Digital Technology

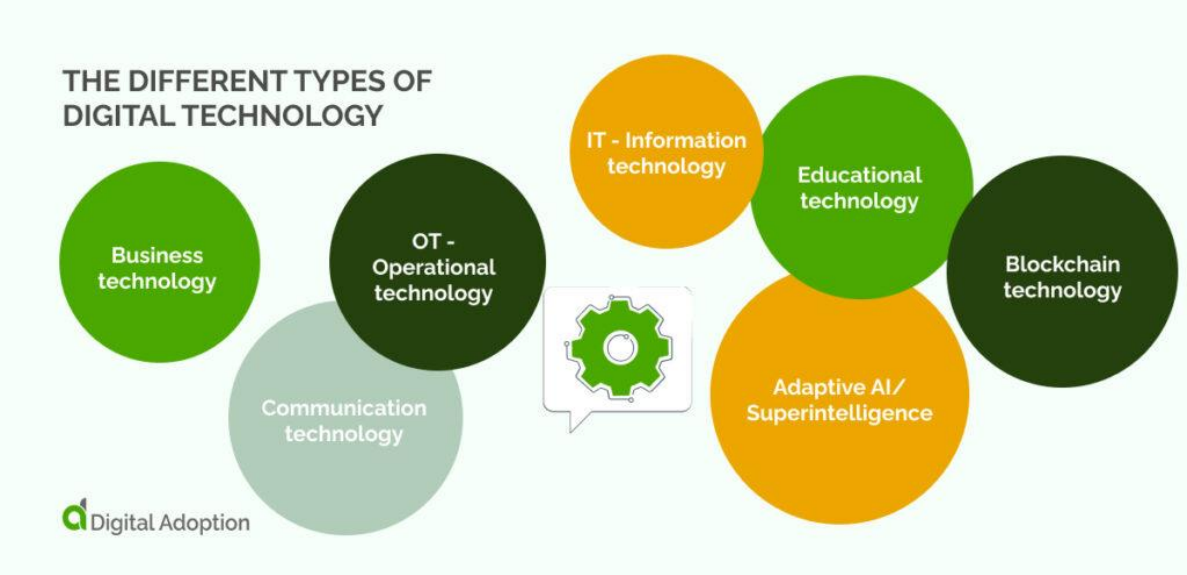
UNIT-I

.What is Digital Technology?

Digital technology means electronic tools, devices, systems, and resources organizations utilize as they process or store data and complete many other functions, increasing **employee productivity and efficiency**. Examples include digital cameras, personal computers, and all devices that utilize increasingly fast data transmission speeds and that store or process data using digital signals.

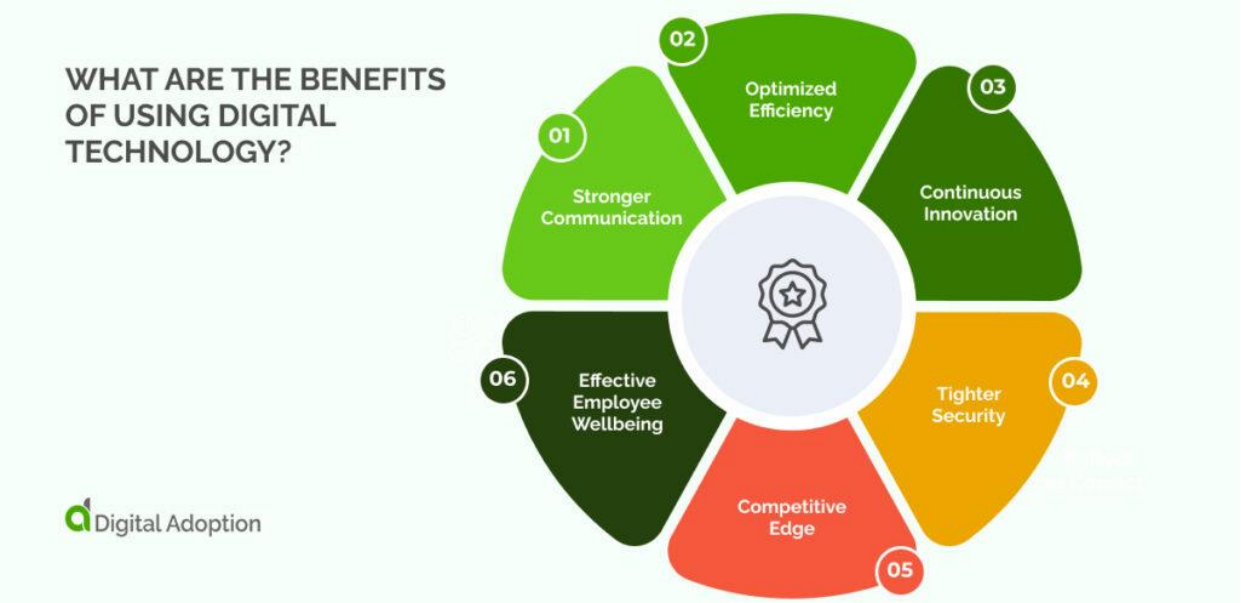
One example of technologies businesses use to utilize tools is cloud platforms, such as **Microsoft 365** or **Google Docs,** that users can utilize on mobile phones. The reason for using digital technology is that it speeds up processes, allowing staff to focus on higher-level functions that technology cannot handle.

The Different Types of Digital Technology



- **Business technology**: Businesses can elevate their operations through cutting-edge technology and science. Business Technology includes information technology, digital marketing, data management, and E-commerce tech.
- **IT – Information technology**: By leveraging IT – Information Technology – comprised of both hardware and software, in addition to telecommunications, businesses can store, send and retrieve data effortlessly.
- **Communication technology**: As an amalgamation of information and communication, Communication Technology (CT) involves digital communication networks for users and devices. Virtual assistants, social media platforms, Wi-Fi networks, and Bluetooth are examples of CT.
- **OT – Operational technology**: Operational Technology is a powerful combination of hardware and software that enables companies to secure their industrial networks.
- **Adaptive AI/ Superintelligence**: Superintelligence uses artificial intelligence and computer systems to expand and upgrade human life. AI-based examples of digital technology include chatbots, virtual agents, and self-driving cars.

