain, create, and deliver goods and services across the globe.

Information Systems play a vital role within the modern economy and enterprise setting characterized by strategic procurement, worldwide outsourcing, physically distributed operational environments, and extensive business alliances.

Amalgamation of various components such as Hardware, Software, Data and Telecommunication Networks is information system. These resources are useful for the processing and dissemination of information for the business. In the process of the information systems, the data is collected, stored, and processed for end users in various projects.

Customization is an important aspect in the growth of the company. Based on the proficiencies of the software, employees can tailor information to their requirements. Like, for instance, a manager can create reports that will be helpful for him to identify the levels of productivity of his employees. He gets real-time data to be able to identify problems that a business has regarding production line and know whether it needs to be shut down.

Information systems help decision-makers at a business to make informed decisions for the company. Information technology helps get prepared data on all areas of the business as it offers current data, background, and trend analysis. To utilize this nitty-gritty information on the company environment and finances to progress business execution within the long- and short-term.

Generally, the application of computer information systems in a business helps to manage operations, interact with customers and suppliers to compete with other business firms and organizations. This motivates more companies to learn about Information Systems (IS) and to utilize it for an added business advantage.

Following are the main reasons, why information system is useful for business:

a. Efficient functioning:

In order to achieve higher profitability for your business, it is essential to improve the efficiency of business operations continually. This is possible to do by continuously storing the correct amount of stock so that you can always give your consumers what they want.

b. New products, services, and business models:

For businesses to make new products and services, information systems play a crucial role. Information System also help create new business models, and these can describe how a company produce, design, and sell their products.

c. Behavioural changes:

The information system can also help to communicate better between the employers and the employee. It works better as it stores information systematically, including the documents and files in folders that can be easily accessed and shared by the employees. This way, it oversees the flow of information between the management and the lower-level employees.

d. Better decision making:

Information systems assist managers in creating informed decisions with the help of real-time data. Continuously making informed decision improves decision power and avoid wastage of time looking for information.

e. Store and Analyse Information:

Most information systems function as delivery vehicles for data stored in databases. Databases support the operations and management aspects of a business. With a database, the collected data is stored and organised. Examples of databases include employee records and product catalogues.

When it comes to analysing collections of stored data, data warehouses are built by information systems from several data sources to analyse the data. These archival data are mined for relevant information to develop and launch new products, reach out to potential customers as well as to serve the existing customers with accuracy and efficiency.

f. Simplify Business Processes:

The integration of information systems in a business enables easier management of certain business processes to save on time and labour. For instance, buyers can have a seamless shopping experience at an online retailer as they can select a particular product display based on best-selling items, price range and customer ratings.

With the help of information systems, these products are neatly organised which enhances the shopping experience. Besides that, business managers can utilise information systems for inventory management. That way, they can determine the inventory needed, reorder with their suppliers in addition to track and receive shipments in a timely and systematic manner.

g. New Products and Services:

Any company looking to improve and secure the future must establish a broader perspective with the use of a well-designed and coordinated information system. The Information System makes it easier to analyze independent processes such as information to produce valuable products or services and organized work activities.

Therefore, an Information System can give a company the competitive advantage by analyzing how a company creates, produce, and sell their products or services. This means that the focus will be put on the main goal ahead.

Transformation of Business through Information System

Information Systems (IS) importance has increased dramatically, and most businesses have been prompted to introduce it to keep their competitive edge. Today, nobody can envisage a business without an effective digital information system.

Introduction of an information system to a business can bring numerous benefits and assist in the external and internal processes that a business encounters daily, and decision-making for the future.

Changes in technology and new innovative business models have transformed social life and business practices. Smartphones, social networking, texting, emailing, and Webinars have all become essential tools of business because that is where the customers, suppliers, and colleagues can be found and explored for advancement in business performance.

Businesses are using information technology to sense and respond to rapidly changing customer demand, reduce inventories to the lowest possible levels, and achieve higher levels of operational efficiency.

Supply chains have become more fast-paced, with companies of all sizes depending on just-in-time inventory to reduce their overhead costs and get to market faster.

As newspaper print readership continues to decline, more than 168 million people read a newspaper online, and millions more read other news sites. About 83 million people watch a video online every day, 66 million read a blog, and 25 million posts to blogs, creating an explosion of new writers and new forms of customer feedback that did not exist five years ago. Social networking site Facebook attracted over 1 billion monthly visitors in 2014 worldwide. Businesses are starting to use social networking tools to connect their employees, customers, and managers worldwide. Many Fortune 500 companies now have Facebook pages, Twitter accounts, and Tumblr sites.

E-commerce and Internet advertising continues to expand. Google's online ad revenues surpassed $17 billion in 2013, and Internet advertising continues to grow at more than 15 percent a year, reaching more than $43 billion in revenues in 2013.

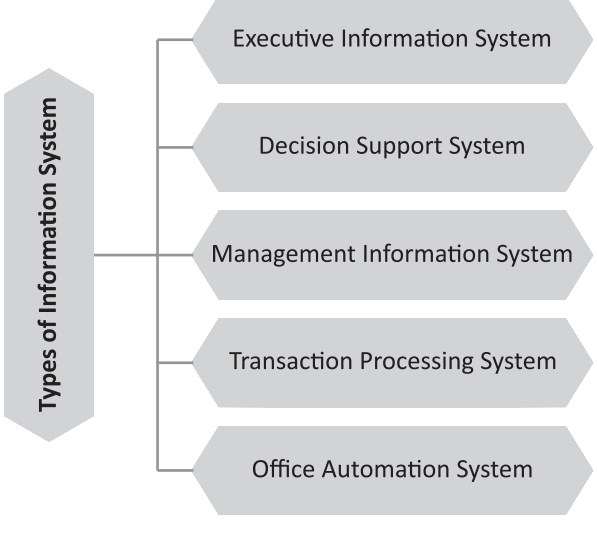
Information system managers oversee a wide assortment of assignments related to the information system, from coordinating or planning to inquire to supervising arrange security or web operations. Also, they can plan the computer-related activities of the company. Since information systems managers manage an assortment of other computer-related employment, they are expected to have knowledge and experience working in IT.

TYPES OF INFORMATION SYSTEM

The introduction of information systems into the business has evoked a chain reaction among different interrelated processes that have only benefited the companies by increasing profits and reducing costs and lead time, among other things. Therefore, it is imperative to understand the growing importance of information systems in companies.

Although many information systems offer various benefits, but common benefits should be offered by all information system.

Common Benefits of Information System that should be offered	It will induce innovation in business activities through its research and development.
	It will enable automation, reducing steps undertaken to complete a task.
	It helps keep the hardware, software, data storage, and networking system safe and up to date.



1. Executive Information System

An Executive Information System (EIS) is a management support system that facilitates and supports the decision-making requirements of an organization's senior executives. Hence, it is also called an "Executive Support System (ESS)."

An Executive Information System (EIS) is a kind of Decision Support System (DSS) used in organizations to help executives in decision making. It does so by providing easy access to important data needed in an organization to achieve strategic goals. An EIS usually has graphical displays on a user-friendly interface.

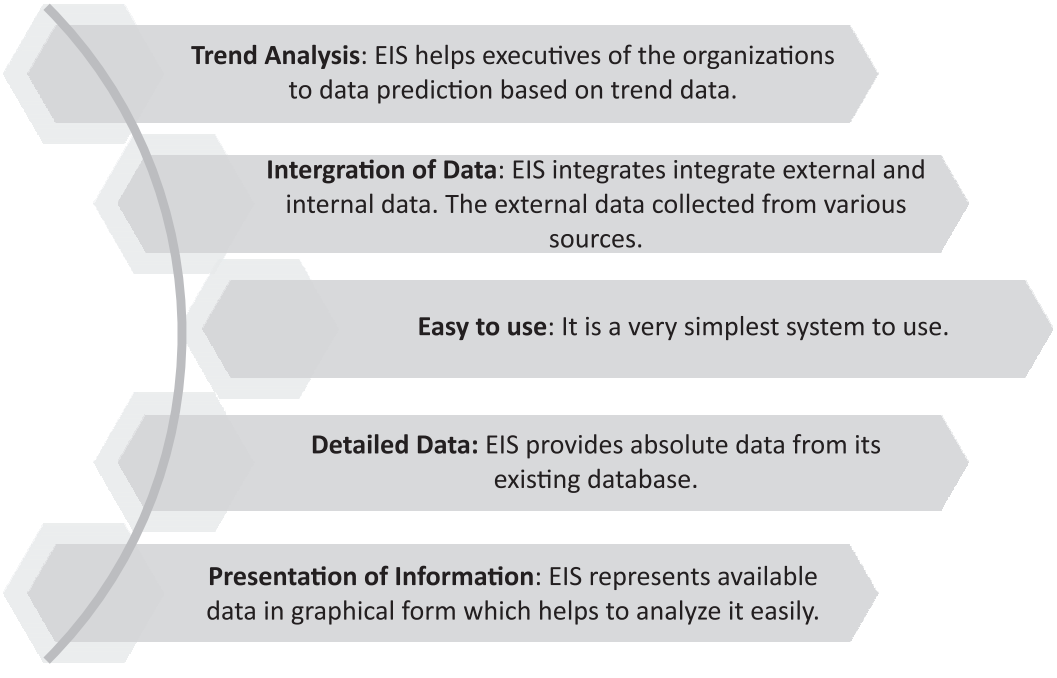
Early executive information systems were developed on mainframe computers as computer-based programs to provide the description, sales performance and/or market research data for senior executives of a company.

Executives, however, were not all literate or confident about the computers. Also, EIS data endorsed only executive-level decisions that did not necessarily support the entire company or enterprise. Current EIS data is available on Local Area Networks (LANs) throughout the company or enterprise, facilitated by personal computers and workstations.

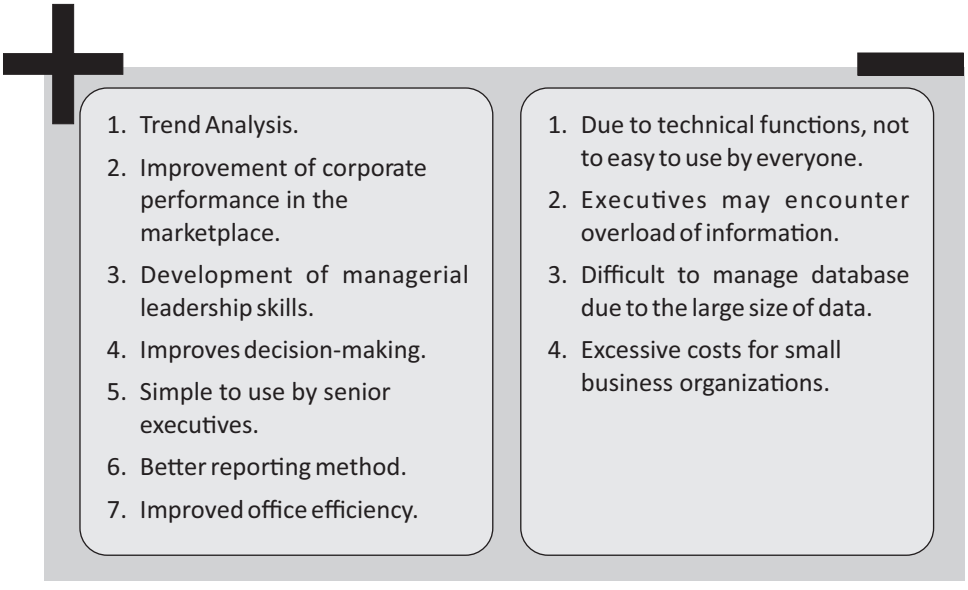
Employees can access company data to help make decisions in their workplaces, departments, divisions, etc. This enables employees to provide relevant information and ideas above and below the level of their company.

Executive support systems are intended to be used directly by senior managers to support unscheduled strategic management decisions. Often such information is external, unstructured, and even uncertain. Often, the exact scope and context of such information are not known in advance.

Key Characteristics of Executive Information System



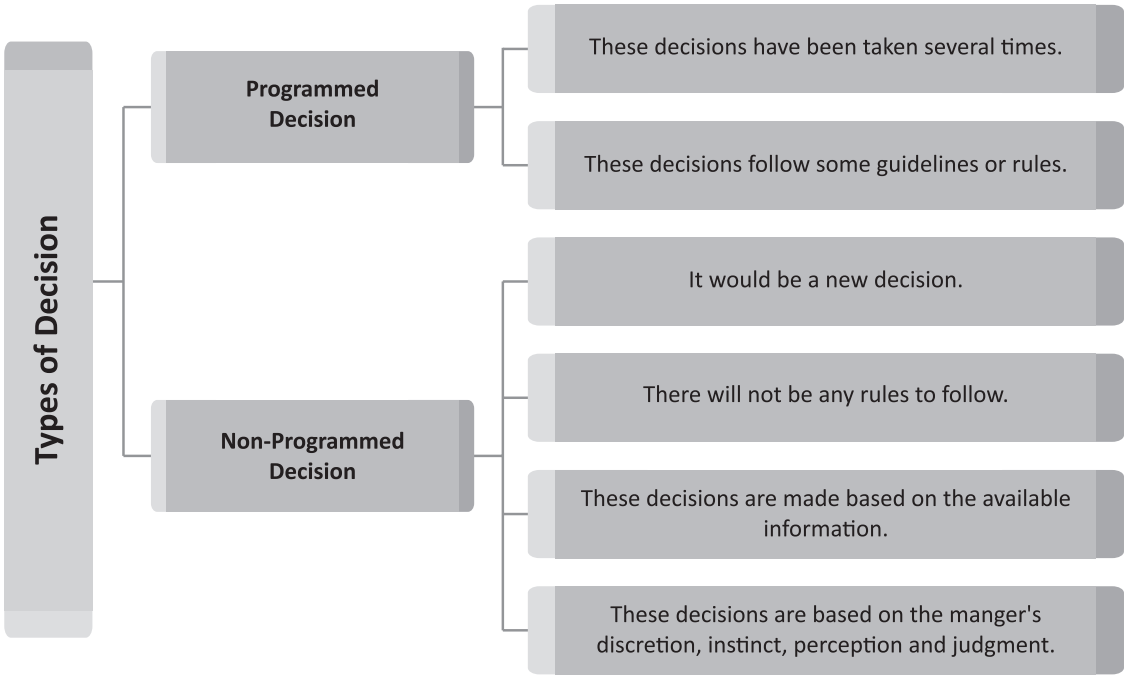
Advantages and Disadvantages of Executive Information System



2. Decision Support System

Decision Support Systems (DSS) are interactive software-based systems intended to help managers in decision-making by accessing large volumes of information generated from various related information systems involved in organizational business processes, such as office automation system, transaction processing system, etc.

DSS uses the summary information, exceptions, patterns, and trends using the analytical models. A decision support system helps in decision-making but does not necessarily give a decision itself. The decision makers compile useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions.



Attributes of a DSS

- Decision Support System is adaptable and flexible as per the requirement of business and managers.
- Interactivity is one of the main attributes of decision support system wherein it interacts with all the spheres of business and all level managers to improve the efficiency of business.
- Decision support system is curated the way that it very easy to use and understand.
- Decision support system are efficient and effective based of the information being fed into it.
- DSS are completely controlled by the decision-makers.
- Development of DSS is easy and non-complex.
- DSS can be extended to whole organization for more efficient performance with ease.
- DSS support for modeling and analysis.
- Data access is one of the main attributes of decision support system.
- DDS is Standalone, integrated, and Web-based.

Characteristics of a DSS

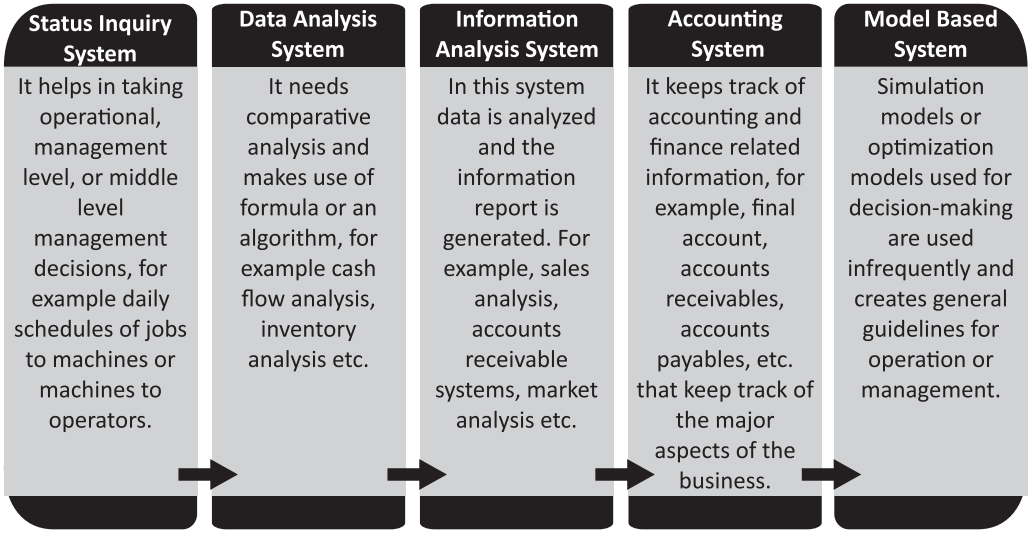
- Support for decision-makers in semi-structured and unstructured problems.
- Support for managers at various managerial levels, ranging from top executive to line managers.
- Support for individuals and groups. Less structured problems often requires the involvement of several individuals from different departments and organization level.
- Support for interdependent or sequential decisions.
- Support for intelligence, design, choice, and implementation.
- Support for variety of decision processes and styles.
- DSSs are adaptive over time.

Components of a DSS

Following are the components of the Decision Support System:

Database Management System (DBMS)	To solve a problem the necessary data may come from internal or external database. In an organization, internal data are generated by a system such as TPS and MIS. External data come from a variety of sources such as newspapers, online data services, databases (financial, marketing, human resources).
Model Management System	It stores and accesses models that managers use to make decisions. Such models are used for designing manufacturing facility, analyzing the financial health of an organization, forecasting demand of a product or service, etc.
Support Tools	Support tools like online help; pulls down menus, user interfaces, graphical analysis, error correction mechanism, facilitates the user interactions with the system.

Types of Decision Support System



3. Management Information System

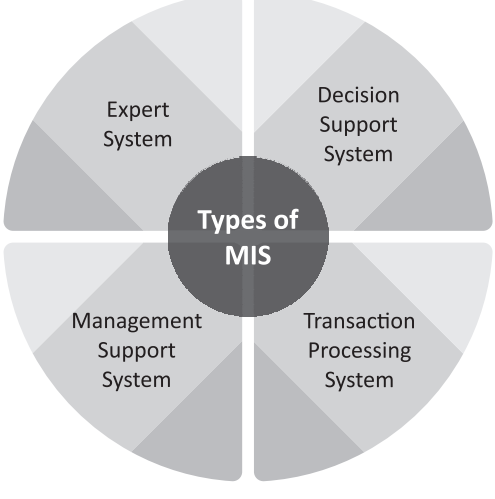
A management information system (MIS) is a computerized database of financial information organized and programmed in such a way that it produces regular reports on operations for every level of management in a company. It is usually also possible to obtain special reports from the system easily.

The main purpose of the MIS is to give managers feedback about company's own performance so that top management can monitor the company. Information displayed by the MIS typically shows "actual" data over against "planned" results and results from a year before, thus it measures progress against goals.

The MIS receives data from company units and functions. Some of the data are collected automatically from computer-linked check-out counters and others are keyed in at periodic intervals.

Routine reports are preprogrammed and run at intervals or on demand while others are obtained using built-in query languages; display functions built into the system are used by managers to check on status at desk-side computers connected to the MIS by networks.

MIS software is used to track sales, inventory, equipment, and related business information. In the past, these applications ran on mainframe computers. However, as computing systems evolved, organizations began to run MIS software on client-server systems. Today, MIS applications are commonly run in the cloud, including hybrid cloud environments.



1. **Expert System:** An expert system provides managers with insights and advice based on Artificial Intelligence (AI). In an expert system, the AI is trained to simulate the knowledge of a human expert in a particular field.
2. **Decision Support System:** A DSS analyzes business data to assist managers with decision making. For example, a DSS could project revenue figures based on new product sales assumptions.
3. **Transaction Process System:** A TPS processes the routine transactions associated with a business. Examples include payroll processing, order processing for an e-commerce business and invoicing.
4. **Management Support System:** An MSS stores and organizes data, enabling end users to generate reports and analyze data to address business needs and inform planning. A data warehouse is an example of a MSS.

The data managed by MIS software tools can help managers make better decisions related to sales, manufacturing, resource allocation and more. Similarly, the MIS department plays an important role in providing support services within an organization, such as the following:

1. **Governance:** Governance involves systems and controls over employees' use of computing systems. The MIS department defines, manages, and enforces the rules covering how and whether employees can access the company's technologies and network infrastructure. The MIS department is responsible for IT security and enforcing codes of conduct related to computer systems use.
2. **Infrastructure:** An organization's IT infrastructure is comprised of the technology systems that support the business' day-to-day functioning -- for example, phones, desktop and laptop computers, servers, application software and cloud computing. The MIS department provides internal help desk and support services, assisting employees and troubleshooting issues related to the infrastructure.
3. **Data management:** Data management involves provisioning and managing systems that enable employees to access and update critical business data. The MIS department is responsible for ensuring the availability and security of the organization's data management systems.

Pros and Cons of Management Information System

The following are some of the benefits that can be attained using MIS:

- Improve an organization's operational efficiency, add value to existing products, engender innovation and new product development, and help managers make better decisions.
- Companies can identify their strengths and weaknesses due to the presence of revenue reports, employee performance records etc. Identifying these aspects can help a company improve its business processes and operations.
- The availability of customer data and feedback can help the company to align its business processes according to the needs of its customers. The effective management of customer data can help the company to perform direct marketing and promotion activities.
- MIS can help a company gain a competitive advantage.
- MIS reports can help with decision-making as well as reduce downtime for actionable items.

Some of the disadvantages of MIS systems:

- Retrieval and dissemination are dependent on technology hardware and software.
- Potential for inaccurate information.

Management Information System and Its Application

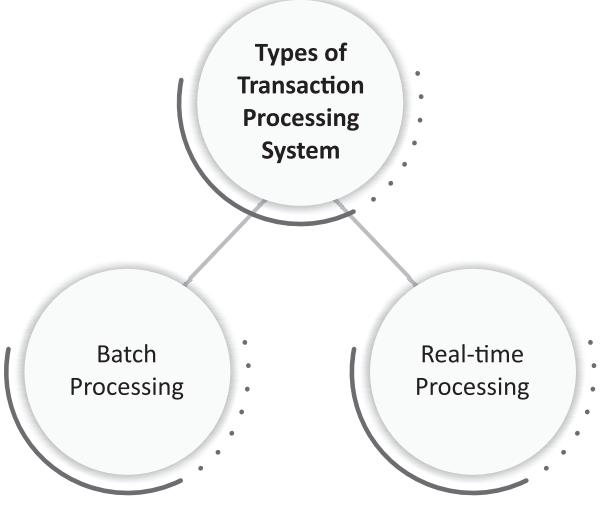
- **Enterprise Systems**—also known as enterprise resource planning (ERP) systems—provide integrated software modules and a unified database that personnel use to plan, manage, and control core business processes across multiple locations. Modules of ERP systems may include finance, accounting, marketing, human resources, production, inventory management, and distribution.
- **Supply Chain Management (SCM)** systems enable more efficient management of the supply chain by integrating the links in a supply chain. This may include suppliers, manufacturers, wholesalers, retailers, and final customers.
- **Customer Relationship** Management (CRM) systems help businesses manage relationships with potential and current customers and business partners across marketing, sales, and service.
- **Knowledge Management System (KMS)** helps organizations facilitate the collection, recording, organization, retrieval, and dissemination of knowledge. This may include documents, accounting records, unrecorded procedures, practices, and skills. Knowledge management (KM) as a system covers the process of knowledge creation and acquisition from internal processes and the external world. The collected knowledge is incorporated in organizational policies and procedures, and then disseminated to the stakeholders.

4. Transaction Processing System

Transaction processing is a style of computing, typically performed by large server computers, that supports interactive applications. In transaction processing, work is divided into individual, indivisible operations, called transactions.

A transaction processing system allows application programmers to concentrate on writing code that supports the business, by shielding application programs from the details of transaction management, transaction processing system offers following features to the business:

- It manages the concurrent processing of transactions.
- It enables the sharing of data.
- It ensures the integrity of data.
- It manages the prioritization of transaction execution.



a. Batch Processing: Batch processing is when clusters of transactions are refined simultaneously using a computer system. This method, although designed to be efficient for breaking down bulky series of programs, has a drawback as there is a delay in the transaction result.

b. Real-time Processing: Real-time processing carries out its transactions exclusively; this method ensures a swift reply on the condition of the transaction result. It is an ideal technique for dealing with singular transactions.

Transaction Processing System Features

There are several features involved in a good transaction processing system. A few of these critical features are described below.

- **Performance:** The concept behind the use of TPS is to efficiently generate timely results for transactions. Effectiveness is based on the number of transactions they can process at a particular time.
- **Continuous availability:** The transaction processing system should be a very stable and reliable system that must not crash easily. Disruption of TPS in an organization can lead to work disturbance and financial loss.
- **Data integrity:** The TPS must maintain the same method for all transactions processed, the system must be designed to effectively protect data and overcome any hardware/ software issues.
- **Ease of use:** The TPS should be user-friendly in order to encourage the use and decrease errors from inputting data. It should be structured in such a way that it makes it easy to understand as well as guarding users against making errors during data-entry.
- **Modular growth :** The TPS hardware and software components should be able to be upgraded individually without requiring a complete overhaul.
- **Controlled processing:** Only authorized personnel, staff members, or employees should be able to access the system at a time.

Components of Transaction Processing System

Below are some of the components involved in a Transaction Processing System:

a. **Inputs:** These are source documents gotten from transactions which serve as inputs into the computer's accounting system examples are invoices, and customer orders.

b. **Processing:** This requires the breaking down of information provided by the inputs.

c. **Storage:** This is saved information in TPS memory, it may be in the form of ledgers.

d. **Output:** Any generated record may serve as the output.

Limitations of Transaction Processing Systems

- Managing operations with the Transaction Processing System can be complicated if the company is not big enough to efficiently use the transaction processing system.
- Transaction Processing System needs both hardware and software components to efficiently manage high data volume. This capacity makes TPSs susceptible to software security breaches in the form of the virus and faulty hardware issues such as power outage can disrupt the whole system.

- Effective integration of a Transaction Processing System in a company operation requires skilled personnel, it also requires a link with associate company branches to maintain a secure flow of information. This high requirement can create instability and flux in the company's daily operations.

Functions of Transaction Processing System

Transaction Processing Systems can execute input, output, storage, and processing functions.

- *Input functions*: This includes the securing of data on the source document, entering of input data in the system and validate data.
- *Output functions*: This includes the production of the report of the transaction via monitor or paper, examples are exception reports, detail reports, and summary reports.
- *Storage functions*: This is the process by which data is stored. It entails the storage of information, accessing, sorting, and updating stored data.
- *Processing functions*: This entails the transformation of data, it includes calculation, computation, and apt result.

Examples of Transaction Processing System

- TPS accumulates data about transactions and initiates processing that transforms stored data. Examples include order processing, employee records, and hotel reservation systems.
- Batch transaction process examples include bill generation and check clearances.
- Examples of real-time transaction processes are the Point-of-Sale terminals (P.O.S) and microfinance loan systems.

5. Office Automation System

Office Automation Systems (OAS) are configurations of networked computer hardware and software. A variety of office automation systems are now applied to business and communication functions that used to be performed manually or in multiple locations of a company, such as preparing written communications and strategic planning.

In addition, functions that once required coordinating the expertise of outside specialists in typesetting, printing, or electronic recording can now be integrated into the everyday work of an organization, saving both time and money.

Types of functions integrated by office automation systems include

(1) electronic publishing;

(2) electronic communication;

(3) electronic collaboration;

(4) image processing; and

(5) office management.

At the heart of these systems is often a Local Area Network (LAN). The LAN allows users to transmit data, voice, mail, and images across the network to any destination, whether that destination is in the local office on the LAN, or in another country or continent, through a connecting network.

An Office Automation System makes office work more efficient and increases productivity. Office management systems include electronic office accessories, electronic scheduling, and task management. These systems

provide an electronic means of organizing people, projects, and data. Business dates, appointments, notes, and client contact information can be created, edited, stored, and retrieved. Additionally, automatic reminders about crucial dates and appointments can be programmed.

Projects and tasks can be allocated, subdivided, and planned. All these actions can either be done individually or for an entire group. Computerized systems that automate these office functions can dramatically increase productivity and improve communication within an organization.

Benefits of an Office Automation System

Implementing an office automation system offers organizations a broad range of benefits. These benefits include:

a. ***Improved accuracy:*** Humans make errors, properly implemented automated systems do not. Human errors are not only inefficient in that they must be corrected and lead to productivity delays, but they can be costly. For instance, adding too many digits when paying an employee or vendor. Serious mistakes can lead to security and compliance issues, potentially fines and penalties. An office automation system limits human intervention in the transfer of data, which minimizes the occurrence of errors.

b. ***Reduced costs:*** By automating complex business processes, organizations do not need to invest as much into hiring for those tasks. As a result, operational costs are lower, while productivity and profit margins are significantly higher.

c. ***Reduced time and resources:*** Through automation, organizations can accomplish more with less. By eliminating tedious and time-consuming processes, employees can spend their time on more high value tasks. For example, returning to the popular paperless benefit, with office automation software employees do not need to spend as much time collecting important documentation, entering that information, or filing away voluminous paper copies. The system does it for them.

d. ***Data storage and management:*** Office automation systems simplify data storage while giving organizations the ability to monitor and control data through an electronic document management system. Common features include things like task management and reminder systems, as well as easy access to information by key stakeholders.

e. ***Data insights and more informed decisions:*** Office automation systems give organizations access to large data sets, reports, and analytics. Access to data enables more informed decisions. Moreover, by analyzing data and key performance indicators, organizations can implement improvements to their processes to remove bottlenecks and other inefficiencies.

f. ***Business Process Improvement:*** Through business process improvement, organizations optimize performance, improve the quality of their products or services, and ensure a higher level of compliance. The ability to improve business processes is what separates office automation systems from piecemeal automation technology.

Key features of an Office Automation System

There are countless applications and software programs that promise improved efficiency through automation. An office automation system should offer following features:

a. **Process modeling and workflow design:** An important benefit of an office automation system is the ability to design and improve workflows. The solution that you choose should give you the ability to create detailed workflows in a matter of minutes.

b. **Mobile compatibility :** In the age of the stay-at-home economy and the COVID-19 pandemic, mobility is more important than ever. Employees must be able to perform their functions from anywhere. A cloud-based solution is always secure and always accessible.

c. **Integration :** One of the biggest challenges that organizations face when attempting to automate their processes is integrating various third-party software or apps. The office automation system should work seamlessly with your other tools like email marketing and CRM system.

d. **Managing tasks and deadlines:** Task management is an important feature of office automation solutions. For processes to run smoothly, employees must know what to do and when to do it. The office automation system should allow to create and view pending tasks and deadlines, as well as redistribute tasks as needed.

e. **Access control and security:** To protect the security of office systems, it is required to set access privileges throughout the organization. Cloud-based solutions also offer advanced security features to protect data from being compromised.

f. **Communication:** An important feature of any automation system is the ability to communicate seamlessly. Stakeholders should have all the information they need to perform each task, as well as the ability to reach out to others for further assistance.

   The office automation system should offer features like a form builder. Form builders can be used to capture data, display data from other systems, and even design approval screens for managers to make decisions.

g. **Reporting and analytics:** To evaluate and improve the office automation system, access to data and key performance indicators is required.

APPLICATION OF INFORMATION SYSTEMS IN BUSINESS

Advances in computer-based information technology in recent years have led to a wide variety of systems that managers are now using to make and implement decisions. By and large, these systems have been developed from scratch for specific purposes and differ significantly from standard electronic data processing systems. Too often, unfortunately, managers have little say in the development of these decision support systems, at the same time, non-managers who do develop them have a limited view of how they can be used.

Information Systems in Daily Life

Daily Life Situation	*Application of information Systems*
E-Learning	E-learning or electronic learning is an information system that is applied in schools. The application of data that is processed and disseminated through technology. There are many benefits from the presence of information system applications in the field of education, including convenience. The convenience offered not only saves time but also saves paper.
Fleet Management System	The fleet management system is an information system application that will assist the process of monitoring the logistics fleet and delivery of goods so that the tracking process becomes more systematic and continues to be centralized. Usually, this system responds to the detected location by using the help of GPS.
Integrated Service System for Students	This student service system was created to facilitate student activities on campus activities. One of the activities is to obtain results from academic activities in the form of tests or other activities. In addition, the application of this information system can also facilitate the registration of the desired courses each semester. Students do not need to come directly to campus to carry out these activities. These students are only enough to open the available applications.

Daily Life Situation	*Application of information Systems*
Online Booking	Next is the application of information systems in placing orders online. Reservations that can be made online can be in the form of transportation tickets, concert tickets, and hotels. Apart from these things, many other things can be ordered online, either on a website or an application. The way it works is also very easy, one only needs to choose what things they want to order online. Later that person will get evidence in the form of a successful booking. After the evidence is obtained, the person can immediately exchange the existing ticket.
Enterprise Resource Planning	Also called ERP or management systems, they are systems that focus on the administration of the production and distribution of goods generated by a company, and allow to keep track of sales, invoicing, shipments, and many other concepts related to production. As a result of the information processing, the information issued allows top management to make decisions that can positively affect a company. This is an example of a company management information system that not many ordinary people know about. This information system is widely used by several companies because it facilitates their activities. Many large companies have used this system. This system functions in terms of monitoring or supervision of company management. Furthermore, this system is also connected to the fields of work units in finance, marketing, operations, and others. Things that used to take a long time can now be done in a short time.
Artificial Intelligence	One of these information systems was previously used by companies. Artificial Intelligence or artificial intelligence greatly facilitates the transaction process in the company. Seeing the sophistication of A.I, it is not surprising that many have applied this to other places. Perhaps the most widely heard and most often heard is that AI is applied to mobile phones. The way this system works is to solve existing problems with the knowledge of the experts who have been included in it. So, the system that is processed to produce this information still comes from humans as well.
Video Call	This is an information system where the application is on the cellphone. The way it works is extraordinary, it is easy to just download an application that provides video call facilities. Then just register via telephone number. Currently, many applications provide video call facilities, even though these facilities are already built-in on mobile phones. Usually, this video call facility is integrated with a chat application that uses internet quota as a means. So, to make this video call make sure you have an internet connection.

Some of the target areas of implementation of Information Systems are as follows:

a. **Commercial systems.** Better known as point of sales, this type of system is used by economic establishments to keep track of sales and business expenses, facilitates accounting, and allows managers to find weak points that need to be addressed.

b. **Geographic information systems.** These systems model large amounts of information that enable decision-making in fields such as environmental impact, urban planning, or cartography.

c. **Banking systems.** These systems allow the use of monetary transactions quickly between multiple customers regardless of the physical location where they are located or even regardless of the bank of which they are customers.

d. **Communication systems.** Here we can group all the systems that allow us to send and receive information from our friends, colleagues, neighbors, and even people we do not even know physically. A clear example of this type of system is social networks, instant messaging, or e-mail.

e. **Content Management Systems.** The so-called CMS allows us to create and manage content quickly and to some extent easily, that is, it is not necessary to be a web programmer to create a complete structure for a site. As an example, a CMS called Sharepoint hosts the institutional portal and its entire structure of web pages.

f. **Learning Management Systems.** LMS is very similar to CMS, the difference is that they allow creating of educational content and keeping track of a student, using activities ranging from publishing news or events to discussion forums and evaluations that allow automatic grading of the student.

g. **Streaming systems**. YouTube, Spotify, or Netflix are mainly a source of entertainment, they provide a continuous information flow (stream) to the customer and allow them to watch or listen to content from the network.

INFORMATION SYSTEMS AND SECURITY

Technology is a huge part of how business is done, so managing corporate and customer data is a top priority for companies. As this intervention of technology in business is continuously increasing at high pace, it become most essential to keep the data secured and make policies related to data security.

Following should be adhered to while focusing on maintaining security of information system:

a. **Confidentiality:** When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality.

   Confidentiality is the ability not to disclose information to unauthorized persons, programs, or processes. It relates to information security because it requires control over access to protected information. Confidentiality requires measures to ensure that only authorized persons have access to information, and while unauthorized persons are denied access to them. Simply put, confidentiality means that something is secret and should not be passed on to unintentional persons or organizations.

   If confidentiality is compromised, this can lead to loss of privacy and disclosure of confidential information to the public or other persons. There is a wide range of information that could be considered confidential, such as financial information, medical information, and other sensitive information. Some information is more sensitive than others and requires a higher level of confidentiality.

b. **Integrity:** Integrity means that protection against improper modification and destruction of information, ensuring that information cannot be changed undetected, and ensuring the integrity of the information. This means that a cyber threat or vulnerability to cyber-attack can be measured by compromising one or more of its principles. Integrity is based on encryption and hashing to ensure the best possible protection against cyber-attacks and cyber threats such as cyber espionage.

c. **Availability:** Availability ensures that information is available to those in need that includes timely and reliable access, regardless of the time of day, place of residence, location, or other factors.

The accuracy and completeness of the information are crucial to the functioning of an organization. Focus on integrity to ensure that data is considered authentic and reliable and cannot be manipulated. It should be noted that integrity is important in order to protect data in its use, not only in the management of the organization but also in its use by other organizations and individuals.

LESSON ROUND-UP

- Information systems encapsulates the tools that organizations use to collect, manage, and analyze data and encapsulates Hardware, Software, Data and Telecommunication Networks as its components.
- Implementation of Information System in the organisation can be in four ways i.e., Direct Cutover, Parallel Operation, Phased Operation and Pilot Operation.
- Information System will induce innovation in business activities through its research and development. It will also enable automation, reducing steps undertaken to complete a task.
- An executive information system is a management support system that facilitates and supports the decision-making requirements of an organization's senior executives. Hence, it is also called an "executive support system."
- Decision support systems are interactive software-based systems intended to help managers in decision-making by accessing large volumes of information generated from various related information systems involved in organizational business processes, such as office automation system, transaction processing system, etc.
- A management information system is a computerized database of financial information organized and programmed in such a way that it produces regular reports on operations for every level of management in a company.
- Transaction processing is a style of computing, typically performed by large server computers, that supports interactive applications. In transaction processing, work is divided into individual, indivisible operations, called transactions.
- Office automation systems are configurations of networked computer hardware and software.
- ERP or management systems, are systems that focus on the administration of the production and distribution of goods generated by a company, and allow to keep track of sales, invoicing, shipments, and many other concepts related to production.

  Three aspects for system security should be focuses on are Confidentiality, Integrity, and Availability.

GLOSSARY

Telecommunications: Telecommunication is used to connect with the computer system or other devices to disseminate information.

Executive Information System (EIS): It is a management support system that facilitates and supports the decision-making requirements of an organization's senior executives.

Model Management System: It stores and accesses models that managers use to make decisions. Such models are used for designing manufacturing facility, analyzing the financial health of an organization, forecasting demand of a product or service, etc.

Expert System: An expert system provides managers with insights and advice based on Artificial Intelligence (AI).

Knowledge Management System (KMS): helps organizations facilitate the collection, recording, organization, retrieval, and dissemination of knowledge.

Fleet Management System: The fleet management system is an information system application that will assist the process of monitoring the logistics fleet and delivery of goods so that the tracking process becomes more systematic and continues to be centralized.

Artificial Intelligence: Artificial Intelligence or artificial intelligence greatly facilitates the transaction process in the company. Seeing the sophistication of A.I, it is not surprising that many have applied this to other places.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What do you mean by Information System and How it can be implemented in small business?
2. Utilization of Information Systems in small-size and mid-size firms is minimal." Justify the statement.
3. Information System does not only mean application of software. Elaborate the statement.
4. How information systems are benefiting businesses to perform more effectively and efficiently.
5. What are various types of Information Systems?
6. How Management Information System and Decision Support System are interrelated?
7. Transactions are easy to process through information systems. Justify the statement.
8. Office automation system comes with numerous of features. Briefly enumerate such features.
9. All 5 types of Information Systems are inter-related and inter-connected. Explain such inter-relatedness amongst all Information Systems in your own words.
10. Write a note on application of Management Information System in Small Business.

Management Information Systems – An Overview

Lesson 13

KEY CONCEPTS

■ Management ■ Information ■ System ■ Management Information System ■ Expert System ■ Decision Support System ■ Transaction Process System ■ Management Support System ■ Office Automation System

Learning Objectives

To understand:

- The meaning of Management Information System
- Components of Management Information System
- Utilization of Management Information System in Indian Business World
- Management Information System and its relation with other Information Systems
- Management Information System and its Application in Different Spheres of Business

Lesson Outline

- Definition of Management Information System
- Components of Management Information System
- Utilization of Management Information System in Indian Business World
- Management Information System and Its relation with other Information Systems
- Application of Management Information System
- Management Information System and Security
- Lesson Round-Up
- Glossary
- Test Yourself

INTRODUCTION

Management Information Systems (MIS) is the study of people, technology, organizations, and the relationships among them. MIS is a people-oriented field with an emphasis on service through technology. The system gathers data from the internal and external sources of an organisation.

One of the most important tools which aims to provide reliable, complete, accessible and understandable information to managers for effective decisions making and improving business performance is Management information system. The use of management information systems has become necessary for every organization to facilitate the work procedures and improve efficiency and productivity and improve performance in general.

Moreover the importance of management information systems comes from the benefits that generated by that system such providing useful information in a timely manner, improved labor productivity, cost savings, providing the information without any delays and mistakes, and improved the management of work.

A formal method of collecting timely information in a presentable form in order to facilitate effective decision making and implementation, in order to carryout organisational operations for the purpose of achieving the organisational goals." – Walter I. Kennevan

An MIS is a system designed to provide selected decision-oriented information needed by management to plan, control and evaluate the activities of the corporation. It is designed within a framework that emphasises profit planning, performance planning and control at all levels.

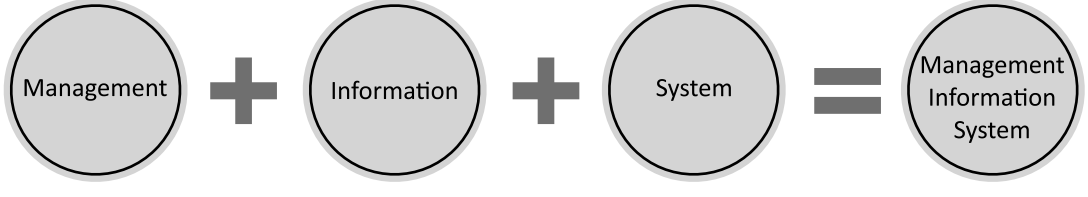
It contemplates the ultimate integration of required business information, sub systems both financial and non-financial within the company"

– Management Information System Committee of the Financial Executive Institute

"Management information system is a computer-based information system that provides for management-oriented reporting based on transaction processing and business operations of the organization."

– Nowduri & Al-Dossary

A Management Information System is an acronym of three words, viz., Management, Information, System.



1. **Management:** Management is the art of getting things done through and with the people in formally organised groups.
2. **Information:** Information is data that is processed and is presented in a form which assists decision making.it may contain an element of surprise, reduce uncertainty, or provoke a manager to initiate an action.

   Data usually take the form of historical records. In contrast to information, raw data may not be able to surprise us, may not be organised and may not add anything to our knowledge.

3. **System:** The term system is the most loosely held term in management literature because of its use in different contexts. However, a system may be defined as a set of elements which are joined together to achieve a common objective. The elements are interrelated and interdependent.

Evolution of the Concept of Management Information System

The earliest use of information system was in a Sumerian temple in the third millennium B.C., to record receipts and issues of grain to individuals out of the temple grain store. But the information system had its fast growth in the last few centuries.

Even though the concept was introduced as a single highly integrated system, it was Later demonstrated to be too complex to implement; and now it is considered as a combination of subsystems conforming to overall plan, standards, and procedures of the organization.

Expansion in organisation size, professionalism, development of technology, etc., is a great fillip to the evolution of the management information system. After the invention of computers, they have been playing a predominant role in MIS.

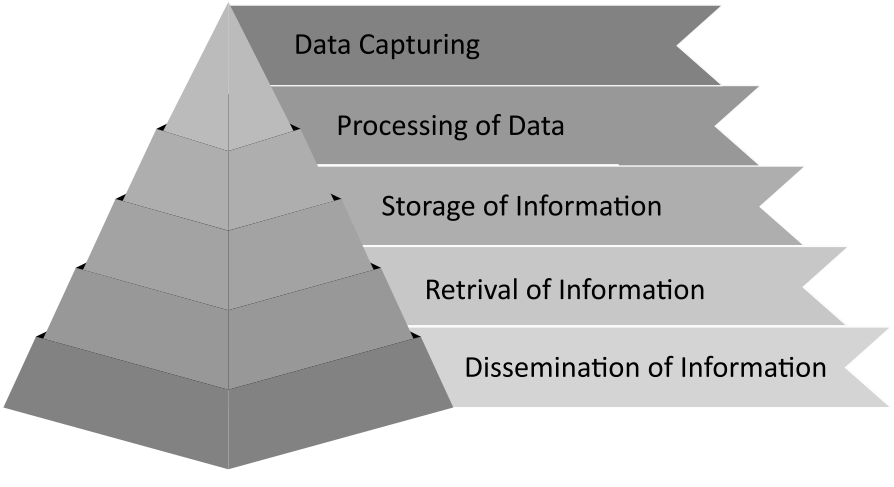
Advancement of computer hardware and software led to the wider application of MIS. Thus, MIS commonly came to be referred to as Information Reporting System since it was mainly used to produce reports for managerial purposes.

In the 1970's, improvements in database technology paved the way for Decision Support System (055), office automation technologies like word processing, desktop publishing, electronic mail, etc. By 1980, Information Technology attained greater momentum, which led to the further development of MIS as a strategic weapon. At present, rather than a single, global MIS, an organization may have many related information system, serving the various managerial needs.

The periods of evolution and the changing focus of MIS are traced below:

Period	*Major Focus*	*Main Functions*
1950-1960	EDP	Transaction processing, record keeping and accounting
1960-1970	IRS	Information Reporting
1970-1980	DSS	Decision Support
1980-Onwards	EIS and KBS	Special information needs of top management and use of artificial intelligence in problem solving

Objectives of Management Information System



a. **Data Capturing :** MIS capture data from various internal and external sources of the organization. Data capturing may be manual or through computer terminals.

b. **Processing of Data:** The captured data is processed to convert into the required information. Processing of data is done by such activities as calculating, sorting, classifying, and summarizing.

c. **Storage of Information:** MIS stores the processed or unprocessed data for future use. If any information is not immediately required, it is saved as an organization record, for later use.

d. **Retrieval of Information:** MIS retrieves information from its stores as and when required by various users.

e. **Dissemination of Information:** Information, which is a finished product of MIS, is disseminated to the users in the organization. It is periodic or online through a computer terminal.

Characteristics of Management Information System

Following are the main characteristics of Management Information System:

a. **System approach:** The management information system follows a System approach. The system's approach implies a holistic approach to the study of the system and its performance to achieve the objective for which it has stood formed.

b. **Management-oriented:** For designing MIS top-down approach should follow. The top-down approach suggests that system development starts from the determination of the management needs and overall business objectives. Management-oriented characteristic of MIS also implies that the management actively directs the system development efforts.

c. **Need-based:** The design of the MIS should be as per the requirements of managers at different levels that are strategic planning level, management control level, and operational control level.

d. **Exception-based:** MIS should develop with the exception-based reporting principle. This means an abnormal situation, that is the maximum, minimum or expected values vary beyond the limits. In such cases, there should be exceptions reporting to the decision-maker at the required level.

e. **Future-oriented:** Besides exception-based reporting, MIS should also look at the future. In other words, MIS should not merely provide past or historical information. Rather it should provide information based on projections based on which actions may initiate.

f. **Integrated:** Integration means taking a comprehensive view of the subsystems that operate within the company and it is significant because of its ability to produce more meaningful information.

   For example, to develop an effective production scheduling system, it is necessary to balance such factors as set-up costs, workforce, overtime rates, production capacity, inventory level, capital requirements, and customer services, so that meaningful and reliable information can be derived by the managers working in such production scheduling system.

g. **Common data flows:** Because of the integration concept of MIS, there is an opportunity to avoid duplication and redundancy in data gathering, storage, and dissemination. System designers are aware that a few key source documents account for much of the information flow. For example, customer's orders are the basis for billing the customer for the goods ordered, setting up accounts receivables, initiating production activity, sales analysis, sales forecasting, etc.

Advantages of Management Information System

Following are the benefits being offered by Management Information System to the organisations:

a) **Increased Efficiency**: One of the primary advantages of MIS is that it can help organizations become more efficient. MIS systems automate many routine tasks, freeing up employees to focus on higher-level tasks. This can save time and reduce errors, ultimately leading to cost savings for the organization.

b) **Improved Decision-Making:** MIS systems provide organizations with real-time data and analytics, which can help managers make more informed decisions. For example, an MIS system can provide data on sales trends, inventory levels, and customer preferences, allowing managers to make decisions based on facts rather than intuition.

c) **Enhanced Communication:** MIS systems can improve communication within an organization. For example, an MIS system can provide a centralized platform for employees to share information, collaborate on projects, and coordinate tasks. This can help teams work more effectively and achieve their goals more efficiently.

d) **Better Data Management:** MIS systems can help organizations better manage their data. For example, an MIS system can provide tools for data entry, storage, and retrieval. This can help ensure data is accurate, up-to-date, and easily accessible when needed.

e) **Competitive Advantage:** MIS systems can provide organizations with a competitive advantage. By using data and analytics to make informed decisions, organizations can become more efficient, more responsive to customer needs, and better able to compete in the marketplace.