- **Educational technology**: EdTech, or educational technology, has revolutionized how students learn by offering breakthroughs such as computer-based instruction, interactive learning tools, audio-visual systems, and online resources.
- **Blockchain technology**: Blockchain offers a secure, web-based financial system with encrypted data. Initially designed to manage digital assets, its applications now extend far beyond that; from online stock exchanges to social media platforms, this tech is quickly becoming an essential tool for businesses.



Stronger Communication

Technological advances can revolutionize how you interact with people worldwide, whether team members, clients, investors, or potential customers. With digital tools like **Skype** and **Zoom** for virtual meetings across great distances and **Slack** or **Asana** for internal communications within your organization, communication has never been simpler or more efficient.

Whether your team is hybrid, office-based, or remote, communication tools will assist you with **tracking projects**, getting the details of tasks right, and **ensuring timely deadlines**. Remember email newsletters, social media accounts, and other resources to keep everyone connected.

Optimized Efficiency

Technology has the potential to enhance systems, products, and services efficiency. From keeping track of processes and **data flow** to managing **contact lists** and **employee records**, technology can streamline operations while effectively decreasing costs and reducing waste – a win-win for any business. With streamlined processes, companies are in a better position for rapid growth.

Technology has undeniably enabled businesses to be more productive and cost-efficient without trading off quality. Manual tasks that staff previously completed manually can now be achieved through software programs, resulting in a significant reduction in labor costs while allowing staff members to focus on the areas where they are most needed.

Continuous Innovation

Innovation thrives in an innovative culture filled with a range of staff with diverse experiences that feel comfortable being creative thinkers to overcome problems. You can facilitate these three conditions by technology in the following ways:

- **Innovative culture**: Offer staff a stipend for technologies that allow them to engage in side projects to encourage innovation and
- **Diverse teams**: Use **AI** to hide personal information about nationality or race to ensure less bias and recruit more diverse talent pools.
- **Creative thinking**: Employ **automation** technologies to complete repetitive tasks, allowing staff to focus on more stimulating, creative activities.

Tighter Security

With cybercrime and data breaches on the rise, strong security is an absolute requirement for any organization. Most businesses store their assets either in the cloud or endpoints, so having stringent measures to protect their information and that of their customers has become essential.

Competitive Edge

Businesses must ensure profits steadily increase, and decreases in revenue means the competition will be taking those profits. Technology has become the edge that every company uses to get one step ahead of their peers, so utilize tech to ensure the sustainability of your business.

Automated metrics can **track your organization's performance**, which you can use to spearhead a new strategy to outcompete your peers. **AI** can also **predict future market trends** to allow you to prepare in advance to optimize your use of emerging tech trends.

Effective Employee Wellbeing

Technology supporting staff well-being is vital to employee retention, productivity, and efficiency and will help employees adapt to digital transformation in the long term. With modern technology, we can access personalized health and wellness solutions. If an employee is under stress, a **meditation app** can help them. Activity trackers will be ideal if they want to increase fitness levels.

The Future Of Digital Technology

Neuromorphic Computing

Neuromorphic computing systems make it easier to develop new products. AI systems can learn about the natural world and react quickly and correctly. Examples of what they can do include recognizing patterns, detecting events, and learning from small amounts of data. We will soon see many products made with this technology.

Human-centered AI

HCAI (Human-Centered Artificial Intelligence) means learning new knowledge, making decisions, or having new experiences. HCAI can also be called “augmented intelligence,” “centaur intelligence,” or “human in the loop.”

Even if a machine works by itself, it still needs people to ensure it operates ethically. HCAI helps vendors stay safe with AI and use devices ethically and responsibly while maintaining the human touch and common sense.

Self-led Learning

Self-supervised models allow AI to deduce connections between different pieces of data, like which scenarios typically occur before or after another and what words usually go together. While self-supervised learning is only recently emerging from academia and a few businesses practice it in the Artificial Intelligence space, some companies specializing in NLP (natural language processing) & computer vision products have included it on their roadmap.

-

Basics of Computer and its Operations

Introduction :
A computer is an electronic device that can receive, store, process, and output data. It is a machine that can perform a variety of tasks and operations, ranging from simple calculations to complex simulations and artificial intelligence.

Computers consist of hardware components such as the central processing unit (CPU), memory, storage devices, input/output devices, and peripherals, as well as software components such as the operating system and applications.

- Accept data
- Store data
- Process data as desired
- Retrieve the stored data as and when required
- Print the result in desired format.

.

Classification of Computers: Computers can be classified based on the technology being used and the way they are designed to perform the various tasks.

1. **Digital Computers :** These are the modern computers which are capable of processing information in discrete form. In digital technology data which can be in the form of letters, symbols or numbers is represented in binary form i.e. 0s and 1s. The digital computers are used in industrial, business and scientific applications. They are quite suitable for large volume data processing.
2. **Analog Computers :** These computers are used to process data generated by ongoing physical processes. A thermometer is an example of an analog computer since it measures the change in mercury level continuously. Analog computers are well suited to simulating systems. A simulator helps to conduct experiments repeatedly in real time environment. Some of the common examples are simulations in aircrafts, nuclear power plants, hydraulic and electronic networks.
3. **Hybrid Computers :** These use both analog and digital technology. It has the speed of analog computer and the accuracy of a digital computer. It may accept digital or analog signals but an extensive conversion

of data from digital to analog and analog to digital has to be done. Hybrid Computers are used as a cost effective means for complex simulations.

4. **Supercomputers:** These are the most powerful and expensive computers that are used for complex scientific calculations, simulations, and research. They are used in fields such as weather forecasting, cryptography, and nuclear research.
5. **Mainframe Computers:** These are large and powerful computers that are used by large organizations such as banks, airlines, and government agencies to process massive amounts of data and handle multiple users simultaneously.
6. **Mini Computers:** These are smaller and less powerful than mainframe computers, but they are still capable of handling multiple users and processing large amounts of data. They are commonly used by small to medium-sized businesses for accounting, inventory management, and other data-intensive tasks.
7. **Personal Computers:** These are small and affordable computers that are designed for individual users. They are commonly used for personal productivity, entertainment, and communication.
8. **Workstations:** These are high-performance computers that are used by professionals such as architects, engineers, and designers to run complex software applications for tasks such as 3D modeling, animation, and scientific visualization.
9. **Embedded Systems:** These are specialized computers that are built into other devices such as cars, appliances, and medical equipment to control their operations and perform specific functions.
10. **Mobile Devices:** These are small and portable computers that are designed for on-the-go use, such as smartphones, tablets, and laptops.