Disadvantages of Management Information System

Despite of various advantages and benefits provided by the Management Information System, there are some disadvantages as well which are associated with it, following are some disadvantages of implementing management information system:

a) **Costly Implementation**: Implementing an MIS system can be costly for organizations. There may be expenses related to purchasing software, hardware, and training employees to use the system. This can be a significant investment for some organizations.

b) **Technical Issues:** MIS systems can experience technical issues, such as system crashes or data loss. This can be frustrating for employees who rely on the system to do their jobs. Organizations may need to invest in additional technical support to address these issues.

c) **Security Risks:** MIS systems can also pose security risks. If the system contains sensitive data, such as customer information or financial records, it could be targeted by cybercriminals. Organizations need to ensure that their systems are secure and take steps to protect against potential data breaches.

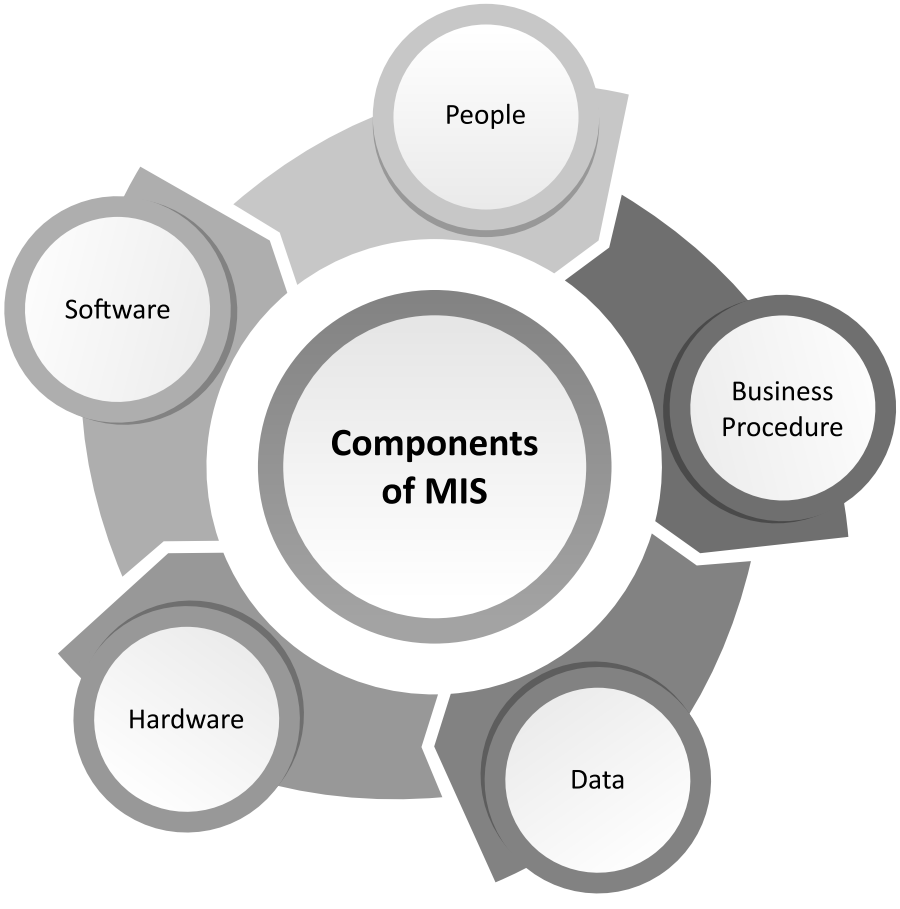
d) **Dependence on Technology:** MIS systems are dependent on technology, which means that if the system goes down, employees may not be able to perform their job duties. This can lead to lost productivity and revenue for the organization.

e) **Potential for Human Error:** MIS systems can be prone to human error. If employees enter incorrect data or fail to update the system in a timely manner, it can lead to inaccurate data and decision-making. This can be a significant issue for organizations that rely heavily on data to make informed decisions.

COMPONENTS OF MANAGEMENT INFORMATION SYSTEM

A management information system is made up of five major components namely people, business processes, data, hardware, and software. All these components must work together to achieve business objects.

a) **People:** People are the users who use the information system to record the day-to-day business transactions. The users are usually qualified professionals such as accountants, human resource managers, etc. The ICT department usually has the support staff who ensure that the system is running properly.



b) **Business Procedures**: Business procedures are agreed upon best practices that guide the users and all other components on how to work efficiently. Business procedures are developed by the people i.e., users, consultants, etc.

c) **Data:** Data encapsulated the recording of day-to-day business transactions. For example, for a bank, data is collected from activities such as deposits, withdrawals, loans, credit cards etc.

d) **Hardware:** Hardware is made up of physical components like the CPU, printers, networking devices, etc. The hardware provides the computing power for processing data. It also provides networking and printing capabilities. The hardware speeds up the processing of data into information.

e) **Software:** Software are programs that run on the hardware. The software is broken down into two major categories namely system software and applications software. System software refers to the operating system i.e., Windows, Mac OS, and Ubuntu, etc. Applications software refers to specialized software for accomplishing business tasks such as a payroll program, banking system, point of sale system, etc.

MIS and Its Functional Subsystems

Based on organizational functions, subsystems can be divided into various categories. Since MIS is a federation of subsystems each organisational function can have a subsystem. Each of these functional systems is unique in its procedures, programmes, models etc. The functional subsystems of MIS are:

I. **Production subsystem:** It deals with production of data reports, and makes production planning, scheduling, and cost control analysis.

II. **Marketing subsystem:** It collects data for sales forecasting and planning. It includes data relating to distribution cost, promotion cost, etc.

III. **Finance and accounting subsystem:** It keeps data on customer credit, accounts payable, accounts receivable, cash management, fund allocation, etc.

IV. **Personal (HRO) subsystem**: This subsystem is concerned with planning personnel requirements, analysing performance, salary administration, etc.

V. **Information processing subsystem:** It focuses on information system planning, cost-effectiveness analysis, etc.

VI. **R&D subsystem:** It deals with research and development activities in an organization.

UTILIZATION OF MANAGEMENT INFORMATION SYSTEM IN INDIAN BUSINESS SCENARIO

Management Information Systems provide the owner and other decision-makers at a business with the data needed to make informed decisions for the company. A MIS provides background, current data, and trend analysis so you have ready information on all areas of the business.

Information systems gain their importance by processing the data from company inputs to generate information that is useful for managing your operations.

Management information system can be utilised in below mentioned manner for more efficient utilisation of such information system:

1. **Business Communication System**: Part of management is gathering and distributing information, and information systems can make this process more efficient by allowing managers to communicate rapidly. Email is quick and effective, but managers can use information systems even more efficiently by storing documents in folders that they share with the employees who need the information. This type of communication lets employees collaborate in a systematic way.

   Each employee can communicate additional information by making changes that the system tracks. The manager collects the inputs and sends the newly revised document to his target audience.

2. **Business Operations Management**: How the company's operations are being managed are highly depended on information such company managers possess. Information systems can offer more complete and more recent information, allowing managers to operate the company more efficiently, one can use information systems to gain a cost advantage over competitors or to differentiate itself by offering better customer service. Sales data give sales managers insights about what customers are buying and let one knows stock or produce items that are selling well. With guidance from the information system, company can streamline your operations.

3. **Company Decision-Making**: The company information system can help decision maker to make better decisions by delivering all the information one need and by modelling the results decisions taken. A decision involves choosing a course of action from several alternatives and carrying out the corresponding tasks. When company's decision makers have accurate, up-to-date information, they can make the choice with confidence.

If more than one choice looks appealing, managers can use information system to run different scenarios. For each possibility, the system can calculate key indicators such as sales, costs, and profits to help them to determine which alternative gives the most beneficial result.

4. **Company Record-Keeping**: Company needs records of its activities for financial and regulatory purposes as well as for finding the causes of problems and taking corrective action. The information system stores documents and revision histories, communication records and operational data. The trick to exploiting this recording capability is organizing the data and using the system to process and present it as useful historical information. Users can use such information to prepare cost estimates and forecasts and to analyze how your actions affected the key company indicators.

Role of Management Information System in Decision Making

Management information systems can help the decision maker to make valid decisions by providing accurate and up-to-date information and performing analytic functions. The user has to make sure the management information system that has been chosen can work with the information formats available within the company and has the features the organisation need. Suitable management information systems can structure the basic data available from the company operations and records into reports to present users with guidance for the decisions.

Following points highlights how Management Information System assist the organisations in decision making:

1. **Information from Company Operations:** When the base of decisions on data available from management information systems, it reflects information that comes from the operations of the company. Management information systems take data generated by the working level and organize it into useful formats. Management information systems typically contain sales figures, expenses, investments, and workforce data. If one need to know how much profit the company has made each year for the past five years to decide, management information systems can provide accurate reports giving you that information.

2. **Capability to Run Scenarios:** The capability to run scenarios is a key decision-making tool. Some management information systems have this feature built in, while others can provide the information required for running scenarios on other applications, such as spreadsheets. The decision is influenced by what happens if decision maker decide a certain way. What-if scenarios show you how different variables change when one plan.

   The manager can enter reduced staff levels or increased promotion budgets and see what happens to revenue, expenses, and profit for different levels of cuts or increases. Management information systems play a critical role in making realistic scenarios possible.

3. **Projections to Assist in Decision Making:** Any decisions decision maker make result in changes in the projected company results and may require modifications in the business strategy and overall goals. Management information systems either have trend analysis built in or can provide information that lets managers carry out such an analysis. Typical business strategies include projections for all fundamental operating results.

   A trend analysis allows the managers to show what these results would be in the current situation and how they will change once you have implemented the decisions decision maker have taken. The new values form the basis of your strategic approach going forward.

4. **Implementation and Evaluation:** While decisions made with specific goals in mind and have the documentation from management information systems and trend analysis to support your expectations, the managers must track company results to make sure they develop as planned. Management

information systems gives the data the managers need to determine whether the decisions have had the desired effect, or whether decision maker must take corrective action to reach organisation's goals. If specific results are not on track, managers can use management information systems to evaluate the situation and decide to take additional measures if necessary.

MANAGEMENT INFORMATION SYSTEM AND OTHER INFORMATION SYSTEMS

Information System is a computer or manual-based system used to store and process data into information or knowledge. O'brien and Marakas (2010:4) also explain that Information System can be defined as a combination of individuals, hardware, software, telecommunication network, data, and policy procedures used to store and receive data to be subsequently transformed into information in an organization. Thus, it can be said that Information System is related and interconnected components/elements to gather, change and spread processed data result useful for an organization in decision-making.

An Information System depends on human resources (system users and system developers), hardware (machinery and media), software (programs and procedures), data (data and knowledge base) and network (telecommunication and network support).

On the other hand, Management Information System is a group of users, procedure, software, database, and devices that provide information for managers and decision makers. Management Information System refers to a system that changes data into useful information for managers and other users. Management Information System is a system providing feedback on organisations activities and supporting managerial decision making. From the experts' opinion, it is concluded that Management Information System is a set of Hardware, Software, database, procedures, user and interconnected and integrated telecommunication network in processing data into useful information to support managerial decision-making process.

The management information system is not something distinct and separate from other information systems. It provides a general framework based on the information systems that are compatible with each other. Over time it became clear that it is very difficult to implement the concept of a fully integrated system.

Management Information System encapsulates other information systems to assist the managers to take well informed and proper decision, management information system utilizes other information systems to derive data and help management to take decisions, following are some vital information systems that are part of management information system:

1. **Expert System:** An expert system provides managers with insights and advice based on artificial intelligence (AI). In an expert system, the AI is trained to simulate the knowledge of a human expert in a particular field.

2. **Decision Support System:** Decision support systems (DSS) are interactive software-based systems intended to help managers in decision-making by accessing large volumes of information generated from various related information systems involved in organizational business processes, such as office automation system, transaction processing system, etc.

   DSS uses the summary information, exceptions, patterns, and trends using the analytical models. A decision support system helps in decision-making but does not necessarily give a decision itself. The decision makers compile useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions.

3. **Transaction Process System:** Transaction processing is a style of computing, typically performed by large server computers, that supports interactive applications. In transaction processing, work is divided into individual, indivisible operations, called transactions.

A transaction processing system allows application programmers to concentrate on writing code that supports the business, by shielding application programs from the details of transaction management

4. **Management Support System:** The Management Support System stores and organizes data, enabling end users to generate reports and analyze data to address business needs and inform planning. A data warehouse is an example of a Management Support System.

5. **Office Automation System:** Office automation systems (OAS) are configurations of networked computer hardware and software. A variety of office automation systems are now applied to business and communication functions that used to be performed manually or in multiple locations of a company, such as preparing written communications and strategic planning.

APPLICATIONS OF MANAGEMENT INFORMATION SYSTEM

Today's business managers are faced with an abundance of information. Information as data processing system must be able to understand, diagnosis, maintenance, and retrieval. On the other hand, systems management, and monitoring tools changes manifolds over the time.

Information is crucial in solving organizational problems and non-enterprise, Management Information Systems remain as consultants interacted with the users and administrators are not inevitable.

A Management Information Systems supports various levels of management (individual and group), from top managers to lower managers and supports all decision process level and various styles of deciding.

One of the major utilisations of management information system is in education sector and Smooth MIS application in educational institutions can be implemented with the following conditions:

- Crucial and demanded by the majority of university personnel processes primary inclusion in the plan of university automation which performance is impossible without IT application.
- MIS is not created for one or two managers.
- MIS application responsibility division between administrative personnel, developers, and employees.
- Advanced development of administrative and educational problems solution techniques and technologies focused on IT application.
- Necessary resources (material and human) allocation for high-grade pre-project inspection, analysis, and technical designing of MIS components.
- Standardizations and documenting of all automation stages.
- University structure reorganization and processes re-engineering management.
- Firm belief about transition to modern information technologies inevitability creation in university collective.
- Parameters system creation, which will allow defining an extent of goals achievement in the field of MIS application.
- Economic and other kinds of MIS effects on university's activities estimation.

In consideration of the technical aspects the most suitable conception for MIS creation is rather popular during last year's ideas of integration connected with WEB-technologies use. The concept of WEB-technologies or WEB-services allows uniting various technologies in the uniform information environment and is deprived negative sides of other integration technologies.

Applications of Management Information System in Service Sectors

Customer satisfaction is the main goal of the service industry while this is not true for the manufacturing industry and varies from industry to industry. To maintain its position in the market and remain ahead of others the industry must provide services that are distinct in nature. The service industry must know the services that are required, perceptions and expectations. It must also perform customer and market research to identify the segments that it is going to serve. It is also necessary to carry out the research on perceptions, requirements, and expectations on a regular basis for enhancing and upgrading the facilities provided by the services because the demands for services are dynamic in nature as compare to products.

In the service industries, Management Information System (MIS) gives its prime focus on the services that are needed to the people. Hence, a continuous monitoring should be done in order to understand the changes occurring to the services demand based on level and scope.

A regular scrutiny should be done to understand what the customer perceives by good service. After that a strategy should be adopted that will address the perception of good service to a customer. With the help of the MIS, the management can provide services. of the highest level by understanding the needs that enhances the communication, physical and human related processes to maintain this level.

Information systems are also used in the service sector for process automation in order to take competitive advantages over the others. The information system that is being used differs from service to service. Some of these services are listed below:

a. **Hospital Information Systems :** Hospital's management provides distinctive services to a wide variety of customers having different perceptions and expectations regarding the services. Discrimination can be easily carried out by the customers regarding various aspects such as personal and medical treatment (quality of caring and quality of care), effective and efficient service and service provided at minimum cost. Customer mainly focuses on the result of the service and appraises the management on the performance of service process.

   So it is concluded that, "Hospital Information System (HIS) is a computerized system that regulates all the medical and administrative information processing activities in order to achieve an efficient and effective work performance by health professionals of a hospital."

   The hospital information system is also known as Integrated Hospital Information Processing System (IHIPS) because it integrates various components like Clinical Information System (CIS), Financial Information System (FIS), Laboratory Information System (LIS), Nursing Information System (NIS), Pharmacy Information System (PIS), etc.

b. **Hotel Information System:** People generally take the service of the hotels when they are visiting some other place and do not have a place to stay there. It is a place where a person can stay conveniently. However, in the recent times there have been several changes in the concept of hotel due to several causes. People always search for differentiated services in a hotel.

   One of the common problems that are faced by the managers of hotels is regarding differentiated service to the customers. The prime objective of any hotel is to offer a room with the basic facilities and amenities to the customer and ensure that the stay is comfortable. The hotel gets a successful business if the most of the rooms are occupied and the visitors take those services that can be billed separately. The hotel business is said to perform well if its occupancy and turnover is high.

   The Management Information System that is used in the hotels helps in understanding the expectations and perceptions of the customers.

Following are the main responsibilities of Hotel Information System:

- Keep Track of the Customer Profile;
- Monitoring Occupancy Level;
- Project Future Needs;
- Monitor the Level of Expectations;
- Monitor the Communication Needs;
- Customer Database.

c. Banking Information System: Banks are organisations that provide various types of financial services such as savings, clearing checks. and providing loans to the account holders. The function of the bank in today's world has increased as they are offering financial assistance to the customers by offering various policies. The bank also has to meet various socio-economic obligations.

The banks handle many transactions which are different from each other in terms of complexity and length. Like the customer of any other service, the customer of the bank also expects to get the end results as fast as possible.

The prime service that is offered in the banking industry is to solve the financial problems that the customers of the bank are facing. The time elapsed for executing a transaction is the most widely used measurement for performing a service. The MIS in a bank must be designed in such a manner that it is able to provide differentiated services to the varied service requests of the customers.

Factors and Requirements Affecting Bank Information System Design:

- Customer Database;
- Service to the Account Holders;
- Service for Business Promotions;
- Index Monitoring System;
- Human Resource Upgrade.

Management Information System and Other Academic Disciplines

Many ideas of MIS are found in various other academic disciplines. Four major areas related to MIS are:

(i) ***Management Accounting*** **vs.** ***MIS*****:** Management accounting is concerned with determining relevant costs and performing other analyses useful for managerial decision making and control. It tends to be the focus for the preparation of budgets and performance analysis. Historically, the accounting development is always responsible for data processing. Management accounting knowledge is of great help in ascertaining the information requirements, carrying analysis in designing forms for processing, procuring, and providing information. Thus, the MIS concept includes much of the content of management accounting.

(ii) ***Operations Research*** **vs.** ***MIS*****:** Operations research is the use of scientific methods and quantitative analysis to solve the problems of management. It has a significant relationship with MIS since it has developed procedures for analysis and computer- based solutions to decision problems. The systematic approach to problem solving, use of models, and computer-based solution algorithms are generally incorporated in the Decision Support System of MIS.

(iii) ***Management Theory* vs. *MIS*:** There were several management theories-Behavioral, Empirical, Quantitative, Decision theory and Management process. Out of these, decision theory and management process are the more relevant to MIS. According to decision theory, the most important task of managers is to take decisions. Under the management process concept, management is defined as what managers do. The knowledge of these theories enabled the MIS designers to ascertain the type of decisions made and functions performed by executives in business organizations.

(iv) ***Information Technology* vs. *MIS*:** Computer science is used in information systems to provide accurate and speedy information to the managers. Information technology facilitated the growth of MIS. It is important because it covers topics such as algorithms, computation software, and data structures. Today, computer has a major role in data processing. So, computer technology has been considered a major factor for MIS development.

MANAGEMENT INFORMATION SYSTEM AND SECURITY

Information system security refers to the way the system is defended against unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

There are two major aspects of information system security –

a. *Security of the information technology used* – securing the system from malicious cyber-attacks that tend to break into the system and to access critical private information or gain control of the internal systems.

b. *Security of data* – ensuring the integrity of data when critical issues, arise such as natural disasters, computer/server malfunction, physical theft etc. Generally, an off-site backup of data is kept for such problems.

Information systems bring about immense social changes, threatening the existing distributions of power, money, rights, and obligations. It also raises new kinds of crimes, like cyber-crimes.

Following organizations promote ethical issues –

- The Association of Information Technology Professionals (AITP);
- The Association of Computing Machinery (ACM);
- The Institute of Electrical and Electronics Engineers (IEEE);
- Computer Professionals for Social Responsibility (CPSR).

LESSON ROUND-UP

- Management Information Systems (MIS) is the study of people, technology, organizations, and the relationships among them. MIS is a people-oriented field with an emphasis on service through technology.
- The management information system follows a System approach. The system's approach implies a holistic approach to the study of the system and its performance to achieve the objective for which it has stood formed.
- Management Information System (MIS) can improve communication within an organization. For example, an MIS system can provide a centralized platform for employees to share information, collaborate on projects, and coordinate tasks. This can help teams work more effectively and achieve their goals more efficiently.

- A management information system is made up of five major components namely people, business processes, data, hardware, and software.
- Information systems can offer more complete and more recent information, allowing managers to operate the company more efficiently, one can use information systems to gain a cost advantage over competitors or to differentiate itself by offering better customer service.
- Management information systems gives the data the managers need to determine whether the decisions have had the desired effect, or whether decision maker must take corrective action to reach organisation's goals.
- The Management Support System stores and organizes data, enabling end users to generate reports and analyze data to address business needs and inform planning. A data warehouse is an example of a Management Support System.
- A Management Information Systems supports various levels of management (individual and group), from top managers to lower managers and supports all decision process level and various styles of deciding.
- In the service industries, Management Information System (MIS) gives its prime focus on the services that are needed to the people. Hence, a continuous monitoring should be done in order to understand the changes occurring to the services demand based on level and scope.

GLOSSARY

System: The term system is the most loosely held term in management literature because of its use in different contexts. However, a system may be defined as a set of elements which are joined together to achieve a common objective. The elements are interrelated and interdependent.

Information: Information is data that is processed and is presented in a form which assists decision making. it may contain an element of surprise, reduce uncertainty, or provoke a manager to initiate an action.

People: People are the users who use the information system to record the day-to-day business transactions. The users are usually qualified professionals such as accountants, human resource managers, etc. The ICT department usually has the support staff who ensure that the system is running properly.

Business Procedures: Business procedures are agreed upon best practices that guide the users and all other components on how to work efficiently. Business procedures are developed by the people i.e., users, consultants, etc.

System software: It refers to the operating system i.e., Windows, Mac OS, and Ubuntu, etc.

Applications software: It refers to specialized software for accomplishing business tasks such as a payroll program, banking system, point of sale system, etc.

Operations Research: It is the use of scientific methods and quantitative analysis to solve the problems of management. It has a significant relationship with MIS since it has developed procedures for analysis and computer- based solutions to decision problems.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. What do you understand by Management Information System? Write a brief note.
2. What are important components of Management Information System? Discuss in detail.
3. "Role of Management Information System in organisation in manifold." Comment on Statement with example.
4. Despite of many advantages, management information system does suffer from various limitations. Write briefly upon the limitations of management information system.
5. How management information system and executive information system differ from each other?
6. "Management Information System and other Information System compliments each other in effective decision making." Comment on Statement with appropriate example.
7. "Management Information System is vital for small & mid-size firms as well." Discuss.
8. Explain the relationship between management information system and other academic disciplines.
9. How the concept of Management Information System got evolved. Also explain MIS evolution in relation to computer technology.
10. How management information system is helping service sector to maximise customer satisfaction?

Enterprise Resource Management

Lesson 14

KEY CONCEPTS

■ Enterprise Resource Planning ■ Mobile ERP ■ Cloud ERP ■ Predictive Analytics

Learning Objectives

To understand:

- The concept and meaning of Enterprise Resource Planning
- The advantages and disadvantages of Enterprise Resource Planning
- The functioning of an ERP system
- How to analyse the Before ERP and after ERP position of organisations
- The different types of ERP system modules
- The ERP related technologies
- The planning, evaluation and selection of ERP systems
- An overview of the recent trends in ERP

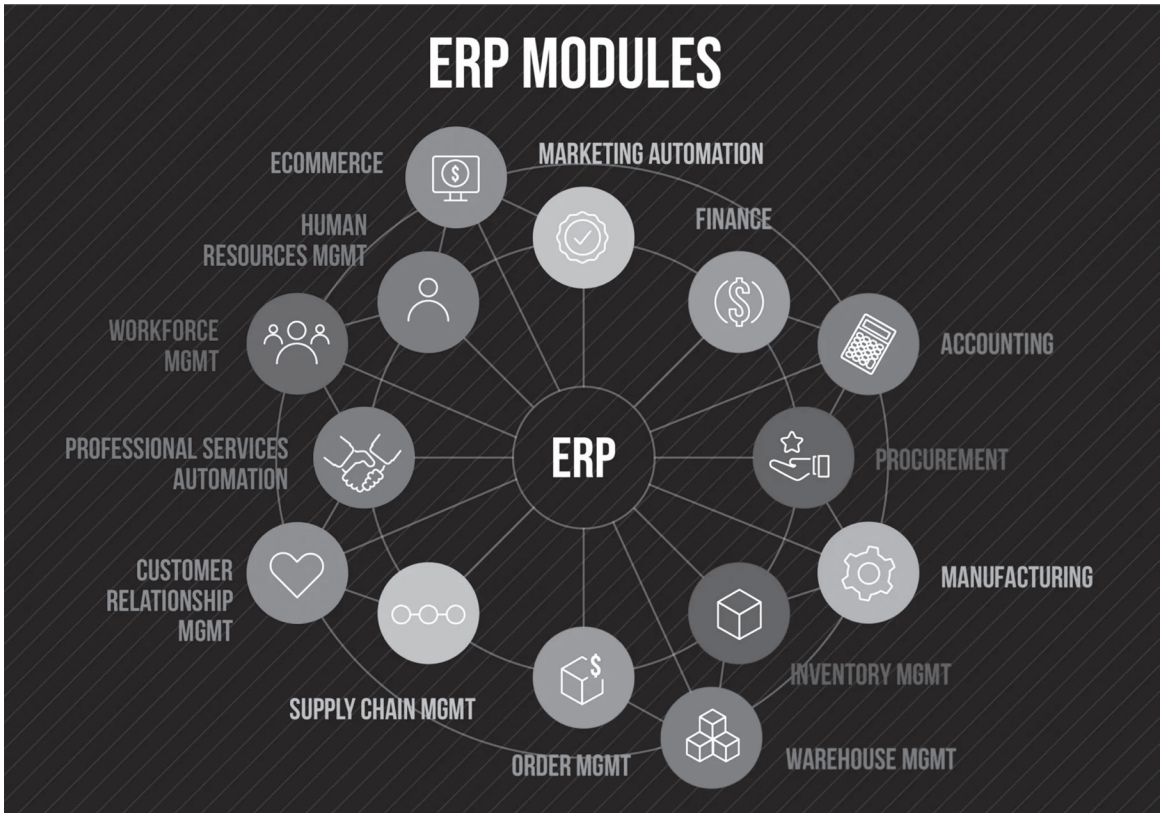
Lesson Outline

- Enterprise Resource Management: Introduction
- Understanding Enterprise Resource Planning
- Significance of ERP
- How ERP works
- Before ERP and After ERP
- Benefits of ERP
- Limitations of ERP
- ERP related Technologies
- Types of ERP system modules
- Planning Evaluation and Selection of ERP systems
- Recent trends in ERP: 2023
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

ENTERPRISE RESOURCE MANAGEMENT: INTRODUCTION

Enterprise Resource Planning ("**ERP**") is a type of software which is used by businesses and organisations to automate and manage the day-to-day business activities and operations such as manufacturing, accounting, procurement, supply chain operations, risk management and compliance management. ERP is a platform that is used by companies to manage and integrate the essential parts of their businesses. Many ERP software applications are critical to companies because they help them implement resource planning by integrating all the processes needed to run their companies within a single system.

Enterprise Resource Planning (ERP) is business process management software that allows an organization to use a system of integrated applications to manage the business and automate many back-office functions related to technology, services and human resources.



Source: https://www.stampli.com/blog/accounting/erp-modules-integrations/

ERP software typically integrates all facets of an operation — including product planning, development, manufacturing, sales and marketing — in a single database, application and user interface.

An ERP software system can also integrate planning, purchasing inventory, sales, marketing, finance, human resources, and more.

Key Takeaways

- ERP software can integrate all of the processes needed to run a company.
- ERP solutions have evolved over the years, and many are now typically web-based applications that users can access remotely.

- Some benefits of ERP include the free flow of communication between business areas, a single source of information, and accurate, real-time data reporting.
- There are hundreds of ERP applications a company can choose from, and most can be customized.
- An ERP system can be ineffective if a company doesn't implement it carefully.

UNDERSTANDING ENTERPRISE RESOURCE PLANNING (ERP)

It will be appropriate to state that an Enterprise Resource Planning (ERP) system works as the glue that binds together the different computer systems for a large organization. Without an ERP application, each department would have its system optimized for its specific tasks. With ERP software, each department still has its system, but all of the systems can be accessed through one application with one interface.

Significance of ERP

ERP applications also allow the different departments to communicate and share information more easily with the rest of the company. It collects information about the activity and state of different divisions, making this information available to other parts of the company, where it can be used productively.

ERP applications can help a corporation become more self-aware by linking information about production, finance, distribution, and human resources together. Because it connects different technologies used by each part of a business, an ERP application can eliminate costly duplicates and incompatible technology. The process often integrates accounts payable, stock control systems, order-monitoring systems, and customer databases into one system.

How ERP Works

ERP has evolved over the years from traditional software models that made use of physical client servers and manual entry systems to cloud-based software with remote, web-based access. The platform is generally maintained by the company that created it, with client companies renting services provided by the platform.

Businesses select the applications they want to use. Then, the hosting company loads the applications onto the server the client is renting, and both parties begin working to integrate the client's processes and data into the platform.

Once all departments are tied into the system, all data is collected on the server and becomes instantly available to those with permission to use it. Reports can be generated with metrics, graphs, or other visuals and aids a client might need to determine how the business and its departments are performing.

Before ERP and After ERP

In order to better appreciate the ERP process, let us look at the state of affairs which existed within organizations and companies before the ERP came into picture and how after introduction of ERP, companies are able to perform more efficiently and effectively.

Before ERP:

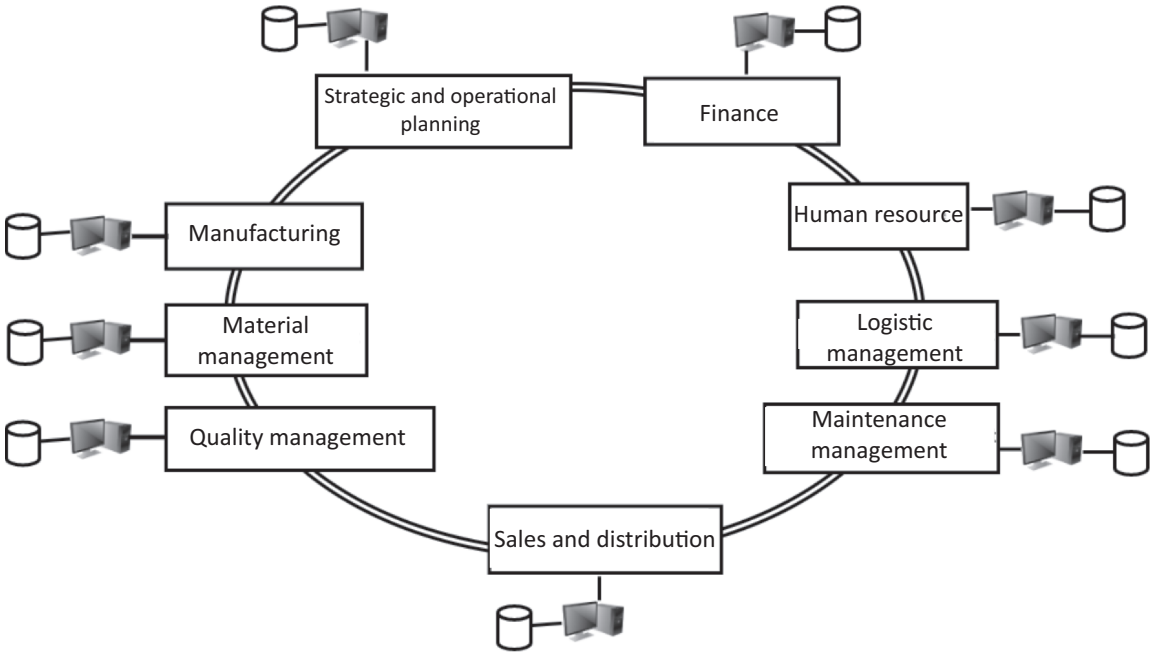


Figure – Before ERP

Before introduction of an ERP system, companies had different databases of different departments which they managed by their own. The employees of one department did not know anything about another department.

After ERP:

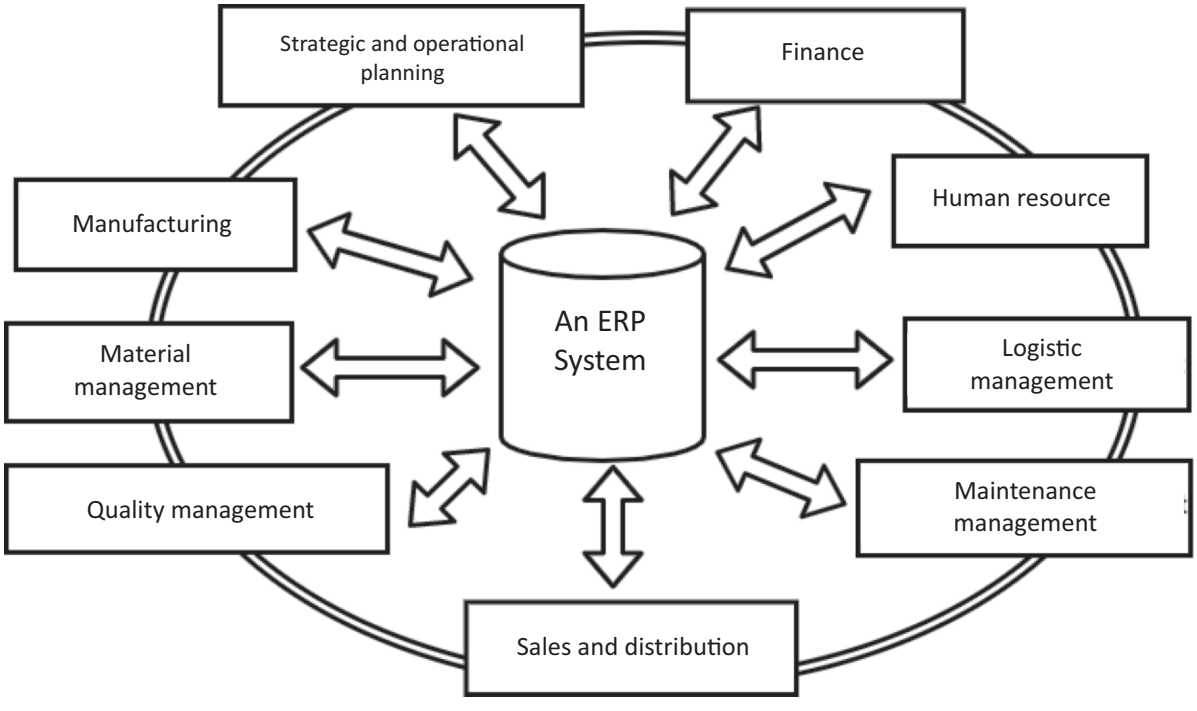


Figure – After ERP

After introduction of ERP system, databases of different departments are managed by one system called ERP system. It keeps tracks of all the database within system. In this scenario, employee of one department have information regarding the other departments.

BENEFITS OF ENTERPRISE RESOURCE PLANNING

There are many advantages to implementing an Enterprise Resource Planning (ERP) software solution. Among countless other advantages, implementing ERP software can improve productivity, increase efficiencies, decrease costs and streamline processes. Businesses employ enterprise resource planning (ERP) for various reasons, such as expanding, reducing costs, and improving operations. The benefits sought and realized between companies may differ; however, some are worth noting, which have been set out herein under:

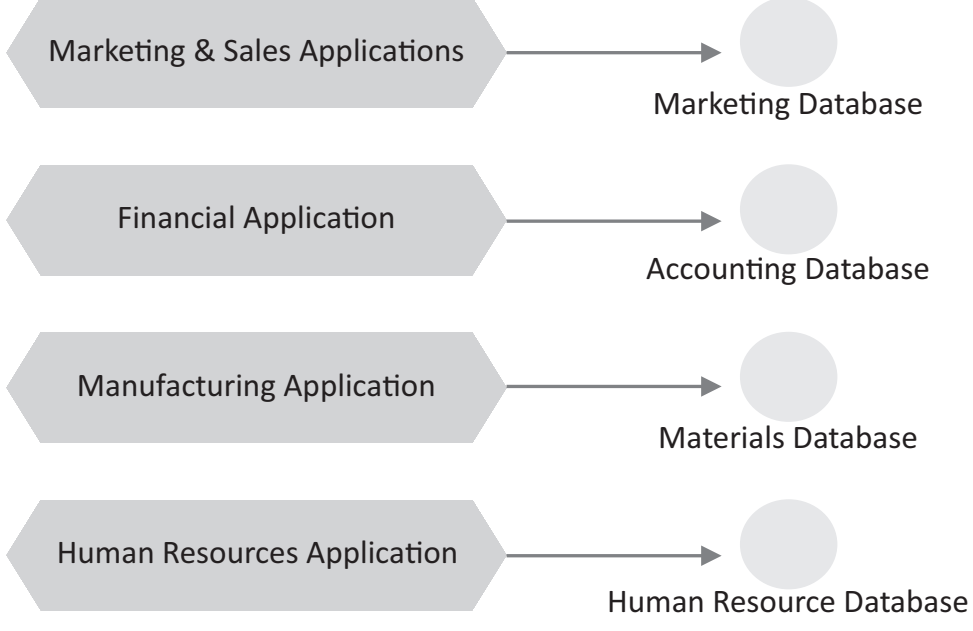
- **Integration and Cost Effectiveness**

  In a nutshell, Enterprise Resource Planning software tries to integrate all the different departments and functions of an organization into a single computer system to serve the needs of different departments.

  The task at hand, of implementing one software program that looks after the needs of the Finance Department together with the needs of the Human Resource Department and the Warehouse, seems impossible. These different departments usually have an individual software program that is optimized in the way each department works.

  However, if installed correctly this integrated approach can be very cost effective for an organization. With an integrated solution, different departments can easily share information and communicate with one another.

  The following diagram illustrates the differences between non-integrated systems versus an integrated system for enterprise resource planning.



Source: https://www.tutorialspoint.com/management_concepts/enterprise_resource_planning.htm#

- **Improves Accuracy and Productivity:** Integrating and automating business processes eliminates redundancies and improves accuracy and productivity. In addition, departments with interconnected processes can synchronize work to achieve faster and better outcomes.
- **Improves Reporting:** Some businesses benefit from enhanced real-time data reporting from a single source system. Accurate and complete reporting help companies adequately plan, budget, forecast, and communicate the state of operations to the organization and interested parties, such as shareholders.
- **Increases Efficiency:** ERPs allow businesses to quickly access needed information for clients, vendors, and business partners. This contributes to improved customer and employee satisfaction, quicker response rates, and increased accuracy rates. In addition, associated costs often decrease as the company operates more efficiently.
- **Increases Collaboration:** Departments are better able to collaborate and share knowledge; a newly synergized workforce can improve productivity and employee satisfaction as employees are better able to see how each functional group contributes to the mission and vision of the company. Also, menial and manual tasks are eliminated, allowing employees to allocate their time to more meaningful work.
- **Competition:** It's true that ERP software requires a major investment, but this cost of investment is nothing as compared to the bigger cost in not making the investment. While some manufacturers choose to stick to the tried-and-tested methods of the past, others seek technology solutions. Manufacturers cannot afford to put off an ERP implementation while their competition invests in ERP and starts reaping the many benefits that ERP offers.
- **Forecasting:** Enterprise resource planning software gives users, and especially managers, the tools they need to create more accurate forecasts. Since the information within ERP is as accurate as possible, businesses can make realistic estimates and more effective forecasts.
- **Collaboration:** Nobody wants to run a siloed business with each department functioning separate from the other. Collaboration between departments is a crucial and often necessary part of the business.

With the data entered into ERP systems being centralized and consistent, there's no reason why departments cannot work together. The software also touches on almost every aspect of a business, thus naturally encouraging collaborative, interdepartmental efforts.

- **Regulatory Compliance:** A benefit of ERP software which sometimes goes unnoticed is how it ties well into regulatory compliance in the manufacturing industry. Powerful ERP solutions will keep track of regulations within the industry and monitor changes in compliance.
- **Flexibility:** Modern ERP software systems are robust, flexible, and configurable. They are not a one size-fits-all proposition but can be tailored to the unique needs of a business. ERP systems also can adapt to the ever-changing needs of a growing business, ensuring you won't have to buy a new solution once your needs change or your business grows.
- **Customer Service:** It's easier to provide high-quality customer service using an enterprise solution, especially when you're using one as well-equipped as Work Wise ERP. Sales and customer service people can interact with customers better and improve relationships with them through faster, more accurate access to customers' information and history. ERP also facilitates access to marketing automation and contact center software, ensuring consistent and simultaneous customers interaction.
- **Security:** ERP systems can help in protection of data. In an ERP system, data is spread across multiple systems with varying levels of security. This is coupled with built-in resources and firewalls, thereby increasing the level of protection and also safeguarding against a single point of failure. ERP system will improve the accuracy, consistency, and security of data, which becomes increasingly important if the company deals with a lot of sensitive data and information.

LIMITATIONS OF ENTERPRISE RESOURCE PLANNING

ERP system has following significant limitations:

- Managers generate custom reports or queries only with help from programmers which causes a delay in transfer and receipt of information quickly, which is essential for making a competitive advantage.
- There is no proper decision-making scenario i.e., these systems provide only the current status, such as open orders. Whenever there is need to look for past status to find trends and patterns that aid better decision making, it becomes difficult.
- No doubt that data is integrated within the system, but there is no integration of data with other enterprise or division systems and it does not include external intelligence.
- High implementation costs: Implementing an ERP system can be expensive and time-consuming. It requires significant investment in hardware, software, and personnel, as well as training and consulting costs.
- Complex customization: Customizing an ERP system to meet the specific needs of an organization can be complex and require specialized knowledge. This can lead to delays and additional costs.
- Resistance to change: ERP systems often require significant changes to an organization's processes and workflows, which can be met with resistance from employees who are comfortable with existing practices.
- Data security risks: Centralizing sensitive business data in an ERP system creates potential security risks, especially if the system is not properly secured or if there are vulnerabilities in the software.
- Limited flexibility: ERP systems are designed to provide standardization and control, which can limit the flexibility of an organization to respond to changing business needs and market conditions.

- Dependence on vendor support: Organizations that use ERP systems are often heavily dependent on the vendor for support, maintenance, and upgrades. This can create a risk of vendor lock-in and limit an organization's ability to switch to other systems or providers.

ERP RELATED TECHNOLOGIES

Before giving you an ERP technologies list, it is very important to understand the typical structure of ERP systems. In a real life, enterprise resource planning solutions consist of dozens of connected applications, databases, modules, APIs etc. However, as any applications, they can be viewed as a structure built of the database, backend or server part and the frontend or the user interface:

- Database – It is where the data about the assets (like the number of products in the warehouse etc.) is stored.
- Backend – It refers to the engine that performs the operations in the system according to the users' request, for example, make a request for the database to make a list of the products and goods on the particular warehouse and render it to the user.
- Frontend – It refers to the graphical interface that allows the users to communicate with the backend and to form the requests and then display the received information.

Note: API or Application Programming Interface, is defined as an interface which enables two applications to interact, communicate and exchange data with each other without any user intervention.

TYPE OF ERP SYSTEM MODULES

Each ERP software module is designed to fit a specific business function by automating and supporting key processes and sharing business data that will help employees do their work. They can be designed to support best practices and standards for the function they are supporting: for example, a finance and accounting module can provide built-in financial controls and support for compliances under the relevant Income Tax laws. Here are the core modules offered by most ERP solutions:

- **Finance and Accounting:** The finance and accounting module is the core module of most ERPs. This module lets you understand the current financial state of the business, prepare and analyze financial statements and reports, and forecast financial performance to make better business decisions. The main functions of the finance and accounting module include accounts receivable, accounts payable, managing the general ledger, and creating and storing financial documents like P&L statements, tax statements, payment receipts, and balance sheets.

  The financial management module automates tasks associated with budgeting, billing, cash flow management, account reconciliation, and supplier payments to help the business remain compliant and close its books on time.

- **Procurement:** The procurement or purchasing module automates the processes associated with buying the materials, products, and services the business needs for its operations. This module can maintain lists of approved vendors, connect vendors with specific categories, goods, or services, track and apply discounts, and maintain supplier contracts. The module helps procurement teams automate requests for a quote, track and analyze quotes received, and prepare and send Purchase Orders (POs) to the selected supplier. Once the PO is issued, the procurement module tracks the PO as the supplier fulfills the purchase order and delivers the goods or services, then updates inventory levels when the order arrives.

- **Manufacturing & Production Management:** The manufacturing module enables production planning and ensures the business has what it needs (raw materials and machinery capacity) for production runs.

During the manufacturing process, the module updates the status of goods-in-progress and tracks actual production output against forecasts. It can also provide real-time status of the shop floor by capturing information on the production process and finished goods. The manufacturing module can assist in planning adequate production by calculating the average time to produce an item and then comparing supply with demand forecasts.

- **Inventory Management:** The inventory control module tracks item quantities and locations down to individual Stock Keeping Units to provide a complete picture of current and incoming inventory (when combined with the procurement module). This module helps manage inventory costs by ensuring sufficient stock without tying up cash in excess inventory. It can also analyze sales trends and compare them to available inventories to help the business make informed decisions to increase inventory turn, boost margins, and prevent stockouts and delays.
- **Warehouse Management:** The warehouse management module guides warehouse employees through processes, including put away when shipments arrive, picking, packing, and shipping. The module can help businesses plan labor based on forecasted order volume and support picking strategies to maximize employee productivity. The warehouse management module is often integrated with inventory management and order management modules to expedite shipping and increase customer satisfaction.
- **Order Management:** The order management module manages customer orders. After a customer place an order, this module transmits it to the warehouse, distribution center, or retail location and tracks the order status as the order is being prepared, fulfilled, and shipped. This boosts the rate of on-time deliveries and prevents orders from being lost, improving customer satisfaction and reducing expediting costs.
- **Supply Chain Management (SCM):** The supply chain module tracks the movement of supplies and goods across the global supply chain. It can provide visibility to every step of the supply chain, from sub-suppliers and suppliers through manufacturers to shippers, distributors, and end customers or retailers. These complex modules can be tightly integrated with other related modules such as procurement, inventory management, and manufacturing. They can also include functionality to manage logistics, trade regulations, and payments.
- **Customer Relationship Management (CRM):** The CRM module stores customer and lead information such as communications history (dates and times of contact), purchase history, and key personnel needed to manage sales leads. The CRM module improves customer service because employees can access customer information while working with a customer. Some CRM modules can also perform analytics and suggest which customers you should target for sales opportunities such as promotions, upselling, or cross-selling.

  Note: Upselling is a sales technique that encourages customers to spend more money by purchasing an upgraded or premium version of the product they originally intended to buy.

  Cross-selling is a sales technique that is used to increase income by persuading the buyer to buy complementary/ancillary products, in addition to their original order.

- **Human Resource Management (HRM):** The human resource management, or human capital management module, helps manage the company's workforce. It stores and maintains employee records and documents such as contracts, job descriptions, offer letters, and performance reviews. It also tracks employee hours and vacation time, paid time off or sick days, and employee benefits information.

  The HRM module may also include a Workforce Management Module that is designed to manage hourly employees. It monitors employee attendance and time and can track and measure productivity and absenteeism.

- **Other Functional Modules:** Some ERP systems may offer additional modules to manage specific business processes. These modules often include:
    - *Professional Services Automation:* Automates and optimizes planning and project management, tracking project status and managing human and capital resources.
    - *Ecommerce:* This module allows companies to launch online B2B or B2C e-commerce websites to enable a business to sell goods and services online. Integration of this module within the ERP system ensures that all payment, order and inventory information is transferred from the ecommerce module into the shared database, which further that ensures all transactions are added to the ledger, out-of-stock items are removed from the site and orders ship on time.
    - *Marketing Automation:* Automatically manages marketing campaigns across digital channels and provides reports and analytics to increase leads and conversions.
    - *Technical Modules of ERP Systems:* Technical modules provide added functionality to the ERP system to facilitate integration across modules and application suites. Common technical modules include
    - *Security Module:* Controls access to the ERP system, manages firewalls and encryption to protect data.
    - *Networking and Interface:* Ensures data flow between the different modules and parts of the ERP system.
    - *Management Information System:* Provides managers with the information and analytical tools they need to make informed decisions.
    - *Application Programming:* Allows businesses to create custom code to extend the functionality of the ERP system.
    - *APIs for External Use:* Allows the integration of third-party applications with the ERP software and facilitates data synchronization.