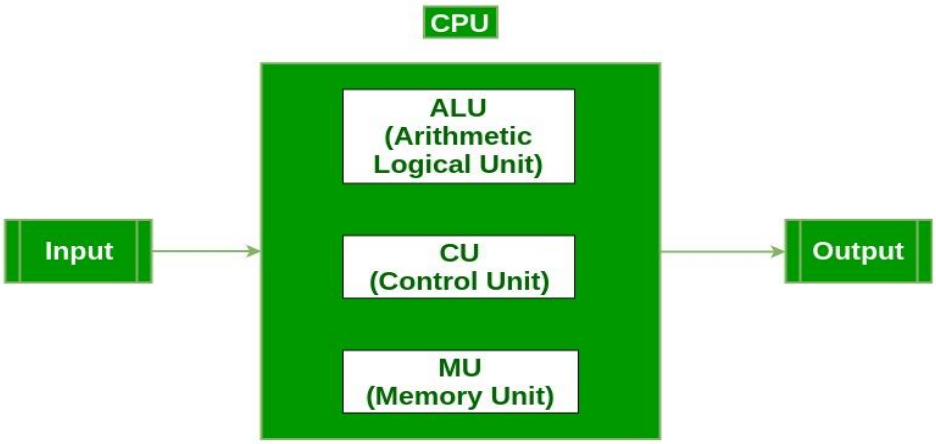
Functional Components of a Computer

- the Input, Process- Output Cycle and these are called as the functional components of a computer. It needs certain input, processes that and produces the desired output.

Computer: A computer is a combination of **hardware and software** resources which integrate together and provides various functionalities to the user. Hardware are the physical components of a computer like the processor, memory devices, monitor, keyboard etc. while software is the set of programs or instructions that are required by the hardware resources to function properly.

Digital Computer: A digital computer can be defined as a programmable machine which reads the binary data passed as instructions, processes this binary data, and displays a calculated digital output. Therefore, Digital computers are those that work on the digital data. . the Input- Process- Output Cycle and these are called as the functional components of a computer.

Details of Functional Components of a Digital Computer

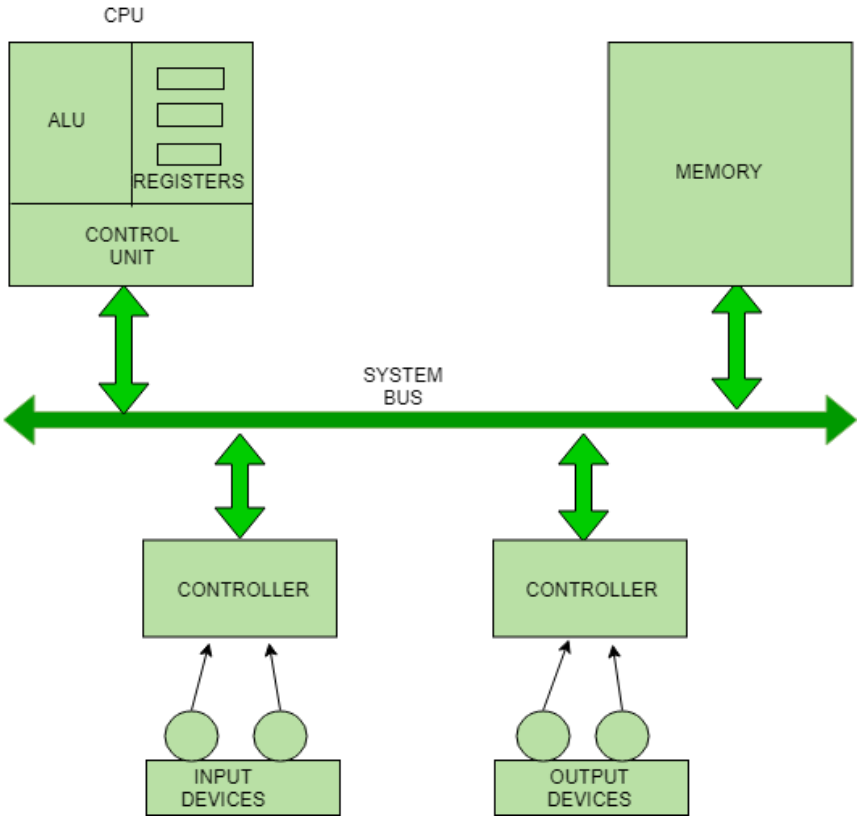


- **Input Unit :**The input unit consists of input devices that are attached to the computer. These devices take input and convert it into binary language that the computer understands. Some of the common input devices are keyboard, mouse, joystick, scanner etc.
- **Central Processing Unit (CPU) :** 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 center 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 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
- **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 comparison of two data items to see which one is larger or smaller or equal.
- **Control Unit :** The Control unit coordinates and controls the data flow in and out of 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.
- **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 :** Memory attached to the CPU is used for storage of data and instructions and is called internal memory The internal memory is divided into many storage locations, each of which can store data or instructions. Each memory location is of the same size and has an address. With the help of the address, the computer can read any memory location easily without having to search the entire memory. when a program is executed, it's data is copied to the internal memory and is stored in the memory till the end of the execution. The internal memory is also called the Primary memory or Main memory. This memory is also called as RAM, i.e. Random Access Memory. The time of access of data is independent of its location in memory, therefore this memory is also called Random Access memory (RAM). Read this for different types of RAMs
- **Output Unit :** The output unit consists of output devices that are attached with the computer. It converts the binary data coming from CPU to human understandable form. The common output devices are monitor, printer, plotter etc.

Interconnection between Functional Components

A computer consists of input unit that takes input, a CPU that processes the input and an output unit that produces output. All these devices communicate with each other through a common bus. A bus is a transmission path, made of a set of conducting wires over which data or information in the form of electric signals, is passed from one component to another in a computer. The bus can be of three types – Address bus, Data bus and Control Bus.