PLANNING EVALUATION AND SELECTION OF ERP SYSTEMS[1]

As per Wei and Wang (2004), a successful ERP project requires selecting an ERP solution, implementing the solution, managing changes and examining the practicality of the system. Choice of a wrong ERP solution would either lead to failure of implementation or weakening of the system, leading to an adverse impact on the enterprise, according to Hicks, (1995) and Wilson (1994).

Most enterprises often jump into looking at ERP functions and features, without examining their strategy and business processes. It is important for management to know the current strategy, processes and supporting systems of their enterprise to understand what changes can be brought through a new ERP system.

For most enterprises, the decision to implement ERP functionalities will require buying a software package from one of the more popular vendors on ERP market like SAP and Oracle. But the selection process is not a straightforward task, hence thorough understanding of what ERP packages are to offer, differences in each of them and what might be at stake in selecting one package over the other should be well examined.

Evaluating and selecting an ERP system can be a very complex process on the other hand, but it should be a 'fact-based' process that will bring the enterprise to the point where comfortable & well-informed decisions can be made.

1. Reproduced from Digital Notes on Enterprise Resource Planning, Department of Mechanical Engineering, Malla Reddy College of Engineering and Technology.

Therefore, research carried out by Management Agility Inc, (2005), revealed that it is imperative to adopt a thorough evaluation process before adopting any ERP solution in SMEs, i.e. Small and Medium Sized Enterprise.

1. Planning
2. Request For Proposal (RFP)
3. Solution Evaluation
4. Negotiation
5. Selection and Agreement
6. Define Requirements
7. Shop Round for Product
8. Clarify Requirements
9. Evaluation Vendor Inquiry
10. Interact with Vendors
11. Negotiate Agreement
12. Action Agreement.

- Define business case/need and spell-out required values. Be specific. Ensure the business sponsor is willing to push through business case for change.
- Look round the market for what product is available. Identify vendors that operate and their general approaches to technologies. Discuss with others in the same industry as you are etc.
- Clarify your requirements and be sure of whether what you are looking for is in line with your business case. Refine requirements if possible and be specific too.
- Find out what product is looking promising in line with the business need and from which vendor. Identify which vendor and their products suits the requirements and invite interesting ones for demo etc. Request for proposal (RFP).
- Invite each shortlisted vendor over for a chat and find out more about the product. List out expectations based heavily on business requirements.
- At this point evaluate the following approach. Can you afford to change your current process? Can you afford the change the new product will bring ?
- Initiate Negotiation for the selected product with the selected vendor. Agree on who does what, when are they to be done. Negotiate deliverables, timelines, cost & payments schedules and terms, support inclusive.
- Review all legal terms, finalise the contract and select product for onward implementation.
- Alignment of business requirement to what the software/hardware can provide. This is the core of the whole exercise else stop the evaluation.
- Evaluate the product capabilities in line with the business requirement. Evaluate the impact of the product on the business requirement.

Stage 1 - Plan Requirement

Business need is defined, along with areas in business that require technical approach. Develop a specific business case with business value for a solution. Ensure that the project sponsor is willing to articulate the business case for change. Identify vendors that operate in the line of products that you are looking for. Get familiar with the software and hardware infrastructure framework for problem solving. Get general view of investment needed, considering software, hardware, other related infrastructure and ongoing support. Based on the survey, evaluate the organization readiness for the investment and decide whether to continue or not. Now define priorities under "must-have" and "nice-to-have" accordingly.

Stage 2 - Request For Proposals (RFP)

Shortlist interesting vendor based on the outcome of market survey for products. Invite interesting vendors for interaction/demonstration of their products. Collect facts/functionalities in line with the business need from various products demonstrations for the developments of unbiased RFP for vendors. Set-up a neutral body to develop RFP using all facts gathered during products demonstration aligned to the business requirements. Distribute out RFP that addresses the vendor as a company and the products they offer. Generate basic expectations from an ideal proposal in line with the business need for onward selection of the ideal software vendor.

Stage 3 - Solution Evaluation

Identify and prioritize remaining gaps between demonstrated software capabilities and business requirements. Identify how the gaps will be bridged in terms of configuration, configuration, process change or combination of all these. If the gaps can be bridged, consider reengineering of those affected business processes and continue with further evaluation.

Stage 4 - Contract Negotiation

Negotiate with each vendor. Establish software, hardware and other infrastructure agreement requirements, which include version, components, maintenance and support. Also negotiate participation in user groups, license costs, maintenance fees and many others. Establish service provider agreement which also include deliverables, timelines, resources, costs and payment schedules. Establish other legal requirements.

Stage 5 - Selection and Agreement

Upon successful negotiation with the right vendor; Review all legal terms on privacy protection, operation guidance and data manipulation etc. Approve agreements with the selected vendors. Agree on implementation plan.

RECENT TRENDS IN ERP: 2023[2]

1. ***Cloud ERP:*** Historically, many organizations used on-premises ERP applications and were reluctant to entrust core business applications to the cloud, but that's changing rapidly. Businesses are adopting cloud ERP to take advantage of a simpler deployment, lower costs, elasticity (i.e., the ability to only use the necessary resources at any given time), new functionality, less need for internal IT resources, and the ability to easily add users and functions to accommodate business growth.

   The pandemic has further established the value of cloud ERP and accelerated the shift from on-premises software, partly because cloud-based applications allow employees to get their work done

2. Luthar David (2023) 8 ERP Trends for 2023, Oracle Netsuite. Available at https://www.netsuite.com/portal/resource/articles/erp/erp-trends.shtml

from anywhere with an internet connection—they don't need to be in an office. Some CFOs looking to cut costs amid the economic uncertainty are actually increasing investment in cloud ERP to drive savings and better support their remote workforce. A 2020 survey of finance executives indicated that 20% expect to spend more on cloud ERP technologies.

2. ***Two-Tier ERP:*** Historically, many companies tried to deploy a single ERP system for both the headquarters and all regional offices and subsidiaries. But in practice, that approach was often costly and extremely challenging to implement; subsidiaries often had specialized requirements which didn't need the full functionality of the corporate system and struggled with the one-size-fits-all approach.

   That's why two-tier ERP is one of the top ERP trends in 2023. Two-tier ERP is a strategy that enables organizations to leverage their investment in existing ERP systems at the corporate level (tier 1), while subsidiaries and divisions operate using a different ERP solution (tier 2), which is often cloud-based. Larger companies may continue to use their core ERP system for financials and other core processes, while smaller business units turn to solutions that address their specialized needs. The effectiveness of this approach depends in part on the ability to exchange data between the tiers—some tier 2 cloud solutions include built-in capabilities for integration with corporate ERP systems.

   There are a number of benefits to this approach. It's often less costly than retrofitting the corporate ERP system to work for the entire business. A tier 2 solution may be simpler to implement and provide subsidiaries with more flexibility to respond to changing business conditions. In addition, the two-tiered approach may be better suited for organizations in high-growth mode. As Gartner puts it, large organizations should "assess whether a two-tier ERP strategy would offer more business benefit than a single-tier one, especially by modernizing small, potentially fast-growing business units."

3. ***Digital Transformation:*** Digital transformation refers to integrating digital technology into all business functions to improve daily operations. This approach can often boost revenue and competitiveness while increasing employee productivity and improving customer service and communication.

   Since an ERP suite typically touches most areas of a company, it's a logical place to start to facilitate this transformation. Indeed, Accenture's 2020 ERP Trends Report found that three-quarters of U.K. businesses are using cloud ERP as a gateway to modernization. Several of the trends highlighted below—including the integration of ERP with IoT devices and the adoption of AI and advanced analytics—can be considered part of this digital transformation.

4. ***Other Technology Integrated With ERP:*** While modern ERP is the main element in a company's digital transformation, it is only part of a bigger investment in technology. Companies are integrating their business applications with other new technologies, including IoT, to improve core processes. For example, retailers use warehouse management systems that collect data from mobile scanners and smart conveyers to track the movement of goods within the warehouse. Some companies integrate ERP with ecommerce to improve online order workflows, automatically triggering order fulfillment, updating inventory levels and recording payment.

   The year ahead will also see a greater connection between social media and ERP. By seeing the social media activity of customers and prospects in one place, companies can develop a more complete understanding of their audience that allows them to enhance their digital marketing strategies and the customer experience. By integrating data from social media interactions with sales order history and communication with customers, companies can gain more insights about the entire sales process and experiment with new ways to target and sell.

5. ***Personalization:*** Historically, ERP platforms with complex scripting languages were difficult to customize to the specialized needs of each business. But organizations can now take advantage of cloud ERP

platforms designed for easier configuration, or what analysts call "low-code" platforms. There's also a growing range of ERP solutions tailored to suit the needs of specific industries.

As companies focus on delivering more personalized, relevant experiences to customers, they need ERP systems that can accommodate those needs with features like highly customizable dashboards. One emerging trend is the growing popularity of AI-based assistive and conversational user interfaces such as chatbots, which can interpret user voice or text input and respond to questions using customer and order information stored within the ERP.

6. ***AI-Powered Insights and Improvements:*** Artificial intelligence and machine learning capabilities embedded into ERP systems work behind the scenes to help meet increased demand for personalization and improve a broad range of business processes. While companies could add AI functionality to some ERP systems in the past, more vendors now offer ERP software having built-in AI capabilities.

   AI can deliver significant benefits for businesses, including:

   - More insights. As organizations gather more operational and customer data than ever before, they look to AI to deliver valuable business insights based on that information. AI technologies scan vast amounts of unstructured information, quickly identify patterns and predict various trends that wouldn't be possible to spot with manual number crunching alone.
   - Improved processes. AI helps to automate and improve a whole range of processes. For example, consider a manufacturer that adopts a just-in-time inventory strategy, which aims to deliver components at the last possible moment to minimize inventory carrying costs. AI, in the form of machine learning, can optimize the supply delivery and labor schedules to increase productivity and lower costs. IFS's 2019 study found that 40% of manufacturers planned to implement AI for inventory planning and logistics, and 36% intended to use it for production scheduling and customer relationship management.

7. ***Predictive Analytics:*** The hunger for AI-infused ERP highlights organizations' increasing desire to mine their operational and customer data for new and relevant insights that will increase the top and bottom lines.

   While it's always been possible to analyze ERP data to reveal what happened in a business's past, the focus lately has been on using predictive analytics to uncover and address what is likely to happen in the future. For example, software with machine learning capabilities can comb through a maintenance company's data about machine repairs to predict when breakdowns are likely to occur. The organization can optimize maintenance schedules so it services or replaces parts right before they cause problems.

8. ***Mobile ERP:*** ERP providers have offered mobile support for some time, and mobile apps are increasingly becoming the norm. ERP solutions are evolving to provide on-the-go access to critical business data, allowing employees to conduct both back-end and front-end tasks no matter where they are, from the warehouse floor to a retail checkout terminal to an airport. Mobile ERP can also encourage collaboration for dispersed workforces in different time zones.

   Mobile ERP apps designed with a user-friendly interface can help users get work done when they're not in front of a computer. Employees can complete tasks like expense reporting, call logging and time tracking, and they can view the status of critical workflows or approvals from their phones. Mobile ERP offers real-time data and insights and provides overall benefits including always-on remote access, improved productivity, faster and more accurate data capture and increased agility.

LESSON ROUND-UP

- Enterprise Resource Planning ("ERP") is a platform companies use to manage and integrate the essential parts of their businesses.
- Enterprise resource planning (ERP) is business process management software that allows an organization to use a system of integrated applications to manage the business and automate many back-office functions related to technology, services and human resources.
- ERP software can integrate all of the processes needed to run a company.
- ERP solutions have evolved over the years, and many are now typically web-based applications that users can access remotely.
- Some benefits of ERP include the free flow of communication between business areas, a single source of information, and accurate, real-time data reporting.
- There are hundreds of ERP applications a company can choose from, and most can be customized.
- An ERP system can be ineffective if a company does not implement it carefully.
- ERP applications also allow the different departments to communicate and share information more easily with the rest of the company.
- ERP applications can help a corporation become more self-aware by linking information about production, finance, distribution, and human resources together.
- ERP has evolved over the years from traditional software models that made use of physical client servers and manual entry systems to cloud-based software with remote, web-based access.
- The platform is generally maintained by the company that created it, with client companies renting services provided by the platform.
- There are many advantages to implementing an Enterprise Resource Planning (ERP) software solution.
- Among countless other advantages, implementing ERP software can improve productivity, increase efficiencies, decrease costs and streamline processes. Businesses employ enterprise resource planning (ERP) for various reasons, such as expanding, reducing costs, and improving operations.
- In a real life, enterprise resource planning solutions consist of dozens of connected applications, databases, modules, APIs etc.
- Each ERP software module is designed to fit a specific business function by automating and supporting key processes and sharing business data that will help employees do their work.
- ERP software module can be designed to support best practices and standards for the function they are supporting. For example, a finance and accounting module can provide built-in financial controls and support for income tax laws compliance.
- A successful ERP project requires selecting an ERP solution, implement the solution, manage changes and examine the practicality of the system.
- Most enterprises often jump into looking at ERP functions and features rather than examining the strategy and business processes.
- Evaluating and selecting an ERP system can be a very complex process on the other hand, but it should be a 'fact-based' process that will bring the enterprise to the point where comfortable & well-informed decisions can be made.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. Write detailed note on ERP.
2. What are the advantages and disadvantages of ERP system? Discuss briefly.
3. What are future trends in ERP systems? Discuss any 4 in detail.
4. Write Case Study on Before ERP and After ERP Scenario of an organization.
5. Write a short note on ERP System Modules.

LIST OF FURTHER READINGS

- Alexis Leon, "ERP Demystified", Tata McGraw Hill, New Delhi, 2000
- Digital Notes on Enterprise Resource Planning, Department of Mechanical Engineering, Malla Reddy College of Engineering and Technology. Available at https://mrcet.com/downloads/digital_notes/ME/III%20year/ERP%20Complete%20Digital%20notes.pdf
- Jagan Nathan Vaman, ERP in Practice, Tata McGraw-Hill, 2008
- Mahadeo Jaiswal and Ganesh Vanapalli, ERP Macmillan India, 2009.

LIST OF OTHER REFERENCES

- Alexis Leon, Enterprise Resource Planning, second edition, Tata McGraw-Hill, 2008
- ERP Modules and Integrations: Our Complete Field Guide, Stampli. Available at https://www.stampli.com/blog/accounting/erp-modules-integrations/
- Enterprise Resource Planning (ERP), Tutorial Point. Available at https://www.tutorialspoint.com/management_concepts/enterprise_resource_planning.htm#
- Joseph A Brady, Ellen F Monk, Bret Wagner, "Concepts in Enterprise Resource Planning", Thompson Course Technology, USA, 2001
- Kawal, Introduction to ERP, Geeksforgeeks. Available at https://www.geeksforgeeks.org/introduction-to-erp/
- Vinod Kumar Grag and N.K. Venkitakrishnan, ERP- Concepts and Practice, Prentice Hall of India, 2nd edition, 2006.

Internet and Other Technologies

Lesson 15

KEY CONCEPTS

■ Internet ■ Internet Protocols ■ E-commerce ■ Supply Chain Management (SCM) ■ Customer Relationship Management (CRM) ■ Payment Portals ■ Digital Currencies ■ M-Commerce ■ Bluetooth and Wi-Fi

Learning Objectives

To understand:

- The concept of internet and internet technologies
- The different types of internet protocols
- The working of internet protocols
- About e-commerce and its stages of development
- The benefits and limitations associated with e-commerce
- About Supply Chain Management
- The Customer Relationship Management
- The concepts of EFT and EDI
- About digital currencies and its various types
- The Block Chain Technology
- The Payment Portal
- The concept of Mobile Commerce and its various types
- The difference between M-Commerce vs. E-Commerce
- The Future of Mobile Commerce
- The distinction between Bluetooth and Wi-Fi

Lesson Outline

- Internet
- Applications of Internet
- Major Types of Internet Application
- Internet Protocols
- Working of Internet Protocols
- Need of Protocols
- Types of Internet Protocols
- E-commerce and its development
- Benefits and Limitations of E-Commerce
- Types of E-Commerce
- Supply Chain Management (SCM)
- Customer Relationship Management (CRM)
- Electronic Data Interchange (EDI)
- Electronic Fund Transfers (EFT)
- Major Features of Electronic Funds Transfer
- Digital Currency
- Types of Digital Currencies
- Advantages and Disadvantages of Digital Currencies
- Block Chain Technology
- Transaction Process of Block Chain Technology
- Payment Portal
- E-Commerce Security- Mobile Commerce
- Types of M-Commerce
- Working of Mobile Commerce
- M-Commerce vs. E-Commerce
- Future of Mobile Commerce
- Bluetooth and Wi-Fi
- Lesson Round-Up
- Test Yourself
- List of Further Readings
- List of Other References

In 1969, the Government of the United States of America used the internet as a network that could continue to be functional even if some nods were destroyed, as long as information could pass through other nodes.[1] At that point of time, the purpose of the US government for using the internet was to create a net that could enable a network for ensuring the continuous working and functioning of the military node.[2] The purpose of information and communication technology was to introduce and allow universal communication between users of computer and other electronic devices with enabled network at a global platform.[3] Over the years, internet has become an imperative mode of transferring and sharing of information at a global platform, which in turn, also impacts various segments of human life. Business and commercial activities are particularly impacted by developments in information and tele-communication technologies. Hence, rapid developments in information and tele-communication technology have substantially changed the shape of business organizations and given shape to various new technologies, including fibre optics, electronic data exchange, e-commerce[4] and many more alike. Hence, this chapter aims to provide an overview of the Internet, its related technologies and other contemporary technologies.

APPLICATIONS OF INTERNET

Applications that can function or can be used only when connected to the internet are called Internet applications. In other words, it can also be said that such applications are made to run from the Internet itself.

Because all the data of internet applications is stored on their servers, if you want to use these applications then you must have an internet connection. So that through the internet your request goes to the server and in return you get information. You can also exchange your information through these applications.

In any case, you need internet service to use the internet application. Without internet service, you cannot access the information of these applications.

Additionally, to use internet applications, you also need a digital device with an internet connection, only then you can use those applications. Examples of digital devices include smartphones, tablet PCs, laptops, desktops, etc.

Application of Internet: Major Types[5]

An Internet application serves some purpose for end users. It is generally not concerned with how data is actually transmitted between the hosts. Here are some distributed applications that require well-defined application-level protocols:

- Sending and receiving email
- Searching and browsing information archives
- Copying files between computers
- Conducting financial transactions
- Navigating (in your car, smart scooter, smart bike, etc.)

1. The internet began as ARPAnet, a U.S. Department of Defense project to create a nationwide computer network that would continue to function even if a large portion of it were destroyed in a nuclear war or natural disaster. (April 30, 2012), http://www.centerspan.org/tutorial/net.htm.

2. U.S. Government used internet for the first time in its practical use with their defense project in 1969.

3 Anthony Giddens, Runaway World: The Reith Lectures Revisited Lecture 1: (1999). (April 30, 2012),

http://news.bbc.co.uk/hi/english/static/events/reith_99/.

4. J.-H. Wu and T.-L. Hisa, Analysis of E-Commerce Innovation and Impact of Hypercube Model, Electronic Commerce Research and Applications, Vol. 3, 389–404 (2004).

5. See, https://cs.lmu.edu/~ray/notes/inetapps/.

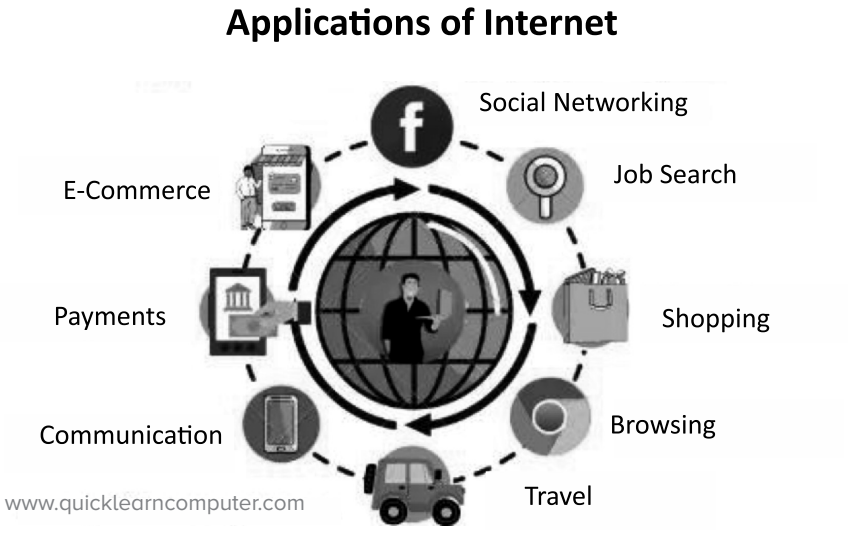
- Playing interactive games
- Video and music streaming
- Chat or voice communication (direct messaging, video conferencing, etc.)

In addition, there are a number of network services such as:

- Name servers
- Configuration servers
- Mail gateways, transfer agents, relays
- File and print servers

Example of Application of Internet[6]

There are various applications of internet in points, which are given below:



- Communication
- Job Search
- Online Shopping
- Web Browsing
- Stock Market Updates
- Travel
- Research
- E-Commerce
- Online Payments
- Social Networking
- E-banking
- Education
- Entertainment

6. Reproduced Pandey Avinash (2022) 10 Applications of Internet. What is Internet Applications. Quick Learn Computers.

INTERNET PROTOCOLS[7]

Internet Protocols are a set of rules that governs the communication and exchange of data over the internet. Both the sender and receiver should follow the same protocols in order to communicate the data. In order to understand it better, let's take an example of a language. Any language has its own set of vocabulary and grammar which we need to know if we want to communicate in that language. Similarly, over the internet, whenever we access a website or exchange some data with another device, then these processes are governed by a set of rules called the internet protocols.

Working of Internet Protocol

The internet and many other data networks work by organizing data into small pieces called packets. Each large data sent between two network devices is divided into smaller packets by the underlying hardware and software. Each network protocol defines the rules for how its data packets must be organized in specific ways according to the protocols the network supports.

> ***Note:*** Hardware refers to all the physical components of the computer system, including the devices connected to it.
>
> Software refers to a set of instructions, data or programs used to operate computers and execute specific tasks.

Need of Protocols

It may be that the sender and receiver of data are parts of different networks, located in different parts of the world having different data transfer rates. So, we need protocols to manage the flow control of data, and access control of the link being shared in the communication channel. Suppose, there is a sender 'X' who has a data transmission rate of 10 Mbps. And, there is a receiver 'Y' who has a data receiving rate of 5Mbps. Since the rate of receiving the data is slow, some data will be lost during transmission. In order to avoid this, receiver Y needs to inform sender X about the speed mismatch so that sender X can adjust its transmission rate. Similarly, the access control decides the node which will access the link shared in the communication channel at a particular instant in time. If not, the transmitted data will collide if many computers send data simultaneously through the same link resulting in the corruption or loss of data.

What is IP Address?

An IP address stands for Internet Protocol address. IP address is a unique address that identifies a device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to improve visual communication between source and destination.

Types of Internet Protocol

Internet Protocols are of different types having different uses. These are mentioned below:

1. TCP/IP (Transmission Control Protocol/ Internet Protocol)
2. SMTP (Simple Mail Transfer Protocol)
3. PPP (Point-to-Point Protocol)

7. Reproduced Kumar Ankit (2023) Types of Internet Protocols, Geeksforgeeks.org.

4. FTP (File Transfer Protocol)
5. SFTP (Secure File Transfer Protocol)
6. HTTP (Hyper Text Transfer Protocol)
7. HTTPS (Hyper Text Transfer Protocol Secure)
8. TELNET (Terminal Network)
9. POP3 (Post Office Protocol 3)
10. IPv4
11. IPv6
12. ICMP
13. UDP
14. IMAP
15. SSH
16. Gopher.

1. **TCP/IP (Transmission Control Protocol/ Internet Protocol):** These are a set of standard rules that allow different types of computers to communicate with each other. The IP protocol ensures that each computer that is connected to the Internet is having a specific serial number called the IP address. TCP specifies how data is exchanged over the internet and how it should be broken into IP packets. It also makes sure that the packets have information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination. The TCP is also known as a connection-oriented protocol.
2. **SMTP (Simple Mail Transfer Protocol):** These protocols are important for sending and distributing outgoing emails. This protocol uses the header of the mail to get the email id of the receiver and enters the mail into the queue of outgoing mail. And as soon as it delivers the mail to the receiving email id, it removes the email from the outgoing list. The message or the electronic mail may contain the text, video, image, etc.
3. **PPP (Point-to-Point Protocol):** It is a communication protocol that is used to create a direct connection between two communicating devices. This protocol defines the rules using which two devices will authenticate each other and exchange information with each other. For example, a user connects his PC to the server of an Internet Service Provider by using PPP. Similarly, for connecting two routers for direct communication, PPP is used.
4. **FTP (File Transfer Protocol):** This protocol is used for transferring files from one system to the other. This works on a client-server model. When a machine requests for file transfer from another machine, the FTO sets up a connection between the two and authenticates each other using their ID and Password. Resultantly, the desired file transfer takes place between the machines.
5. **SFTP (Secure File Transfer Protocol):** SFTP (also known as SSH FTP) refers to File Transfer Protocol (FTP) over Secure Shell (SSH) as it encrypts both commands and data while in transmission. SFTP acts as an extension to SSH and encrypts files and data then sends them over a secure shell data stream. This protocol is used to remotely connect to other systems while executing commands from the command line.

6. **HTTP (Hyper Text Transfer Protocol):** This protocol is used to transfer hypertexts over the internet and it is defined by the 'www' (world wide web) for information transfer. This protocol defines how the information needs to be formatted and transmitted. And, it also defines the various actions the web browsers should take in response to the calls made to access a particular web page. Whenever a user opens their web browser, the user will indirectly use HTTP as this is the protocol which is used to share text, images, and other multimedia files on the World Wide Web. [8]

> ***Note:*** WWW refers to the world wide web, which is a collection of different websites around the world, containing different information shared via local servers (or computers).

7. **HTTPS (Hyper Text Transfer Protocol Secure):** HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network with the SSL/TLS protocol for encryption and authentication. So, generally, a website has an HTTP protocol but if the website is such that it receives sensitive information such as credit card details, debit card details, OTP, etc. then it additionally requires installation of an SSL certificate to make the website more secure. Therefore, before entering any sensitive information on a website, we should check if the link is HTTPS or not. If it is not HTTPS, then it may not be secure enough to share sensitive information.

8. **TELNET (Terminal Network):** TELNET is a standard TCP/IP protocol used for virtual terminal service, provided by the International Organization for Standards (ISO). This enables one local machine to connect with another. The computer which is being connected is called a remote computer and the connecting computer is called the local computer. TELNET operation enables the user to display anything being performed on the remote computer on the local computer. This operates on the client/server principle. The local computer uses the TELNET client program whereas the remote computer uses the TELNET server program.

9. **POP3 (Post Office Protocol 3):** POP3 stands for Post Office Protocol version 3. It has two Message Access Agents (MAAs) where one is client MAA (Message Access Agent) and another is server MAA (Message Access Agent) for accessing the messages from the mailbox. This protocol enables the user to retrieve and manage emails from the mailbox on the receiver mail server to the receiver's computer. This is implied between the receiver and the receiver mail server. It can also be called a one-way client-server protocol. The Pop3 works on two ports, i.e. Port 110 and Port 995.

10. **IPv4:** The fourth and initially widely used version of the Internet Protocol is called IPv4 (Internet Protocol version 4). It is the most popular version of the Internet Protocol and is in charge of distributing data packets throughout the network. Maximum unique addresses for IPv4 are 4,294,967,296 (232), which are possible due to the use of 32-bit addresses. The network address and the host address are the two components of each address. The host address identifies a particular device within the network, whereas the network address identifies the network to which the host belongs. In the "dotted decimal" notation, which is the standard for IPv4 addresses, each octet (8 bits) of the address is represented by its decimal value and separated by a dot (e.g. 192.168.1.1).

> ***Note:*** Dotted Decimal notation is a human-readable representation of IP addresses in the IPv4 (Internet Protocol version 4) format. It is expressed as a series of four decimal numbers, each ranging from 0 to 255, separated by periods (dots). Each decimal number represents an 8-bit binary value (octet), and the entire IP address comprises 32 bits.

11. **IPv6:** The most recent version of the Internet Protocol i.e. IPv6, was created to address the IPv4 protocol's drawbacks. A maximum of 4.3 billion unique addresses are possible with IPv4's 32-bit addresses.

8. Note: Hypertext refers to the special format of the text that can contain links to other texts.

On the contrary, IPv6 uses 128-bit addresses, which enable a significantly greater number of unique addresses. This is significant because IPv4 addresses were running out and there are an increasing number of devices that require internet access. Additionally, IPv6 offers enhanced security features like integrated authentication and encryption as well as better support for mobile devices. IPv6 support has spread among websites and internet service providers, and it is expected to gradually replace IPv4 as the main internet protocol.

12. **ICMP:** ICMP (Internet Control Message Protocol) is a network protocol that is used to send error messages and operational information about network conditions. It is an integral part of the Internet Protocol (IP) suite and is used to help diagnose and troubleshoot issues with network connectivity. ICMP messages are typically generated by network devices, such as routers, in response to errors or exceptional conditions encountered in forwarding a datagram. Some examples of ICMP messages include:

    - Echo Request and Echo Reply (ping)
    - Destination Unreachable
    - Time Exceeded
    - Redirect

    ICMP can also be used by network management tools to test the reachability of a host and measure the round-trip time for packets to travel from the source to the destination and back. It should be noted that ICMP is not a secure protocol, it can be used in some types of network attacks like DDoS amplification.

13. **UDP:** UDP (User Datagram Protocol) a connectionless communication protocol for transporting packets across networks. Unlike TCP, it does not establish a reliable connection between devices before transmitting data, and it does not guarantee that data packets will be received in the order they were sent or that they will be received at all. Instead, UDP simply sends packets of data to a destination without any error checking or flow control. UDP is typically used for real-time applications such as streaming video and audio, online gaming, and VoIP (Voice over Internet Protocol), i.e. a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

    UDP is faster than TCP because it has less overhead. It does not need to establish a connection, so it can send data packets immediately. It also does not need to wait for confirmation that the data was received before sending more, so it can transmit data at a higher rate.

14. **IMAP:** IMAP (Internet Message Access Protocol) is a protocol used for retrieving emails from a mail server. It allows users to access and manage their emails on the server, rather than downloading them to a local device. This means that the user can access their emails from multiple devices and the emails will be synced across all devices. IMAP is more flexible than POP3 (Post Office Protocol version 3) as it allows users to access and organize their emails on the server, and also allows multiple users to access the same mailbox.

15. **SSH:** SSH (Secure Shell) is a protocol used for secure remote login and other secure network services. It provides a secure and encrypted way to remotely access and manage servers, network devices, and other computer systems. SSH uses public-key cryptography to authenticate the user and encrypt the data being transmitted, making it much more secure than traditional remote login protocols such as Telnet. SSH also allows for secure file transfers using the SCP (Secure Copy) and SFTP (Secure File Transfer Protocol) protocols. It is widely used in Unix-based operating systems and is also available for Windows. It is commonly used by system administrators, developers, and other technical users to remotely access and manage servers and other network devices.

16. **Gopher:** Gopher is a type of file retrieval protocol that provides downloadable files with some description for easy management, retrieving, and searching of files. All the files are arranged on a remote computer in a stratified manner. It is an old protocol and it is not used much nowadays.

E-COMMERCE[9]

E-commerce is a process used to distribute, buy, sell or market goods and services, and also transfer the funds online through electronic communication and networks.[10] It facilitates the conduct of commercial transactions electronically at a global level with the help of technologies like internet, electronic data interchange and electronic fund transfer. E-commerce is not only promoting easy access to products and services but also ensures variety of benefits to the sections[11], involved in the e-commerce transactions. Some of the major advantages that e-commerce offers are (a) a large market, (b) extensive access to this large market, (c) easy access to the wide-ranging market of e-commerce porch and alike. These overwhelming benefits of e-commerce market are establishing and sprouting the popularity of e-commerce over the traditional forms of businesses and commerce.

Development of E-commerce

Going back to history, it is important to note that both Electronic Data Interchange and Electronic Fund Transfer were introduced in late 1970s. Introduction of these technologies allowed businesses to send commercial documents like purchase orders, invoices, transactions payments, etc. electronically. In 1979, it was Michael Aldrich who invented the concept of online shopping.[12] In the early 1980s, Credit Cards, Automated Teller Mechanism (ATM) and telephone banking were also developed and they instantly become popular as a form of e-commerce. In 1981, UK launched first B2B[13] online shopping with the introduction of Thomson Holidays.[14] Thereafter, the beginning of 1990 has witnessed the inclusion of enterprise resource planning system,[15] data mining[16] and data warehousing[17] as other categories of e-commerce.

In 1990 only, Tim Berners-Lee invented the concept of World Wide Web, which has transformed the academic telecommunication network into worldwide everyman everyday communication system called the internet.[18] The development of World Wide Web has significantly transformed the use of the Internet. The development

9. Reproduced from Rajvanshi Gargi (2014), Online Privacy vis-à-vis Growth of E-Commerce: A Legal Perspective Study, PhD Thesis submitted for the award of Doctor of Philosophy at Indian Institute of Technology, Kharagpur.

10. eCommerce , eBusiness, Marketing and Design Review; (Online) e-Commerce Optimization. (June 15, 2012), http://www.ecommerceoptimization.com/ecommerce-introduction/

11. Sections here refer as the parties involved in e-commerce transactions. The major parties involved in the e-commerce are Buyers, Sellers and Producers.

12. Ewaryst et al., Internet - Technical Development and Applications, Springer, 255 (2009); ISBN 978-3-642-05018-3. (June 15, 2012), http://books.google.co.in/books/about/Internet.html?id=a9_NJIBC87gCandredir_esc=y

13. Business-to-business (B2B) describes commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.

14. Thomson Holidays is a UK based travel operator and part of TUI Travel PLC.

15. Enterprise resource planning (ERP) systems integrate internal and external management information across an entire organization, embracing finance/accounting, manufacturing, sales and service, customer relationship management, etc. ERP systems automate this activity with an integrated software application. The purpose of ERP is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders. See also, Bidgoli and Hossein, The Internet Encyclopedia, John Wiley and Sons, Inc. Vol. 1, 707 (2004).

16. The overall goal of the data mining process is to extract knowledge from an existing data set and transform it into a human-understandable structure for further use.

17. A data warehouse is a relational database that is designed for query and analysis rather than for transaction processing. It usually contains historical data derived from transaction data, but it can include data from other sources. It separates analysis workload from transaction workload and enables an organization to consolidate data from several sources.

18. Berners-Lee, Tim; Mark Fischetti, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its inventor. Britain: Orion Business. (1999); ISBN 0-7528-2090-7.

of web along with web browsers has opened the access of internet to any person equipped with essential computer understanding, infrastructure and online connectivity.[19]

In 1994, Netscape was introduced, which provided a simple browser to its users to surf the internet and to conduct online transactions secured by a new technology called Secure Sockets Layer.[20] This concept of secured online transactions has served as a basis for development and growth of e-commerce.[21] In 1995, two of the biggest companies 'Amazon.com' and 'e-Bay.com' entered the field of e-commerce.[22] This gave a bounce to B2C[23] commerce. With the contribution of various companies and their presence on the web for the conduct of online transactions, the era of e-commerce has finally ushered in.[24]

Note: B2C commerce or business to consumer commerce refers to a model where a business website is a place where all the transactions take place directly between a business organization and a consumer.

SSL or Secure Sockets Layer is the industry standard when it comes to safe and secure online transactions between websites and users. The SSL technology allows for an encrypted connection to take place between a user's web browser and the web server of the website that the customer is browsing.

Fellenstein and Wood,[25] estimated that in 1996, e-commerce transactions in US earned $707 million which increased to $2.6 billion in 1997 and $5.8 billion in 1998. Though the period of 1998 to 2002 recorded a perceptible fall in the use and growth of e-commerce transactions, yet e-commerce companies survived this roll and again become successful with the beginning of 2002.[26] According to Fraser,[27] 100 companies of U.K. predicted in 2000 that 20% of their revenue would be generated from e-commerce transactions. US Department of Commerce (2002 and 2003) estimated that total e-commerce revenues reached a $45.6 million for 2002 and $54.9 billion for 2003.[28] This trend shows the immense growth in e-commerce businesses.

Indian market of e-commerce is also not an exception. According to a report by IMRB, International and Internet and Mobile Association of India[29] (IAMAI), the e-commerce market in India was expected to be INR 31,598 crore by the end of 2010 which is four times more than the market size of INR 8146 crore back in 2007. Forrester Research Firm has estimated revenue of 1.6 billion US Dollar for Indian e-commerce market in 2012 which is expected to grow at 8.8 billion US Dollar in 2016.[30] 'TECHINASIA' through its report 'Asian E-commerce Sites Net

19. Short Summary of the World Wide Web Project; Groups.google.com, August 6, 1991.

20. Kenney Martin and Curry James, E-commerce: Implication for Firm Strategy and Industry Configuration; E-conomy TM Paper 2, University of California, Economy Project (1999). (June 15, 2012), http://brie.berkeley.edu/econ/publications/wp/ewp2.html.

21. Electronic Commerce, (Online), Reference for Business, Encyclopedia of Business, Eco-Ent. (2nd ed.). (June 15, 2012), http://www.referenceforbusiness.com/encyclopedia/Eco-Ent/Electronic-Commerce.html.

22. See, Garg Pallavi Sharda, E-Tailng in India-Myths, Realities and Marketing Implications, International Journal of Research in Finance and Marketing, Vol.1, Issue 1 (2011).

23. Business to Consumer is a transaction that occurs between a Company and a Consumer, as opposed to a transaction between companies. The term also describes a company that provides goods or services to Consumers.

24. Kim, D.J. et al., A Trust-Based Consumer Decision-Making Model In Electronic Commerce: The Role of Trust, Perceived Risk, And Their Antecedents, Decision Support Systems Vol. 44, 544-564 (2007).

25. Fellenstein, C. and Wood R., Exploring E-Commerce, Global E-Business and E-Societies. Prentice Hall (2000).

26. Cassidy, J. Dot.Com: The Greatest Story Ever Sold, London: Allen Lane; 292-293 (2002): Cassidy has mentioned that the 'gold rush' of the late 1990s came to be known as the 'dot-com bubble,' and 2000 and 2001 saw the bursting of that bubble. From March 10 to April 14, 2000, the NASDAQ, the high-tech stock exchange, dropped 34.2%, and the Dow Jones Composite Internet Index dropped 53.6%. The stock price for all the 20 leading Internet stocks dropped, including Amazon.com by 29.9%, eBay by 27.9%, Internet Capital by 72.1%, and VeriSign by 59.2%.

27. Fraser, J. et al., The Strategic Challenge of Electronic Commerce, Supply Chain Management: An International Journal Vol. 5 No. 1, 7-14 (2000).

28. Johnson Carrie, A Report on The Growth of Multichannel Retailing; A Forrester Document: National Governor's Association and the National Conference of State Legislatures. (June 15, 2012), http://www.gfoa.org/downloads/0407MULTICHANNEL.pdf.

29. Internet and Mobile Association of India (IAMAI). (June 15, 2012), http://www.iamai.in/reports1.aspx.

30. Forrester Report on India to be fastest Growing Market in Asia-Pacific. (June 15, 2012), http://www.iamwire.com/2012/04/india-to-be-the-fastest-growing-e-commerce-market-in-asia-pacific-market-set-to-grow-to-8-8-billion-by-2016/.

$ 6.9 Billion in Past 3 years, But the Exits still Tiny (Stats)' stated that though the e-commerce market in India grew from 43 million US Dollars in 2010 to 138 million US Dollars in first quarter of 2011, but second quarter of 2011 evidenced a fall in e-commerce market and reached to 92 million US Dollars. In the last quarter of 2012, the revenue generated by e-commerce in India 32 US Dollars, wherein second quarter of 2013 evidenced the revenue of 137 million US Dollars in e-commerce in India.[31]

With the theatrical rise and fall of the internet companies, e-commerce has confirmed constant and improved growth in revenues and sale. The development and experience of e-commerce transactions is significantly promoting the advantages not only for the companies and consumers but also for the society as a whole.[32] For companies, e-commerce is improving efficiency, productivity, access to variety of information or data bases and increase in revenues; for consumer, it is providing convenience, ease and 24*7 (24 hours and 7 days) access to product and services; and for society, it is facilitating acceleration of economic growth and opportunities. Hence, a balance in the need, facilitation and difficulties of all the stake-holders will support the growth of e-commerce.

Benefits and Limitations of E-Commerce

Issac Newton's 3rd Law of Motion confirms that 'for every action there is an equal and opposite reaction'. The same principle applies to e-commerce also. The benefits and limitations of e-commerce transactions for (i) businesses, (ii) consumers and (iii) society as a whole have been outlined below:

Benefits

E-commerce serves the following advantages:

- **Increased Convenience:** In e-commerce transactions, consumers can visit multiple websites at any time, be it day or night. With this ease, they can access all e-commerce websites, can compare the prices and availability of goods and services, and make their purchases, without moving from their house or workplace.
- **Increased Choice:** E-commerce transactions have increased consumer's choice for goods and services with their different variety as compared to traditional brick and mortar stores.
- **Enhanced Product Information:** In e-commerce transactions, consumers get an opportunity to analyse information about the particulars of the product like quality, quantity, product performance, durability, drawbacks and limitations of the product.
- **Lower Prices:** The increased competition on e-commerce platforms allows companies to offer goods and services at competitive prices to the customers.
- **Improved Delivery Process:** E-commerce enables faster delivery specially in the electronic goods and services segment where items like software, audio-visual files, access to online journals and books, etc. are quicker and swifter in comparison to the packages delivered by mail or courier.
- **Global Presence:** With the advent of e-commerce, businesses are confirming global presence at global scale in global market.
- **24/7 Opening:** E-commerce business allows business to operate 24 hours a day and seven days a week, which offers competitive advantage over traditional businesses.
- **Reduced Costs:** E-commerce companies are not required to have a building, staff or incur maintenance expenses like physical form of businesses do. Due to the lower operational cost in e-commerce businesses, they are able to provide goods and services at reduced cost.

31. Asian E-commerce Sites Net $ 6.9 Billion in Past 3 years, But the Exits still Tiny (Stats); TECHINASIS, (Mar. 13th, 2014)http://www.techinasia.com/asia-ecommerce-investments-and-exits-2010-to-2013/

32. A Report on Bringing e-commerce benefits to Consumers, by European Commission, The European Parliament, (2011). (June 15, 2012), http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1640_en.pdf.

- **Increased Sales and Profits:** As e-commerce provides 24/7 access to products and services, it provides ease to consumers to transact in e-commerce transactions, which leads to increased sales and profit to e-commerce businesses.
- **Improved Customer Information:** Disclosure of accurate information like name, address, and credit or debit card details, is a compulsory requirement for the completion of e-commerce transactions. Hence, it allows e-commerce companies to collect and store consumers' information, which can be used further for improving their services and for marketing purposes.
- **Economic Benefits:** Running an e-commerce business is economical and cost-effective as it allows businesses to participate in global market, which serves them a greater opportunity to receive revenues at a global platform. Moreover, e-commerce does not demand operational costs like physical store space, maintenance, insurance etc., leading to further savings in cost. All a company needs is an idea, unique product and well-designed web storefront to reach consumers. A combination of these factors provides e-commerce with economic adventure to start with higher margins of profit. Thus, e-commerce transactions have proven to be supportive to growth of economy.
- **Social Benefits:** E-commerce serves a range of benefits to the society in the form of enhanced quality of life by providing services with more convenience and satisfaction. For example, (i) for most of the people, it enables them to work from home and to generate earnings and (ii) it connects people at a global platform.
- **Political Benefits:** E-commerce allows public services like health services (i.e. on-line consultation with doctors and nurses) on internet, filling taxes over internet, filling educational forms and extracting educational guidelines over internet.
- **Technological Benefits:** Introduction of e-commerce in any society will allow people to enhance their IT skills, internet literacy and promote advancement of new technologies through applications on e-commerce.

Limitations of e-commerce can be enumerated as under:

Consumers' Concern about Security and Privacy: Privacy is a critical issue in electronic commerce. E-commerce websites store consumer information to make their online account, which facilitates buying, exchange and return of items purchased on their websites. This information includes personal details like residential address, phone numbers, debit and credit card details, etc. Sharing of such sensitive data raises privacy concerns amongst the customers, who the consumers' privacy concern over their information is supported by various studies and surveys[33] as well.

A Business Week/Harris Poll survey found that over 41% of the online shoppers were very concerned over the use of their personal information. A study conducted by UK Cards Association in 2009 has revealed that fraud losses on UK credit and debit cards caused a loss of 440 million euro to UK based consumers of electronic transactions.[34] Culnan has also argued that privacy concern is a critical reason, which prevents consumers to adopt online transaction or to disclose their information in electronic transactions or to provide false information in the electronic transactions.[35]

- **Lack of Instant Gratification:** A majority of consumers are satisfied with the quality and adequacy of the goods only after they have examined the goods physically. This incentive is not available in e-commerce; as goods can only be seen in virtual form at the time of purchase.

---

33. Public Opinion on Privacy. (June 17, 2012) http://epic.org/privacy/survey/.

34. UK banks do report aggregated fraud losses. In 2009, the total reported losses due to all forms of payment fraud were £440 million (approximately $641 million). Of that total, £59.7 million ($87 million) was attributed to online banking losses. (June 17, 2012), http://www.paymentsnews.com/2010/03/uk-card-and-banking-fraud-losses-down-28-in-2009-to-4403mm.html.

35. Culnan, Mary J., Protecting Privacy Online: Is Self-Regulation Working? Journal of Public Policy and Marketing, Vol. 19, No. 1, 20-26 (2000).

- **Lack of social aspect of Shopping:** Many people like to socialize and they enjoy talking to sales staff, to other shoppers, or to their friends and to take their inputs about the efficiency of product and services while they are out for shopping. This retail therapy does not exist in online shopping to some extent.
- **Inconsistent Return Policies:** Sometimes, consumers suffer on account of poor customer services and return policies in online goods and services. This difficulty is not encountered in traditional physical shopping.
- **Start-up Costs:** Creating a website suitable for an e-commerce undertaking is costly as well as time consuming. There are three major costs involved in starting up of an e-commerce website, namely a) purchasing and updating hardware, b) purchasing and updating software, c) employing a web-designer.
- **Issues with Access:** According to Statista, as of April 2023, there are 5.18 billion internet users worldwide, which amounts to 64.6% of the global population[36]. As everyone is not having access to Internet; limited access to internet may affect the development of e-commerce.
- **Not suitable for all products:** E-commerce is not suitable for some products like perishable goods, food items, furniture[37] etc.
- **Increased Competition:** With the increased access to internet and spreading of online markets, e-commerce companies have to face increased level of competition on a global scale in a global market.
- **Social Limitations:** In e-commerce businesses, as people have to interact electronically, this adversely affects personal and social skills of human interactions. Apart from this, e-commerce may lead to social division, as there are probable threats of increase in social divide between technical haves and have-nots.
- **Economic Limitations:** E-commerce markets are quite competitive, leading to a number of economic limitations, e.g. (i) successful companies of other states may earn revenues from the developing and under developed countries, which may be detrimental to the economy of such countries; (ii) lack of proper and adequate regulatory environment may be detrimental to information privacy of individuals and therefore may slow down the development of e-commerce itself; (iii) in e-commerce businesses, tradition of just-in-time manufacturing and procurement is adopted, hence this could shake the economy in the times of crises[38] as stocks are kept to the minimum requirement and deliveries are not instant in all cases. Economic crisis may also hamper either the delivery of goods or payment of price on the delivery of goods.
- **Political Limitations:** Ecommerce security threats have the potential to cause havoc in online trading. Frauds, tax evasion, impersonation, debit and credit card frauds, eavesdropping and denial of service attacks are some of the threats associated with online transactions. For example e-commerce businesses may lead to the access of obscene material, misuse of individual's information, theft of financial information, entrapping of children, non-identification of parties etc., hence it creates a liability on the state or industry to address the political and legal challenges arising out of such e-commerce transactions.
- **Technological Limitations:** (i) Reliance on telecommunication infrastructure, power and IT skills may nullify the benefits of e-commerce in developing countries where advanced telecommunication

36. https://www.statista.com/statistics/617136/digital-population-worldwide/ (June 5, 2023).

37. Khurana Ajeet, Disadvantages of e-commerce (Online). (June 17, 2012), http://ecommerce.about.com/od/eCommerce-Basics/a/Disadvantages-Of-Ecommerce.htm.

38. See, Choi et al., The Economics of Electronic Commerce, Vol. 18, Macmillan Technical Publications, (1997).

infrastructure, power and IT skills are unavailable, scare or underdeveloped as in developing countries, (ii) the quick development of new technologies may result in wasted resources in the form of disposal of old computers, hardware, software systems etc.

However, despite the various limitations, e-commerce has come to stay in present day business world. Considering its various benefits, it has been accepted as a viable tool for successful business advances.[39] The numerous advantages offered by e-commerce to businesses, consumers and society as a whole over the traditional means of commerce is influencing the growth of e-commerce. According to the market research reports and analysis by IBISWORLD, e-commerce and online auction arena grew 10.4% from 2007 to 2012, with 8.8% more growth expected annually through 2017.[40]

The growth of e-commerce is impacting the Indian commerce market as well. According to Grant Thornton, e-commerce in India is expected to be worth US$ 188 billion by 2025 and with a turnover of US$ 50 billion in 2020, India became the eighth-largest market for e-commerce, trailing France, and a position ahead of Canada[41]. Along with the enormous benefits served by e-commerce to businesses, consumers and to society as a whole,[42] one of the major disadvantages of e-commerce is the probability of loss of information shared by the customers and accessed in e-commerce transactions.