Following figure shows the connection of various functional components:



The address bus carries the address location of the data or instruction. The data bus carries data from one component to another and the control bus carries the control signals. The system bus is the common communication path that carries signals to/from CPU, main memory and input/output devices. The input/output devices communicate with the system bus through the controller circuit which helps in managing various input/output devices attached to the computer.

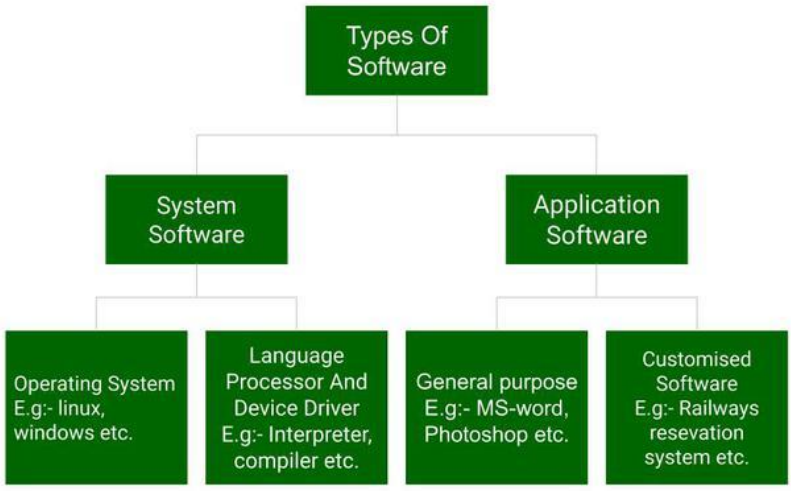
Software and its Types

- In a computer system, the software is basically a set of instructions or commands that tell a computer what to do. In other words, the software is a computer program that provides a set of instructions to execute a user's commands and tell the computer what to do. For example like MS-Word, MS-Excel, PowerPoint, etc.

Types of Software

It is a collection of data that is given to the computer to complete a particular task. The chart below describes the types of software:

1. **System Software :** These are those software,without which our PC,laptop won't run, i.e it is must for a device to be operating. For Example: Linux,Unix,Windows,etc.
2. **Application Software :** These are those software,without which our PC,laptop can run, i.e these software are not necessary for a device to be operating. For Example: Facebook,What's App,Games.



1. **system Software**
   - Operating System
   - Language Processor
   - Device Driver
2. **Application Software**
   - General Purpose Software
   - Customize Software
   - Utility Software

System Software

System software is software that directly operates the computer hardware and provides the basic functionality to the users as well as to the other software to operate smoothly. Or in other words, system software basically controls a computer's internal functioning and also controls hardware devices such as monitors, printers, and storage devices, etc.

Types of System Software

1. **Operating System:** It is the main program of a computer system. When the computer system ON it is the first software that loads into the computer's memory. Basically, it manages all the resources such as computer memory, CPU, printer, hard disk, etc., and provides an interface to the user, which helps the user to interact with the computer system. It also provides various services to other computer software. Examples of operating systems are Linux, Apple macOS, Microsoft Windows, etc.
2. **Language Processor:** As we know that system software converts the human-readable language into a machine language and vice versa. So, the conversion is done by the language processor. It converts programs written in high-level programming languages like Java, C, C++, Python, etc(known as source code), into sets of instructions that are easily readable by machines(known as object code or machine code).
3. **Device Driver:** A device driver is a program or software that controls a device and helps that device to perform its functions. Every device like a printer, mouse, modem, etc. needs a driver to connect with the computer system eternally. So, when you connect a new device with your computer system, first you need to install the driver of that device so that your operating system knows how to control or manage that device.

Features of System Software

- System Software is closer to the computer system.
- System Software is written in a low-level language in general.
- System software is difficult to design and understand.
- System software is fast in speed(working speed).
- System software is less interactive for the users in comparison to application software.

Application Software

Software that performs special functions or provides functions that are much more than the basic operation of the computer is known as application software. Or in other words, application software is designed to perform a specific task for end-users. It is a product or a program that is designed only to fulfill end-users' requirements. It includes word processors, spreadsheets, database management, inventory, payroll programs, etc.

Types of Application Sofware

1. **General Purpose Software:** This type of application software is used for a variety of tasks and it is not limited to performing a specific task only. For example, MS-Word, MS-Excel, PowerPoint, etc.
2. **Customized Software:** This type of application software is used or designed to perform specific tasks or functions or designed for specific organizations. For example, railway reservation system, airline reservation system, invoice management system, etc.
3. **Utility Software:** This type of application software is used to support the computer infrastructure. It is designed to analyze, configure, optimize and maintains the system, and take care of its requirements as well. For example, antivirus, disk fragmenter, memory tester, disk repair, disk cleaners, registry cleaners, disk space analyzer, etc.

Features of Application Software

Let us discuss some of the features of Application Software:

- An important feature of application software is it performs more specialized tasks like word processing, spreadsheets, email, etc.
- Mostly, the size of the software is big, so it requires more storage space.
- Application software is more interactive for the users, so it is easy to use and design.
- The application software is easy to design and understand.
- Application software is written in a high-level language in general.

Difference Between System Software and Application Software

System Software	Application Software
It is designed to manage the resources of the computer system, like memory and process management, etc.	It is designed to fulfill the requirements of the user for performing specific tasks.

System Software	Application Software
Written in a low-level language.	Written in a high-level language.
Less interactive for the users.	More interactive for the users.
System software plays vital role for the effective functioning of a system.	Application software is not so important for the functioning of the system, as it is task specific.
It is independent of the application software to run.	It needs system software to run.

What is an Operating System?

Operating System lies in the category of system software. It basically manages all the resources of the computer. An operating system acts as an interface between the software and different parts of the computer or the computer hardware. The operating system is designed in such a way that it can manage the overall resources and operations of the computer.