TYPES OF E-COMMERCE (B2B, B2C, C2C AND C2B)

Business models of e-commerce can be classified into the following four models: (1) Business to Business (B2B); (2) Business to Consumer (B2C); (3) Consumer to Consumer (C2C); (4) Consumer to Business (C2B).[43] These models with the possibility of loss of individual's personal data in the transactions are discussed in detail[44] as follows:

(1) Business to Business Model (B2B): The B2B model involves electronic transactions between two businesses for ordering, purchasing, selling or distributing the goods. For example, online retail store 'Amazon' provides an online book store which sells books from various publishers. Here, publishers are making business transactions with Amazon to display and sell their books on the Amazon site to get access to a larger audience. This business transaction between business houses for displaying and selling their books to public at large is a business-to-business model. Under this model, majorly businesses are taking the optimum benefit out of other business houses. As customers' personal information are not involved in this model, so there is minimum possibility of loss of personal information in such B2B model.

(2) Business to Consumer (B2C) Model: The B2C model involves transactions between business organizations and consumers. This implies a model whereby business organizations sell their product or services to consumers over the internet. In this model, e-commerce companies directly deal with the consumers and sell goods and services at consumer's offer and demand. This model includes services like online shopping, online banking, travel services, health information etc. For example, eBay is business website which sells diverse goods and services to public at large through online mechanism. Ebay will display and sell a range of products on their website, i.e., 'www.ebay.com'. Details of all the

39. Yen C-H. and Lu H-P., Factors Influencing Online Auction Repurchase Intention, Internet Research, Vol. 18, No.1, 7-25 (2008).

40. See also, IBISWorld (June 15, 2012), http://www.ibisworld.com/search/default.aspx?st=e-commerce and Business Opportunities in E-commerce, http://www.inc.com/best-industries-2012/judith-ohikuare/ecommerce.html.

41. Indian Brand Equity Foundation, E-commerce Industry in India, Available at: https://www.ibef.org/industry/ecommerce.

42. See, Ray Sarbapriya, Emerging Trends of E-commerce in India: Some Crucial Issues and Challenges, Computer Engineering and Intelligent Systems, Vol. 2, No. 5 (2011).

43. Mahadevan B., Business Models for Internet based E-commerce: An Anatomy, Working paper, Indian Institute of Management, Bangalore. See also, Timmers P., Business Models for Electronic Markets, Electronic Markets, Vol. 8, No. 2, 3-8 (1998).

44. e-Commerce Models. (May 20th, 2013), http://www.eservglobal.com/uploads/files/index.pdf.

products offered for sale will be available in the catalogue maintained by eBay. Any individual who is interested in purchasing those goods and services can visit the website and choose the product from the website catalogue. The catalogue will give information about the product like price, availability, discounts and other information which are essential for consumers to decide regarding the purchase of product. Finally, when the consumer will decide to buy the product, he needs to place the order. For placing the order, the consumer needs to specify his personal details like name, address of delivery and credit/debit card information for completion of the transaction. This system involves business organizations on one side and consumers on the other for the completion of business transactions. By the very nature of conduct of business transactions, B2C model of e-commerce seems to be the most fatal for the infringement of data privacy as enormous amounts of consumer information and database is collected, stored and processed by the e-commerce businesses.[45] Apart from it, B2C model of e-commerce is more prone to security threats because individuals provide their personal information and credit card information for the completion of transactions. In addition to it, consumers might have concerns regarding their personal information and whether it has been secured or used effectively by business organizations or not.[46]

(3) Consumer to Consumer (C2C) Model: The C2C model involves business transactions between consumers. In such model, one consumer sells directly to another consumer. For example, www.olx.in is one of the websites which allows consumers to advertise and sell their products online to another consumer. Here, olx, as an auction website, brings the buyer and seller together to conduct business transactions with a payment of fee by the seller of products.

(4) Consumer to Business (C2B) Model: The C2B is similar to B2C model of e-commerce. C2B model also involves business transactions between consumers and a business organization. In C2B, consumer is the seller and business organization is the buyer. For example in www.monster.com, individuals can post their bio-data for the services they can offer and then any business organization interested in deploying their service can contact individuals and can employ them accordingly.

Apart from the above business models of e-commerce, there are other e-commerce models as well which comes under the category of e-governance like Government to Government (G2G), Government to Consumer (G2C), Consumer to Government (C2G), Government to Business (G2B) and Business to Government (B2G).

SUPPLY CHAIN MANAGEMENT[47]

At the most fundamental level, supply chain management (for brevity, 'SCM') is management of the flow of goods, data, and finances related to a product or service, right from the procurement of raw materials to the delivery of the product at its final destination.

Although many people equate the supply chain with logistics, logistics is actually just one component of the supply chain. Today's digitally based SCM systems include material handling and software for all parties involved in product or service creation, order fulfillment, and information tracking such as suppliers, manufacturers, wholesalers, transportation and logistics providers, and retailers.

Supply chain activities span procurement, product lifecycle management, supply chain planning (including inventory planning and the maintenance of enterprise assets and production lines), logistics (including transportation and fleet management), and order management. SCM can also extend to the activities around global trade, such as the management of global suppliers and multinational production processes.

45. Elliot Steve, Electronic Commerce: B2C Strategies and Models, London, John Wiley and Sons Ltd. U.K. (2002).

46. Timmers P., Business Models for Electronic Markets, Electronic Markets, Vol. 8, No. 2, 3-8 (1998).

47. Fernando Jason (2022) Supply Chain Management (SCM): How it Works and Why It Is Important

Note: Product Lifecycle Management (PLM) is the process of managing the entire lifecycle of a product, right from its inception through the engineering, design and manufacture, as well as the service and delivery of manufactured products. PLM integrates people, data, processes, and business systems and provides a product information backbone for companies and their extended enterprises.

Productivity and efficiency improvements can go straight to the bottom line of a company. Good supply chain management keeps companies out of the headlines and away from expensive recalls and lawsuits. In SCM, the supply chain manager coordinates the logistics of all aspects of the supply chain which consists of the following five parts:

- **Planning:** To get the best results from SCM, the process usually begins with planning to match supply with customer and manufacturing demands. Firms must predict what their future needs will be and act accordingly. This relates to raw materials needed during each stage of manufacturing, equipment capacity and limitations, and staffing needs along with the SCM process. Large entities often rely on ERP system modules to aggregate information and compile plans.
- **Sourcing:** Efficient SCM processes rely very heavily on strong relationships with suppliers. Sourcing entails working with vendors to supply the raw materials needed throughout the manufacturing process. A company may be able to plan and work with a supplier to source goods in advance. However, different industries will have different sourcing requirements. In general, SCM sourcing includes ensuring:
  - the raw materials meet the manufacturing specification needed for the production of goods.
  - the prices paid for the goods are in line with market expectations.
  - the vendor has the flexibility to deliver emergency materials due to unforeseen events.
  - the vendor has a proven record of delivering goods on time and in good quality.

  Supply chain management is especially critical when manufacturers are working with perishable goods. When sourcing goods, firms should be mindful of lead time and how well a supplier can comply with those needs.
- **Manufacturing:** At the heart of the supply chain management process, the company transforms raw materials by using machinery, labor, or other external forces to make something new. This final product is the ultimate goal of the manufacturing process, though it is not the final stage of supply chain management.

  The manufacturing process may be further divided into sub-tasks such as assembly, testing, inspection, or packaging. During the manufacturing process, a firm must be mindful of waste or other controllable factors that may cause deviations from original plans. For example, if a company is using more raw materials than planned and sourced, due to a lack of employee training, the firm must rectify the issue or revisit the earlier stages in SCM.
- **Delivering:** Once products are made and sales are finalized, a company must get the products into the hands of its customers. The distribution process is often seen as a brand image contributor, as up until this point, the customer has not yet interacted with the product. In strong SCM processes, a company has robust logistic capabilities and delivery channels to ensure timely, safe, and inexpensive delivery of products.

  This includes having a backup or diversified distribution methods in case any mode of transportation is temporarily rendered unusable. For example, how might a company's delivery process be impacted by record snowfall in distribution center areas.

- **Returning:** The supply chain management process concludes with support for the product and customer returns. It's bad enough that a customer needs to return a product, and it's even worse if its due to an error on the company's part. This return process is often called reverse logistics, and the company must ensure it has the capabilities to receive returned products and correctly and promptly assign refunds for returns received. Whether a company is performing a product recall or a customer is simply not satisfied with the product, the transaction with the customer must be remedied.

  Many consider customer returns as an interaction between the customer and the company. However, a very important part of customer returns is the intercompany communication to identify defective products, expired products, or non-conforming goods. Without addressing the underlying cause of a customer return, the supply chain management process will have failed, and future returns will likely persist.

Customer Relationship Management (CRM)

Customer Relationship Management (CRM) is a technology for managing all your company's relationships and interactions with customers and potential customers. The goal is simple: Improve business relationships. A CRM system helps companies stay connected to customers, streamline processes, and improve profitability.

When people talk about CRM, they usually refer to a CRM system or platform, a tool that helps with contact management, sales management, productivity, and more.

CRM software helps you focus on your organization's relationships with individual people — including customers, service users, colleagues, or suppliers — throughout your lifecycle with them, including finding new customers, winning their business, and providing support and additional services throughout the relationship.

With a CRM solution, the sales and marketing team can track and follow a customer's interaction journey with your business. This can enhance the customer journey and experience by refining each customer touchpoint.

While all those benefits apply on some level to just about any CRM, customer relationship management includes a large category of customer service, marketing, and sales tools. Different CRM products and methodologies vary in terms of features and focus, and they can be divided into three main categories.

- Collaborative CRM systems
- Operational CRM systems
- Analytical CRM systems

1. ***Collaborative CRM systems:*** Collaborative CRMs ensure all teams have access to the same up-to-date customer data, no matter which department or channel they work in. Not only does customer support have all the information that marketing and sales teams collected when working with a prospective customer, but agents in a call center have updated data on customer interactions that happened over email or messaging channels.

   Collaborative CRM treats each interaction as part of a larger, integrated conversation between the brand and the customer. The integration between departments and channels saves customers from the dreaded experience of repeating themselves each time they speak to a new executive of the company. Each employee they interact with can quickly and easily pull up a record of all past interactions with the consumer to address the query and grievance of the customer.

2. ***Operational CRM systems:*** Operational CRMs help streamline a company's processes for customer relationships. They provide tools to better visualize and more efficiently handle the full customer journey—even when it includes a high number of touchpoints. It starts from their first interactions with

your company's website, through the whole lead management process as they move through the sales pipeline, and continues with their behaviors once they've become a customer.

Operational CRM systems typically provide automation features. Marketing automation, sales automation, and service automation offload some of the work that your employees would otherwise have to handle. This opens up the schedule of the employees for more creative and personal aspects of their jobs—the stuff that needs a human touch. And it makes it much easier for growing companies to continue to provide top-notch service to scale.

3. ***Analytical CRM systems:*** Analytical CRMs have the primary focus of helping in the analysis of customer data, in order to gain important insights. Digital tools and platforms now make it easy to collect large quantities of data. But data analysis—the step required to turn that data into something useful for your company—is a difficult feat. In fact, estimates suggest that over half of the data collected by companies never gets used.

ELECTRONIC DATA INTERCHANGE (EDI)[48]

Electronic Data Interchange (EDI) is a computer-to-computer exchange of business documents in a standard electronic format between two or more trading partners. It enables companies to exchange information electronically in a structured format, eliminating the need for manual data entry and reducing the cost and time associated with paper-based transactions.

EDI was first introduced in the 1960s as a way for companies to exchange business documents electronically. Over time, the standardization of EDI formats and protocols has enabled businesses to integrate their internal systems with those of their trading partners, improving efficiency and reducing errors.

EDI transactions can include purchase orders, invoices, shipping notices, and other business documents. The EDI standard defines the format and content of these documents, ensuring that they are easily interpreted by both the sender and the receiver.

EDI has become an important part of many businesses, particularly those in the supply chain and logistics industries. It allows for faster and more accurate processing of transactions, leading to improved customer satisfaction and increased profits.

Imagine writing a letter to your friend while communicating every time. This may be a little hard to imagine since today humans live in an era where they can very easily communicate through the internet. Now, imagine the same case with businesses, where communication and exchange of important documents are constantly required. Following the traditional method of sending letters for all communications, it will take forever for the messages to reach the other party, but also the documents will pile up as there is a lot of information that is needed to be stored and kept. It is a tedious and cumbersome process indeed and this is where EDI plays its role.

Electronic Data Exchange is the direct exchange of data and important business documents through the Internet in a professional manner. Two different companies sitting at extreme corners of the world can very easily interchange information or documents (like sales orders, shipping notices, invoices, etc.) with the help of EDI.

EDI Documents:

The most common documents exchanged via EDI are:

- Invoices
- Purchase Orders

48. Source: What is EDI (Electronic Data Interchange) (2023), geeksforgeeks.

- Financial Information letters
- Transaction Bills
- Shipping requests and notifications
- Acknowledgment and Feedback
- Transcripts
- Claims
- Business Correspondence letters.

EDI Users:

- Central and State Government agencies
- Industry
- Banking
- Retailing
- Manufacturing
- Insurance
- Healthcare
- Automotive
- Electronics
- Grocery
- Transportation.

ELECTRONIC FUNDS TRANSFER (EFT)[49]

Electronic Funds Transfer (EFT) is the process by which a user of one bank can transfer money from their account to another by way of payment. It is also called a direct deposit since it directly deposits money into the receiver's account without the need for any physical interaction involving use of documents and cheques.

Electronic Funds Transfer (EFT): How it works

ETFs work via electronic signals that the sender generates when initiating payments, i.e. sending money to the receiver. Instantly, the networks and the servers or payment terminals receive the signals to initiate and continue with the payment. It involves transactions where receiver and the sender can be parties like employers to their employees, vendors to customers, retailers, etc. The reason why ETFs are so popular is because of easy accessibility and safety of the transaction. They're also very swift, with the money being credited almost instantly or within a window of a few days. ETF is possible by initiating a digital cheque — usually between vendors and retailers during the purchase, direct deposit and phone payments — for utility payments, ATMs and card payments or internet transactions via proper authorization. ETFs are encrypted across 128-bit signals, ensuring security. As such, they are secure and swift, and cost effective for businesses. It requires very little effort to set up, usually requiring a bank account and proper documents to allow transfers at the time of set-up only. During the transfer, there is no necessity of providing documents or physical presence to initiate the transaction.

49. Reproduced from Adithyan (2023) Electronic Fund Transfer, Clear Tax.

Major Features of Electronic Funds Transfer (EFT)

- Usually, a very small fee is charged to process the payment across a window.
- To make an EFT payment, all you need is your bank information and the receiver's bank information.
- You cannot stop an ETF payment after you've initiated it by clicking continue after entering your bank details.

DIGITAL CURRENCY[50]

Digital currency is a form of currency that is available only in digital or electronic form. It is also called digital money, electronic money, electronic currency, or cyber cash.

- Digital currencies are currencies that are only accessible with computers or mobile phones because they only exist in electronic form.
- Typical digital currencies do not require intermediaries and are often the cheapest method for trading currencies.
- All cryptocurrencies are digital currencies, but not all digital currencies are cryptocurrencies.
- Some of the advantages of digital currencies are that they enable seamless transfer of value and can make transaction costs cheaper.
- Some of the disadvantages of digital currencies are that they can volatile to trade and are susceptible to hacks.

Note: Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It's a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

Digital currencies do not have physical attributes and are available only in digital form. Transactions involving digital currencies are made using computers or electronic wallets connected to the internet or designated networks. In contrast, physical currencies, such as banknotes and minted coins, are tangible, meaning they have definite physical attributes and characteristics. Transactions involving such currencies are made possible only when their holders have physical possession of these currencies.

Digital currencies have utility similar to physical currencies. They can be used to purchase goods and pay for services. They can also find restricted use among certain online communities, such as gaming sites, gambling portals, or social networks.

Digital currencies also enable instant transactions that can be seamlessly executed across borders. For instance, it is possible for a person located in the United States to make payments in digital currency to a counterparty residing in Singapore, provided they are both connected to the same network.

Types of Digital Currencies

Digital currency is an overarching term that can be used to describe different types of currencies that exist in the electronic realm. Broadly, there are three different types of currencies:

50. Reproduced from Frankefield Jake (2023) Digital Currency Types, Characteristics, Pros and Cons, Future Uses, Investopedia.

- **Cryptocurrencies:** Cryptocurrencies are digital currencies that use cryptography to secure and verify transactions in a network. Cryptography is also used to manage and control the creation of such currencies. Bitcoin and Ethereum are examples of cryptocurrencies. Depending on the jurisdiction, cryptocurrencies may or may not be regulated. Cryptocurrencies are considered virtual currencies because they are unregulated and exist only in digital form.
- **Virtual Currencies:** Virtual currencies are unregulated digital currencies controlled by developers or a founding organization consisting of various stakeholders involved in the process. Virtual currencies can also be algorithmically controlled by a defined network protocol. An example of a virtual currency is a gaming network token whose economics is defined and controlled by developers.

Digital Currencies	Virtual Currencies	Cryptocurrencies
Regulated or unregulated currency that is available only in digital or electronic form.	An unregulated digital currency that is controlled by its developer(s), its founding organization, or its defined network protocol.	A virtual currency that uses cryptography to secure and verify transactions as well as to manage and control the creation of new currency units.

ADVANTAGES AND DISADVANTAGES

Advantages of Digital Currencies

The advantages of digital currencies are as follows:

- Fast Transfer and Transaction Times
- No Physical Manufacturing Required
- Monetary and Fiscal Policy Implementation
- Cheaper Transaction Costs
- Decentralized
- Privacy
- Accessible Around the World.

Disadvantages of Digital Currencies

The disadvantages of digital currencies are as follows:

- Storage and Infrastructure Issues
- Hacking Potential
- Volatile Value
- Limited Acceptance
- Irreversibility
- Change in legal framework may render these currencies infructuous.

Pros and Cons of Digital Currencies

Pros	Cons
• Faster transaction times. • Do not require physical manufacturing. • Lower transaction costs. • Make it easier to implement monetary and fiscal policy. • Offers greater privacy than other forms of currency.	• Can be difficult to store and use. • Can be hacked. • Can have volatile prices that result in lost value. • May not allow for irrevocability of transactions. • Still has limited acceptability.

BLOCK CHAIN TECHNOLOGY

Blockchain is a distributed database or ledger shared amongst a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—the term used to describe the inability to be altered.

Because there is no way to change a block, the only trust needed is at the point where a user or program enters data. This aspect reduces the need for trusted third parties, which are usually auditors or other humans that add costs and make mistakes.

Since Bitcoin's introduction in 2009, blockchain uses have exploded via the creation of various cryptocurrencies, Decentralized Finance (DeFi) applications, Non-Fungible Tokens (NFTs), and smart contracts.

Note: Non-Fungible Token (NFT) is a unique digital identifier that is recorded on a blockchain, and is used to certify ownership and authenticity. It cannot be copied, substituted, or subdivided.

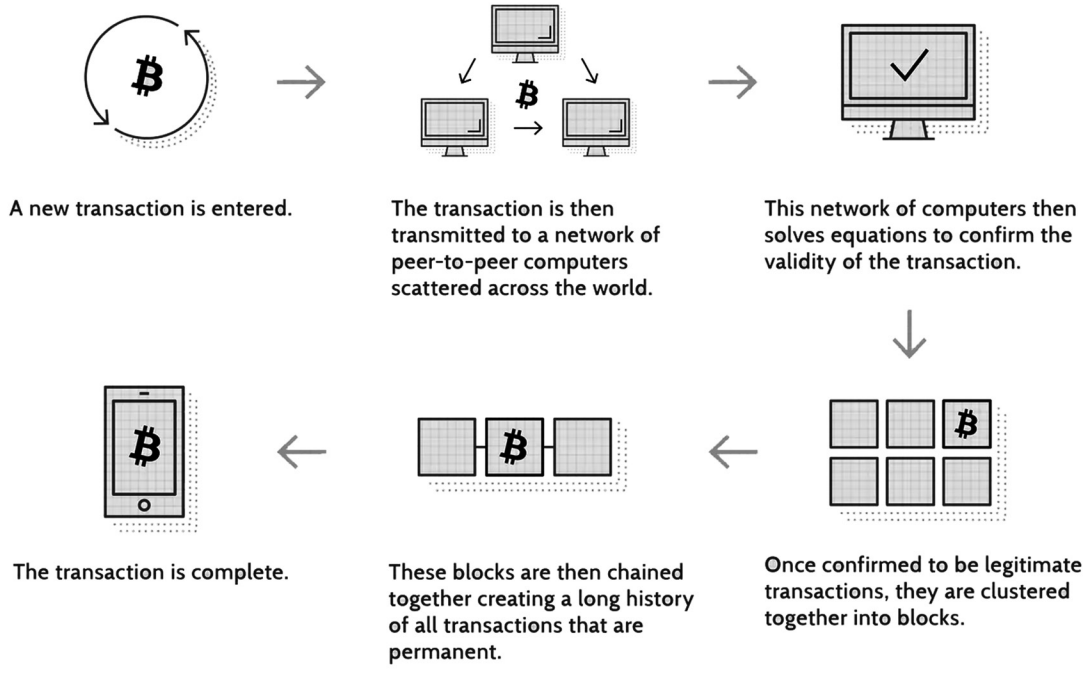
Decentralized Finance (DeFi) is an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries.

- Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.
- Different types of information can be stored on a blockchain, but the most common use for transactions has been as a ledger.
- In Bitcoin's case, blockchain is decentralized so that no single person or group has control—instead, all users collectively retain control.
- Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, transactions are permanently recorded and viewable to anyone.

Transaction Process

Transactions follow a specific process, depending on the blockchain they are taking place on. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events.

In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner or validator picks it up. Once it is entered into a block and the block fills up with transactions, it is closed and encrypted using an encryption algorithm. Then, the mining begins.



Source: Investopedia

The entire network works simultaneously, trying to "solve" the hash. Each one generates a random hash except for the "nonce," short for number used once.

Every miner starts with a nonce of zero, which is appended to their randomly-generated hash. If that number isn't equal to or less than the target hash, a value of one is added to the nonce, and a new block hash is generated. This continues until a miner generates a valid hash, winning the race and receiving the reward.

Once a block is closed, a transaction is complete. However, the block is not considered to be confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals about 60 minutes).

Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process.

PAYMENT PORTAL[51]

A payment gateway is a technology used by merchants to accept debit or credit card purchases from customers. The term includes not only the physical card-reading devices found in brick-and-mortar retail stores but also the payment processing portals found in online stores. However, brick-and-mortar payment gateways in recent years have begun accepting phone-based payments using QR codes or Near Field Communication (NFC) technology.

51. Reproduced from Fernando Jason (2021) What is a Payment Gateway? Definition, How It Works and Example, Investopedia

- Payment gateways are the consumer-facing interfaces used to collect payment information.
- In physical stores, payment gateways consist of the point of sale (POS) terminals used to accept credit card information by card or by smartphone.
- In online stores, payment gateways are the "checkout" portals used to enter credit card information or credentials for services such as PayPal.
- Payment gateways are distinct from payment processors, which use customer information to collect payments on behalf of the merchant.
- There are also payment gateways to facilitate payment in cryptocurrencies, such as Bitcoin.

Examples of Payment Gateways

Merchants can gain access to payment gateway systems through merchant acquiring bank partnerships, or else they can select their own payment gateway system. Large banks such as Bank of America (BAC) and JPMorgan Chase (JPM) have sophisticated payment gateway systems that they offer to customers along with their own merchant acquiring bank services. Ultimately, merchants can choose a variety of payment gateway technologies as long as they are compatible with the merchant acquiring bank that is being used for payment processing.

One recent example of a payment gateway is Square (SQ), which emphasizes flexible mobile payments for retail businesses. The company's Square Reader technology allows customers to easily accept payments at ad-hoc locations such as conventions or farmer's markets, or through roaming storefronts such as food trucks.

With the Square Reader payment gateway technology, a merchant can attach a small piece of hardware to their mobile phone which allows the customer to swipe their payment card for processing through the mobile phone's electronic connection. The Square Reader sends the payment information to a merchant's acquiring bank which then processes the information for the merchant momentarily.

It is likely that new products will continue to increase the versatility and speed of payment gateways. In recent years, blockchain startups have even introduced payment gateways for cryptocurrencies.

E-COMMERCE SECURITY – MOBILE COMMERCE (M-commerce)

M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as smartphones and tablets. M-commerce is a form of e-commerce that enables users to access online shopping platforms without the use of a desktop computer.

Over time, content delivery through wireless devices has become faster, more secure and scalable. As a result, mobile commerce has grown rapidly.

M-commerce encompasses three major approaches to mobility and business.