Functions of the Operating System

- **Resource Management:** The operating system manages and allocates memory, CPU time, and other hardware resources among the various programs and processes running on the computer.
- **Process Management:** The operating system is responsible for starting, stopping, and managing processes and programs. It also controls the scheduling of processes and allocates resources to them.
- **Memory Management:** The operating system manages the computer's primary memory and provides mechanisms for optimizing memory usage.
- **Security:** The operating system provides a secure environment for the user, applications, and data by implementing security policies and mechanisms such as access controls and encryption.
- **Job Accounting:** It keeps track of time and resources used by various jobs or users.
- **File Management:** The operating system is responsible for organizing and managing the file system, including the creation, deletion, and manipulation of files and directories.
- **Device Management:** The operating system manages input/output devices such as printers, keyboards, mice, and displays. It provides the necessary drivers and interfaces to enable communication between the devices and the computer.
- **Networking:** The operating system provides networking capabilities such as establishing and managing network connections, handling network protocols, and sharing resources such as printers and files over a network.
- **User Interface**: The operating system provides a user interface that enables users to interact with the computer system. This can be a Graphical User Interface (GUI), a Command-Line Interface (CLI), or a combination of both.

- **Backup and Recovery:** The operating system provides mechanisms for backing up data and recovering it in case of system failures, errors, or disasters.
- **Virtualization:** The operating system provides virtualization capabilities that allow multiple operating systems or applications to run on a single physical machine. This can enable efficient use of resources and flexibility in managing workloads.
- **Performance Monitoring:** The operating system provides tools for monitoring and optimizing system performance, including identifying bottlenecks, optimizing resource usage, and analyzing system logs and metrics.
- **Time-Sharing:** The operating system enables multiple users to share a computer system and its resources simultaneously by providing time-sharing mechanisms that allocate resources fairly and efficiently.
- **System Calls:** The operating system provides a set of system calls that enable applications to interact with the operating system and access its resources. System calls provide a standardized interface between applications and the operating system, enabling portability and compatibility across different hardware and software platforms.
- **Error-detecting Aids:** These contain methods that include the production of dumps, traces, error messages, and other debugging and error-detecting methods.

Types of Operating Systems

- What is an Operating System?

An Operating System performs all the basic tasks like managing files, processes, and memory. Thus operating system acts as the manager of all the resources, i.e. **resource manager**. Thus, the operating system becomes an interface between the user and the machine. It is one of the most required software that is present in the device. Operating System is a type of software that works as an interface between the system program and the hardware..

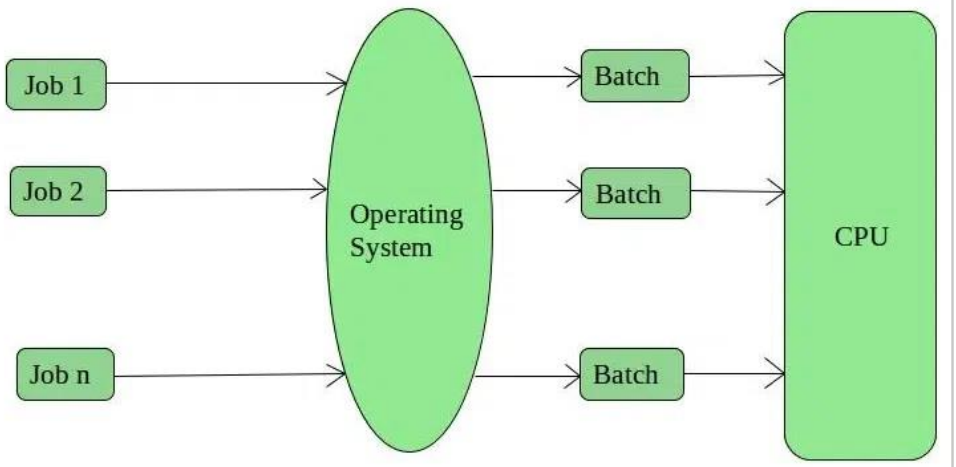
Types of Operating Systems

There are several types of Operating Systems which are mentioned below.×

- Batch Operating System
- Multi-Programming System
- Multi-Processing System
- Multi-Tasking Operating System
- Time-Sharing Operating System
- Distributed Operating System
- Network Operating System
- Real-Time Operating System

1. Batch Operating System

This type of operating system does not interact with the computer directly. There is an operator which takes similar jobs having the same requirement and groups them into batches. It is the responsibility of the operator to



sort jobs with similar needs.

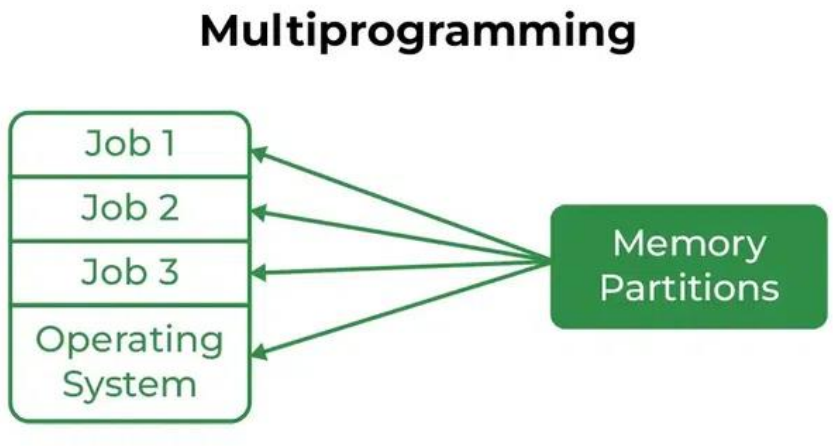
Advantages of Batch Operating System

- It is very difficult to guess or know the time required for any job to complete. Processors of the batch systems know how long the job would be when it is in the queue.
- Multiple users can share the batch systems.
- The idle time for the batch system is very less.
- It is easy to manage large work repeatedly in batch systems.

Examples of Batch Operating Systems: Payroll Systems, Bank Statements, etc.

2. Multi-Programming Operating System

Multiprogramming Operating Systems can be simply illustrated as more than one program is present in the main memory and any one of them can be kept in execution. This is basically used for better execution of resources.



Advantages of Multi-Programming Operating System

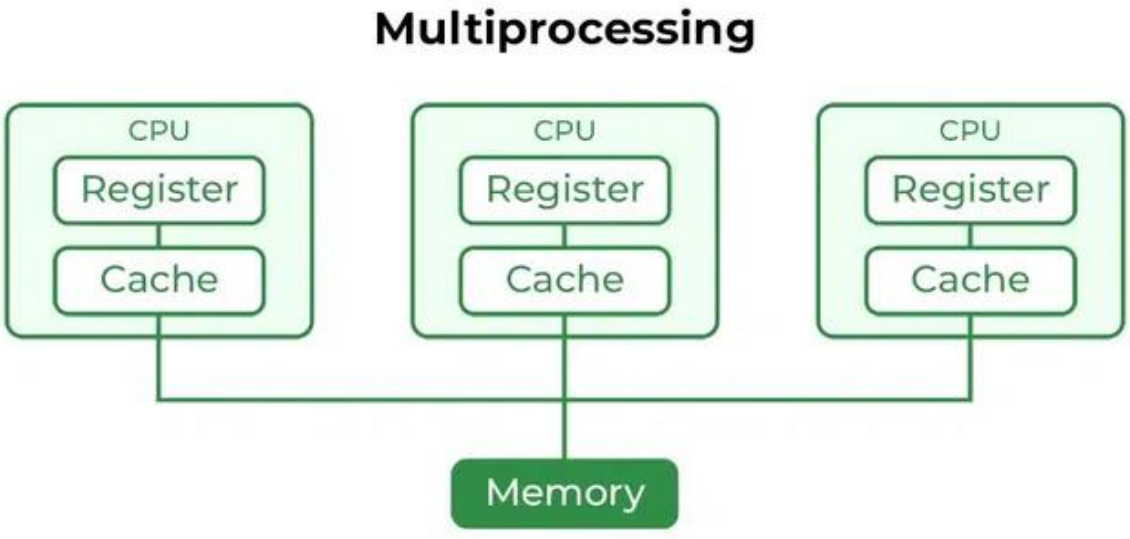
- Multi Programming increases the Throughput of the System.
- It helps in reducing the response time.

3. Multi-Processing Operating System

Multi-Processing Operating System is a type of Operating System in which more than one CPU is used for the execution of resources. It betters the throughput of the System.

Advantages of Multi-Processing Operating System

- It increases the throughput of the system.
- As it has several processors, so, if one processor fails, we can proceed with another processor.

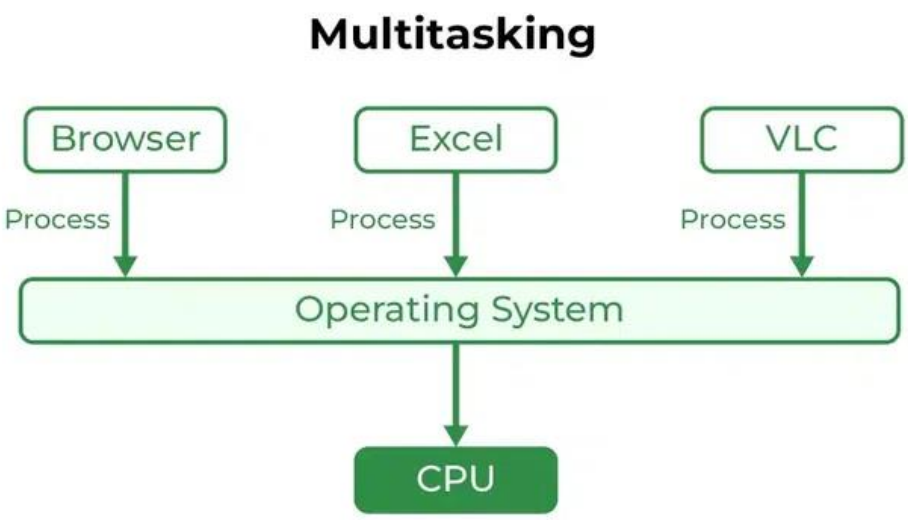


4. Multi-Tasking Operating System

Multitasking Operating System is simply a multiprogramming Operating System with having facility of a Round-Robin Scheduling Algorithm. It can run multiple programs simultaneously.

There are two types of Multi-Tasking Systems which are listed below.

- Preemptive Multi-Tasking
- Cooperative Multi-Tasking

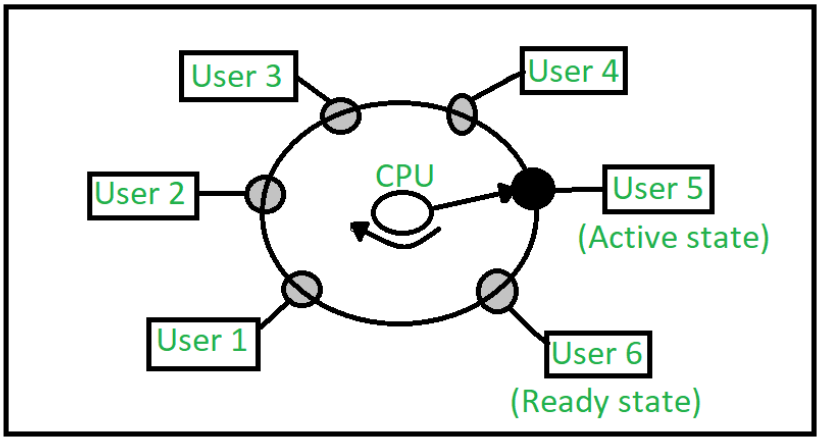


Advantages of Multi-Tasking Operating System

- Multiple Programs can be executed simultaneously in Multi-Tasking Operating System.
- It comes with proper memory management.

5. Time-Sharing Operating Systems

Each task is given some time to execute so that all the tasks work smoothly. Each user gets the time of the CPU as they use a single system. These systems are also known as Multitasking Systems. The task can be from a single user or different users also. The time that each task gets to execute is called quantum. After this time interval is over OS switches over to the next task.