- Examples of M-commerce include in-app purchasing; mobile banking virtual marketplace apps, such as the Amazon mobile app; and digital wallets, such as Apple Pay, Google Pay and Samsung Wallet.

Examples of M-commerce use in specific industries include the following:

- *Financial services*: Mobile banking and brokerage transactions are done from mobile devices.
- *Telecommunications*: Handheld devices are used to make service changes and bill payments, and to do account reviews.
- *Service and retail*: Consumers place and pay for orders on-the-fly through online stores.
- *Information services*: Financial, sports, traffic, weather and many other news updates are accessed through mobile devices.

Types of M-commerce

M-commerce is categorized based on the following three basic functions:

- **Mobile shopping** enables customers to buy a product using a mobile device with an application such as Amazon or a web app. A subcategory of mobile shopping is app commerce, which is a transaction that takes place over a native app.
- **Mobile banking** is online banking designed for handheld technology. It enables customers to access accounts and brokerage services, conduct financial transactions, pay bills and make stock trades. This is typically done through a secure, dedicated app provided by the banking institution. Mobile banking services may use SMS or chatbots and other conversational app platforms to send out alerts and track account activities. For example, the WhatsApp chatbot lets customers view their account balance, transfer funds, review loans and conduct other transactions in real time through WhatsApp.
- **Mobile payments** are an alternative to traditional payment methods, such as cash, check, credit and debit cards. They enable users to buy products in person using a mobile device. Digital wallets, such as Apple Pay, let customers buy products without swiping a card or paying with cash. Mobile payment apps, such as PayPal, Venmo and Xoom serve the same purpose and are popular options. Mobile consumers also use QR codes to pay for things on their mobile phones. With mobile payments, users send money directly to the recipient's cell phone number or bank account.

Working of Mobile Commerce

With most M-commerce enabled platforms, the mobile device is connected to a wireless network that is used to conduct online product purchases and other transactions.

For those in charge of developing an M-commerce application, important key performance indicators to monitor include the following:

- total mobile traffic;
- total application traffic;
- average order value; and
- the value of orders over time.

Similarly, tracking the mobile add-to-cart rate will help developers see if users are becoming customers. M-commerce developers may also be interested in logging average page loading times, mobile cart conversion rates and SMS subscriptions.

Mobile payment products operate through a form of peer-to-peer sharing. Once a mobile device is paired with a user's bank card information, the phone can be waved over a payment terminal to pay for a product. Contactless payment using a mobile device uses near-field communication technology.

M-commerce vs. E-commerce

Electronic commerce, or e-commerce refers to buying and selling goods and services over the internet. E-commerce and M-commerce are similar, but they come with a few distinctions from each other, such as the following:

- **Mobility:** E-commerce transactions can be conducted through a desktop computer where the user is in a fixed spot. This reduces mobility as it can be difficult to move around a desktop device. M-commerce offers greater mobility as it's conducted through handheld devices that can be used anywhere provided that there is an internet connection, including buses, trains and airplanes or even when exercising at the gym.

- **Location tracking:** Many e-commerce apps make use of location tracking capabilities to pitch users' opportunities based on their location. However, the location tracking capability of e-commerce is limited when it is used with a non-mobile device. For example, the location of an e-commerce shopper is tracked with their IP address. While the IP address provides a broad region of the user's location, it is not capable of identifying the exact location, which might affect the targeted advertising strategies of a business. M-commerce apps, on the other hand, can track locations using Wi-Fi and GPS-based technologies that enable location-specific content and personalized recommendations. For instance, a provider can send push notifications offering personalized discounts that target certain customers as they walk past a specific store in a mall.
- **Security:** Credit cards are still commonly used for non-mobile e-commerce payments. They are considered riskier than other online payment methods, even with security measures, such as multifactor authentication. Most data breaches and identity thefts happen because of credit card misuse. M-commerce closes some security gaps through the addition of measures such as biometric authentication, mobile wallets, quick response or QR codes and even cryptocurrencies.
- **Reachability and convenience:** M-commerce makes it easier to reach a target audience. With mobile apps, businesses can reach more people and make their buying experience easier and faster.

Future of Mobile Commerce

Mobile commerce is evolving and starting to reach a wider audience. According to Insider Intelligence, M-commerce will account for 10.4% of all retail sales by 2025. Many businesses are adopting mobile commerce to avoid falling behind the competitors.

The following are some of the current and future mobile commerce trends:

Mobile Retargeting: This concept is an extension of location-based mobile marketing. Instead of putting ads at random places, this trend targets them contextually only at potential customers. For example, marketers can send an ad to users who have previously visited their mobile app or they might present an active mobile targeted ad to a user who comes into proximity of their store. Mobile retargeting offers a better return on investment compared with other advertisement strategies and is likely to become more popular in the future.

- **Augmented Reality (AR):** The number of mobile applications with embedded AR is growing rapidly. To improve its brand presence and provide digital content optimization, retail giant Ikea introduced an AR mobile application in 2017 that allows shoppers to test products in real time through Apple iOS 11's ARKit technology. Customers use AR models of IKEA furniture from the mobile app to see how those pieces fit in their home and office spaces. Many brands, including Coca-Cola, Zara, Covergirl and Pez, also use embedded AR in their mobile apps.
- **Mobile SEO.** With the growing number of smartphone users accessing the internet, mobile responsive websites have become a necessity. Websites that are not mobile-friendly or do not provide a good user experience risk user abandonment, which in turn increases the bounce rate of their websites. Websites with higher bounce rates rank lower in SEO and Google searches. Therefore, building mobile websites that are adaptive to handheld devices is an important goal for all businesses.
- **Mobile banking:** The biggest advantage of mobile banking is the ability to send money anywhere, anytime. Users can send money to others and conduct transactions with their bank irrespective of their location. This trend is likely to keep growing. According to Business Insider, as of 2021, there are an estimated 169.3 million mobile banking users in the United States, of whom nearly 80% said that mobile banking was their preferred way to access their accounts.

- **AI, chatbots and shopping assistants:** Powered by AI, chatbots are becoming essential e-commerce tools. They help shoppers around the clock with product recommendations, purchase completion, customer support and other tasks. According to a Grand View Research report, the global AI chatbot market is expected to reach $3.99 billion by 2030. Shoppers are becoming more comfortable with chatbots as they have become accustomed to chatting with their friends and family over chat apps, such as WhatsApp, Facebook Messenger and Telegram.
- **Mobile ticketing**: Gone are the days when users had to wait in long lines to buy movie or concert tickets. With mobile ticketing, users can buy and receive tickets through their smartphones. Mobile ticketing also eliminates the need to print the tickets as users receive them on their phones in a text format with a barcode that gets scanned at events.

BLUETOOTH AND WI-FI[52]

Both Bluetooth and Wi-Fi are used for providing wireless communication through radio signals. The difference between Bluetooth and WiFi is that, Bluetooth is actually accustomed to connect short-range devices for sharing information whereas WiFi is used for providing high-speed web access or internet. WiFi provides high information measure because the speed of web is a vital issue.

Bluetooth, developed in the late 1990s, is a technology designed to enable short-range wireless communication between electronic devices, such as between a laptop and a smartphone or between a computer and a television. Bluetooth works by using radio frequencies, rather than the infrared spectrum used by traditional remote controls. As a result, Bluetooth eliminates the need not only for a wire connection but also for maintaining a clear line of sight to communicate between devices.

Wi-Fi is similar to Bluetooth in that it also uses radio waves for high-speed data transfer over short distances without the need for a wire connection. Wi-Fi works by breaking a signal into pieces and transmitting those fragments over multiple radio frequencies. This technique enables the signal to be transmitted at a lower power per frequency and also allows multiple devices to use the same Wi-Fi transmitter. Initially developed in the 1990s, Wi-Fi has undergone several standardization processes, approved by the Institute of Electrical and Electronics Engineers (IEEE), to allow for greater bandwidth in data transfer.

Although both are wireless forms of communication, Bluetooth and Wi-Fi differ in terms of their purpose, capabilities, and other factors. Bluetooth allows for short-range data transfer between devices. As an example, it is commonly employed in headsets for mobile phones, enabling hands-free phone use, etc. Wi-Fi, on the other hand, allows devices to connect to the Internet. Bluetooth limits the number of devices that can connect at any one time, whereas Wi-Fi is open to more devices and more users. In addition, Bluetooth, because it requires only an adapter on each connecting device, tends to be simpler to use and needs less power than Wi-Fi, although this is achieved at the expense of range and speed of data transfer, in which Wi-Fi typically exceeds Bluetooth's capabilities.

Let's see the difference between Bluetooth and Wi-Fi:

Bluetooth	***Wi-Fi***
Bluetooth has no full form.	Wi-Fi stands for Wireless Fidelity.
It requires Bluetooth adapter on all devices for connectivity.	It requires wireless adapter on all devices and wireless router for connectivity.
Bluetooth consumes low power.	It consumes high power.

52. Difference between Wi-Fi and Bluetooth, Geeksofgreeks. Available at https://www.geeksforgeeks.org/difference-between-bluetooth-and-wi-fi/

The security of bluetooth is less in comparison to Wi-Fi.	It provides better security than bluetooth.
Bluetooth is less flexible means in this limited users are supported.	Wi-Fi supports large number of users.
The radio signal range of bluetooth is ten meters.	In Wi-FI, transmission range is hundred meters.
Bluetooth require low bandwidth.	It requires high bandwidth.
Bluetooth frequency ranges from 2.400 GHz to 2.483 GHz.	WiFi frequency ranges from 2.4GHz to 5 GHz.
Bluetooth demands a bluetooth setting or adapter on all devices to set up connectivity.	WiFi demands a wireless router to set up the connectivity and adapter on the device.
WiFi demands a wireless router to set up the connectivity and adapter on the device.	In WiFi, modulation technique is OFDM (Orthogonal Frequency Division Multiplexing) and QAM (Quadrature Amplitude Modulation).
Bit-rate in bluetooth is 2.1 Mbps.	Bit-rate in WiFi is 600 Mbps.
Applications Consumer Games Industry Sport training	Wifi analyser Wifi inspector
It's under IEEE 802.15.	It's under IEEE 802.11 Standard.

LESSON ROUND-UP

- Internet Protocols are a set of rules that governs the communication and exchange of data over the internet. Both the sender and receiver should follow the same protocols in order to communicate the data.
- IP address is a unique address that identifies a device over the network.
- Electronic commerce, or e-commerce refers to buying and selling goods and services over the internet.
- Business models of e-commerce can be classified into the following four models: (1) Business to Business (B2B) (2) Business to Consumer (B2C) (3) Consumer to Consumer (C2C) (4) Consumer to Business (C2B).
- Supply Chain Management (SCM) is the management of the flow of goods, data, and finances related to a product or service, right from the procurement of raw materials to the delivery of the product at its final destination.
- Customer Relationship Management (CRM) is a technology for managing all your company's relationships and interactions with customers and potential customers.

- Electronic Data Interchange (EDI) is a computer-to-computer exchange of business documents in a standard electronic format between two or more trading partners.
- Electronic Funds Transfer (EFT) is the process by which a user of one bank can transfer money from their account to another by way of payment.
- Digital currency is an overarching term that can be used to describe different types of currencies that exist in the electronic realm.
- Cryptocurrencies are digital currencies that use cryptography to secure and verify transactions in a network.
- Virtual currencies are unregulated digital currencies controlled by developers or a founding organization consisting of various stakeholders involved in the process.
- Blockchain is a distributed database or ledger shared amongst a computer network's nodes.
- A payment gateway is a technology used by merchants to accept debit or credit card purchases from customers.
- M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as smartphones and tablets. M-commerce is a form of e-commerce that enables users to access online shopping platforms without the use of a desktop computer.
- Bluetooth, developed in the late 1990s, is a technology designed to enable short-range wireless communication between electronic devices, such as between a laptop and a smartphone or between a computer and a television.
- Wi-Fi is similar to Bluetooth in that it also uses radio waves for high-speed data transfer over short distances without the need for a wire connection. Wi-Fi works by breaking a signal into pieces and transmitting those fragments over multiple radio frequencies.

TEST YOURSELF

(These are meant for recapitulation only. Answer to these questions are not to be submitted for evaluation.)

1. Enlist and briefly discuss the various internet protocols.
2. Write a brief note on blockchain technology.
3. Discuss the categories of CRM systems.
4. Discuss the pros and cons of digital currencies.
5. What are the benefits and limitations of e-commerce?
6. Discuss the C2C model.
7. Write a short note on:
    a. Payment Gateway
    b. EDI
    c. UDP
    d. TELNET
    e. PPP
    f. EFT

8. Enumerate the differences between M-commerce and e-commerce.
9. Discuss the current and future mobile commerce trends.
10. List out the differences between Bluetooth and Wi-Fi.

LIST OF FURTHER READINGS

- Understanding the Internet: A Clear Guide to Internet Technologies by Keith Sutherland (published by Routledge).
- Web Programming and Internet Technologies, 2nd Edition by Scobey (Released September 2016, Published by Jones & Bartlett Learning).
- Internet Technology and Web Design by Dr. R.K. Jain (Published by Khanna Book Publishing Company)

LIST OF OTHER REFERENCES

- Digital Currency Types, Characteristics, Pros and Cons, Future Uses, Investopedia.
- Electronic Fund Transfer, Clear Tax.
- What is EDI (Electronic Data Interchange) (2023), geeksforgeeks.
- Supply Chain Management (SCM): How it Works and Why It Is Important Fernando Jason (2022).
- Elliot Steve, Electronic Commerce: B2C Strategies and Models, London, John Wiley and Sons Ltd. U.K. (2002).
- Timmers P., Business Models for Electronic Markets, Electronic Markets, Vol. 8, No. 2, 3-8 (1998).
- e-Commerce Models. (May 20th, 2013), http://www.eservglobal.com/uploads/files/index.pdf.
- Ray Sarbapriya, Emerging Trends of E-commerce in India: Some Crucial Issues and Challenges, Computer Engineering and Intelligent Systems, Vol. 2, No. 5 (2011).
- Mahadevan B., Business Models for Internet based E-commerce: An Anatomy, Working paper, Indian Institute of Management, Bangalore.
- Timmers P., Business Models for Electronic Markets, Electronic Markets, Vol. 8, No. 2, 3-8 (1998).
- Johnson Carrie, A Report on The Growth of Multichannel Retailing; A Forrester Document: National Governor's Association and the National Conference of State Legislatures. (June 15, 2012), http://www.gfoa.org/downloads/0407MULTICHANNEL.pdf.
- Internet and Mobile Association of India (IAMAI). (June 15, 2012), http://www.iamai.in/reports1.aspx.
- Forrester Report on India to be fastest Growing Market in Asia-Pacific. (June 15, 2012), http://www.iamwire.com/2012/04/india-to-be-the-fastest-growing-e-commerce-market-in-asia-pacific-market-set-to-grow-to-8-8-billion-by-2016/.
- Asian E-commerce Sites Net $ 6.9 Billion in Past 3 years, But the Exits still Tiny (Stats); TECHINASIS, (Mar. 13th, 2014) http://www.techinasia.com/asia-ecommerce-investments-and-exits-2010-to-2013/
- A Report on Bringing e-commerce benefits to Consumers, by European Commission, The European Parliament, (2011). (June 15, 2012), http://ec.europa.eu/internal_market/ecommerce/docs/communication2012/SEC2011_1640_en.pdf.

WARNING

Regulation 27 of the Company Secretaries Regulations, 1982

In the event of any misconduct by a registered student or a candidate enrolled for any examination conducted by the Institute, the Council or any Committee formed by the Council in this regard, may suo-moto or on receipt of a complaint, if it is satisfied that, the misconduct is proved after such investigation as it may deem necessary and after giving such student or candidate an opportunity of being heard, suspend or debar him from appearing in any one or more examinations, cancel his examination result, or registration as a student, or debar him from re-registration as a student, or take such action as may be deemed fit.

It may be noted that according to regulation 2(ia) of the Company Secretaries Regulations, 1982, 'misconduct' in relation to a registered student or a candidate enrolled for any examination conducted by the Institute means behaviour in disorderly manner in relation to the Institute or in or around an examination centre or premises, or breach of any provision of the Act, rule, regulation, notification, condition, guideline, direction, advisory, circular of the Institute, or adoption of malpractices with regard to postal or oral tuition or resorting to or attempting to resort to unfair means in connection with writing of any examination conducted by the Institute, or tampering with the Institute's record or database, writing or sharing information about the Institute on public forums, social networking or any print or electronic media which is defamatory or any other act which may harm, damage, hamper or challenge the secrecy, decorum or sanctity of examination or training or any policy of the Institute.

PROFESSIONAL PROGRAMME

ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

GROUP 1 • ELECTIVE PAPER 4.4

(This test paper is for practice and self-study only and not to be sent to the Institute)

Time allowed: 3 hours *Maximum Mark: 100*

Answer all Questions

Question 1

Read the following case study and answer the questions that follow:

M/s Tech Info consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of $10,000, all originating from South America. There was an additional $1,000 overdraft fee.

The criminals installed an ATM skimmer device to record card account credentials. Many false debit cards were manufactured and used at ATMs in different cities across South America.

Realizing they had been defrauded, the firm contacted their bank and closed the impacted account immediately. Their attempts to pursue reimbursement from the bank were unsuccessful. The commercial account used at the ATM for local currency had different protections from consumer accounts and the bank was not required to reimburse them for their losses. The bank went on to deduct the $1,000 overdraft fee from the firm owner's personal account. The firm severed ties with that bank. The new bank offered comprehensive fraud protection guarantees. The firm created two business accounts: one for receiving funds and making small transfers and another one for small expense payments. The firm updated travel protocols, banning the use of company-provided debit cards. Employees now prepay expenses electronically, pay cash, or use a major credit card, as necessary.

The entire cash reserve for the small business was wiped out, netting losses of almost $15,000.

In view of the above, answer the following:

(i) Knowing how the firm responded, what would you have done differently?

(ii) What are some steps you think the firm could have taken to prevent this incident?

(iii) Is your business susceptible?

(iv) How are you going to reduce your risk?

(v) Explain efforts made by India to ensure cybersecurity.

(5 Marks each)

Question 2

(a) A small family-owned construction company made extensive use of online banking and Automated Clearing House (ACH) transfers. Employees logged in with both company and user-specific ID and password. Two challenge questions had to be answered for transactions over Rs.10,000. The owner

was notified that an ACH transfer of Rs. 1,00,000 was initiated by an unknown source. They contacted the bank and identified that in just one-week cybercriminals had made six transfers from the company bank accounts, totaling Rs. 5,50,000. Cybercriminals were able to install malware onto the company's computers, using a keylogger to capture the banking credentials.

One of their employees had opened an email from what they thought was a materials supplier but was instead a malicious email laced with malware from an imposter account. How this malware impacted the banking transactions of the company?

(5 Marks)

(b) One group of cyber attackers transferred Rs. 10,00,000 from one of the Indian banks to another foreign bank situated in London. The criminals have hacked into the bank's computer system network through the use of some information they acquired from the keylogger programs.

What do you understand by keylogger? What type of keylogger used in the above scenario.

(5 Marks)

(c) A new start-up SME (Small-Medium Enterprise) based in Singapore with an Egovernment model has recently noticed anomalies in its accounting and product records. It has undertaken an initial check of system log files, and there are several suspicious entries and IP addresses with a large amount of data being sent outside the company firewall. They have also recently received several customer complaints saying that there is often a strange message displayed during order processing, and they are often re-directed to a payment page that does not look legitimate.

What do you understand by cybersecurity forensics and how would you like to have cybersecurity forensics for the given scenario?

(5 Marks)

(d) The accused in the case were working in a BPO, that was handling the business of a multinational bank. The accused, during the course of their work had obtained Personal Identification Numbers (PIN) and other confidential information about the bank's customers. Using these the accused and their accomplices, through different cyber cafes, transferred huge amount of money from the accounts of different customers to fake accounts.

How are you going to reduce your risk of online banking specific in the above scenario?

(5 Marks)

Analytics is the discovery and communication of meaningful patterns in data. Especially, valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operation research to qualify performance. Analytics often favors data visualization to communicate insight. In a nutshell, analytics is the scientific process of transforming data into insight for making better decisions. Data Analytics aims to get actionable insights resulting in smarter decisions and better business outcomes. It is critical to design and built a data warehouse or Business Intelligence (BI) architecture that provides a flexible, multifaceted analytical ecosystem, optimized for efficient ingestion and analysis of large and diverse data sets.

What is Data Analytics and Business Intelligence?

(5 Marks)

Question 3

(a) Mr. Akash is running one small business with his family. Their employees do the online transactions by logged in with both company and user-specific IDs and password. The net banking facility of their

bank won't allow any transaction without giving answers to two challenge questions for transactions over Rs.1,000. They receive few messages of debit form their company accounts which were initiated by an unknown source. They contacted the bank and identified that in just one-week cybercriminals had made ten transfers from the company bank accounts for Rs. 4,50,000. Cybercriminals had installed the malware onto the company's computers, using a keylogger to capture the banking credentials.

One of their employees received an email from an unknown sender about winning a lottery price of $1,00,000 and he opened that email on his office laptop which he used for net banking transactions. That email was malicious email laced with malware from an imposter account. What precautions one should have while reading email received from an unknown sender?

(5 Marks)

(b) ACH (Automated Clearing House) is run by an organisation called Nacha (previously NACHA - National Automated Clearing House Association) and may also be referred to as the ACH network or ACH scheme. Payment processing via the ACH network has existed since the 1970s. ACH moved financial transactions worth more than Rs.72.6 trillion in 2021, an increase of over 17 percent from the previous year.

What do you understand by Automated Clearing House (ACH) transfers?

(5 Marks)

(c) A staff member in advisory practice opened a file attached to an email received one morning. It turned out the attachment contained a 'worm' that infected not only the staff member's computer, but it also spread to all other computers in the practice network. This malware caused all computers in the office to shut down. The adviser needed to use the platform software that day to ensure his clients participated in a Corporate Action that was closing the following day. With the help from their Business Development Manager, the office worked through the issue, so they were able to log into the platform software to complete this critical work from a home laptop that hadn't been infected with the virus.

Define malware and how you would like to save your system through malware in the above scenario?

(5 Marks)

(d) Technological advances have great societal benefits and make it easier for people to access information, and to collaborate with their communities. They also expose users to risks such as cybercrime, identity theft or misuse of personal data. Software companies share a responsibility to design and operate products and services in a manner that both helps protect customers from these harms and promotes respect for fundamental rights. And software companies share, with many other stakeholders, a collective responsibility to help make the Internet more reliable and trustworthy.

How are you going to improve the security aspects in the above scenario?

(5 Marks)

(e) The banking systems need reporting systems and improve the data warehouse architecture to achieve a smooth and consistent workflow. The challenge was to develop and integrate a data warehouse, to implement a liquidity risk management system in cooperation with the European Bank for Reconstruction and Development. The final goal was to get a "golden source" and develop the main analytical and reporting dashboards.

Define data warehouse architecture for the above scenario?

(5 Marks)

Question 4

(a) Imagine a scenario where you are visiting some websites and one of them seems to be a little slow. You might blame their servers to improve their scalability as they might be experiencing a lot of user traffic on their site. Most of the sites already take this issue into account beforehand. Chances are, they might be a victim of what is known as a DDoS attack, Distributed Denial of Service Attack.

Discuss the types of DDoS (Distributed Denial of Service) used in the above scenario.

(5 Marks)

(b) The online threat landscape continues to evolve at an accelerating pace with hackers launching more distributed denial of service attacks than ever before, taking aim at new targets, and creating new botnets. The demand for solutions for a wide range of business needs and the rollout of 5G technologies has accelerated the proliferation of Internet of Things (IoT) around the world, creating a huge pool of unsuspecting and under protected new recruits for botnet armies used to launch attacks on massive scales. DDoS attacks are expected to continue to increase in number and complexity as botnets and inexpensive DDoS-as-a-service platforms proliferate.

Based on the above scenario differentiate the DoS and DDoS attack.

(c) Mr. B want to start a new business of trading of readymade garments. He wants to set up his office in his home. He approached you to get knowledge of hardware and software required to set up his small office at home. Assume you are computer hardware and software specialist and advise him as per his requirements.

(5 Marks)

(d) ABC Hospital is top ranked hospital out of 10 pediatric specialty hospitals, with about 25,000 inpatient admissions each year and 5,28,000 patients' visits scheduled annually through 200 plus specialized clinical programs. One fine day their computer systems were stopped working and the entire network go down. Later on, it came to their knowledge that the hackers entered in to their server and the entire data of patients was stolen.

Now hospital want to know that what remedies for such cyber-attack on their server are available for an organization and under which law?

(5 Marks)

(e) Company X is in retail business that wants to improve its sales. They have collected data on their sales over the past year, including information on the products that were sold, the location of the stores, and the demographics of the customers. The data analytics team at Company X is asked to analyze this data to identify trends and patterns that can inform the company's sales strategy.

Discuss the different approach of Data Analytics?

(5 Marks)