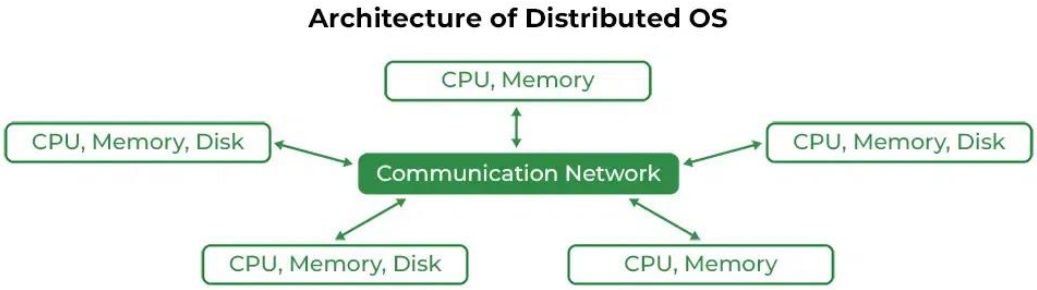
Time-Sharing OS

Advantages of Time-Sharing OS

- Each task gets an equal opportunity.
- Fewer chances of duplication of software.
- CPU idle time can be reduced.
- Resource Sharing: Time-sharing systems allow multiple users to share hardware resources such as the CPU, memory, and peripherals, reducing the cost of hardware and increasing efficiency.
- Improved Productivity: Time-sharing allows users to work concurrently, thereby reducing the waiting time for their turn to use the computer. This increased productivity translates to more work getting done in less time.

6. Distributed Operating System

These types of operating system is a recent advancement in the world of computer technology and are being widely accepted all over the world and, that too, at a great pace. Various autonomous interconnected computers communicate with each other using a shared communication network. Independent systems possess their own memory unit and CPU. These are referred to as loosely coupled systems or distributed systems. These systems' processors differ in size and function. The major benefit of working with these types of the operating system is that it is always possible that one user can access the files or software which are not actually present on his system but some other system connected within this network i.e., remote access network.



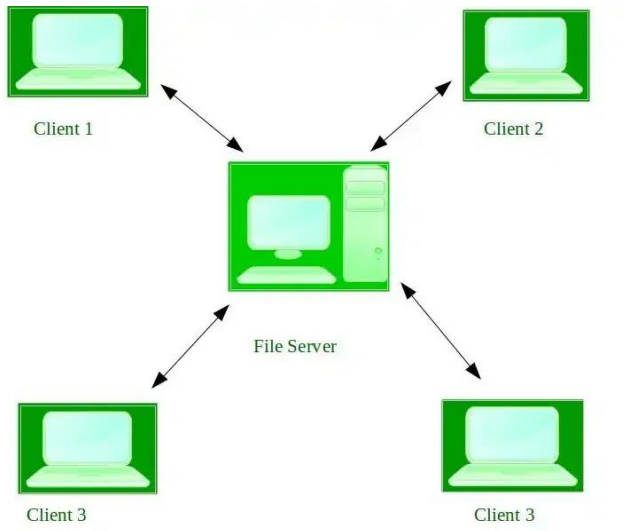
Advantages of Distributed Operating System

- Failure of one will not affect the other network communication, as all systems are independent of each other.
- Electronic mail increases the data exchange speed.
- Since resources are being shared, computation is highly fast and durable.
- Load on host computer reduces.
- These systems are easily scalable as many systems can be easily added to the network.
- Delay in data processing reduces.

Examples of Distributed Operating Systems are LOCUS, etc.

7. Network Operating System

These systems run on a server and provide the capability to manage data, users, groups, security, applications, and other networking functions. These types of operating systems allow shared access to files, printers, security, applications, and other networking functions over a small private network. One more important aspect of Network Operating Systems is that all the users are well aware of the underlying configuration, of all other users within the network, their individual connections, etc. and that's why these computers are popularly known as tightly coupled systems.



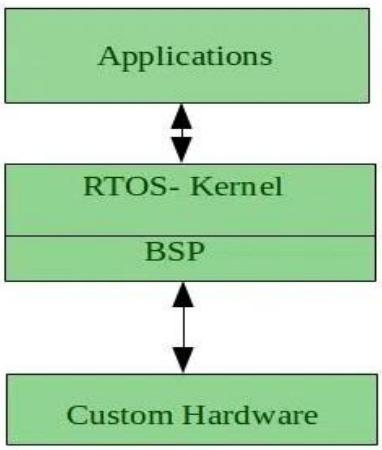
Advantages of Network Operating System

- Highly stable centralized servers.
- Security concerns are handled through servers.
- New technologies and hardware up-gradation are easily integrated into the system.
- Server access is possible remotely from different locations and types of systems.

Examples of Network Operating Systems are Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX, Linux, Mac OS X, Novell NetWare, BSD, etc.

8. Real-Time Operating System

These types of OSs serve real-time systems. The time interval required to process and respond to inputs is very small. This time interval is called **response time**.
Real-time systems are used when there are time requirements that are very strict like missile systems, air traffic control systems, robots,



Advantages of RTOS

- **Maximum Consumption:** Maximum utilization of devices and systems, thus more output from all the resources.

- **Task Shifting:** The time assigned for shifting tasks in these systems is very less. For example, in older systems, it takes about 10 microseconds in shifting from one task to another, and in the latest systems, it takes 3 microseconds.
- **Focus on Application:** Focus on running applications and less importance on applications that are in the queue.
- Real-time **operating system in** the **embedded system:** Since the size of programs is small, RTOS can also be used in embedded systems like in transport and others.
- **Error Free:** These types of systems are error-free.
- **Memory Allocation:** Memory allocation is best managed in these types of systems.

.

Examples of Real-Time Operating Systems are Scientific experiments, medical imaging systems, industrial control systems, weapon systems, robots, air traffic control systems, etc.

-

What is an Algorithm?

Algorithm refers to a set of rules/instructions that step-by-step define how a work is to be executed in order to get the expected results.

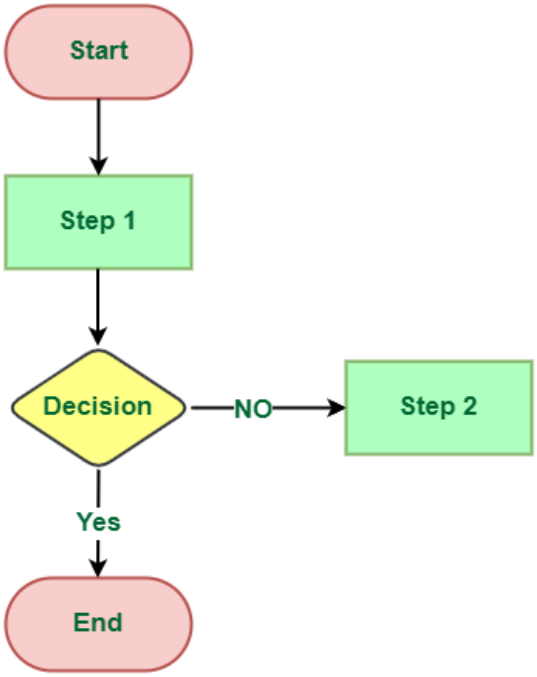
Algorithm of linear search:

- *Start from the leftmost element of arr[] and one by one compare x with each element of arr[].*
- *If x matches with an element, return the index.*
- *If x doesn't match with any of elements, return -1.*

What is a Flowchart**?**

A flowchart is a graphical representation of an algorithm. Programmers often use it as a program-planning tool to solve a problem. It makes use of symbols that are connected among them to indicate the flow of information

and processing. The process of drawing a flowchart for an algorithm is known as "flowcharting".s



Algorithm is a step – by – step procedure which is helpful in solving a problem. If, it is written in English like sentences then, it is called as 'PSEUDO CODE'.

An algorithm must possess the following five properties −

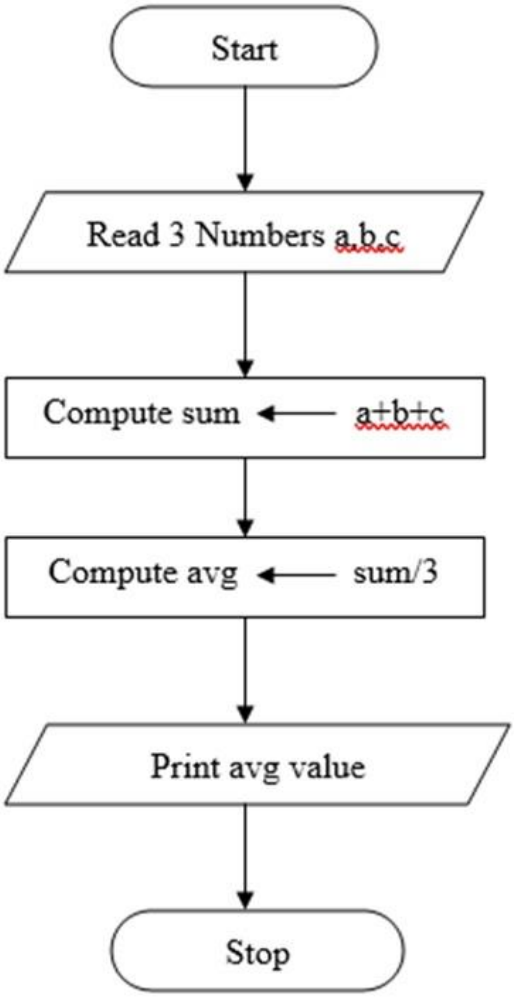
- Input
- Output
- Finiteness
- Definiteness
- Effectiveness

Example **Algorithm for finding the average of three numbers is as follows −**

- Start
- Read 3 numbers a,b,c
- Compute sum = a+b+c
- Compute average = sum/3
- Print average value
- Stop

FLOW CHART **Diagrammatic representation of an algorithm is called flow chart**

Flowchart for finding average of 3 numbers


Start
Read 3 Numbers a,b,c
Compute sum ← a+b+c
Compute avg ← sum/3
Print avg value
Stop

UNIT II

COMPUTER NETOWRK CONCEPTS & APPLICATIONS

Definition:

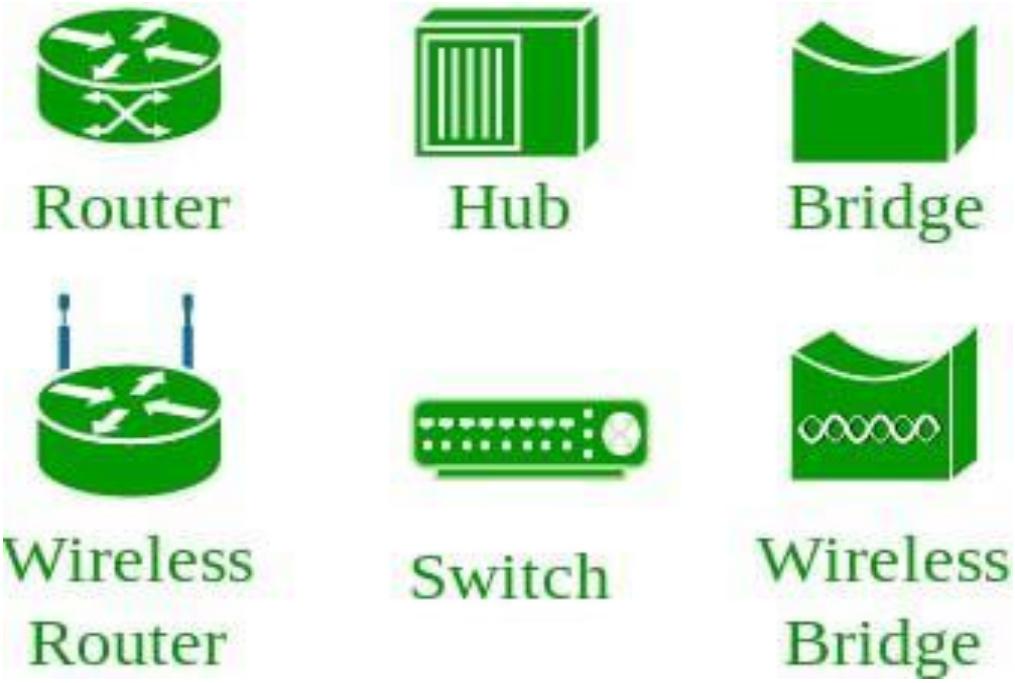
Computer Networking is the practice of connecting computers together to enable communication and data exchange between them. In general, Computer Network is a collection of two or more computers. It helps user to communicate more easily.

Basic Terminologies of Computer Networks

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

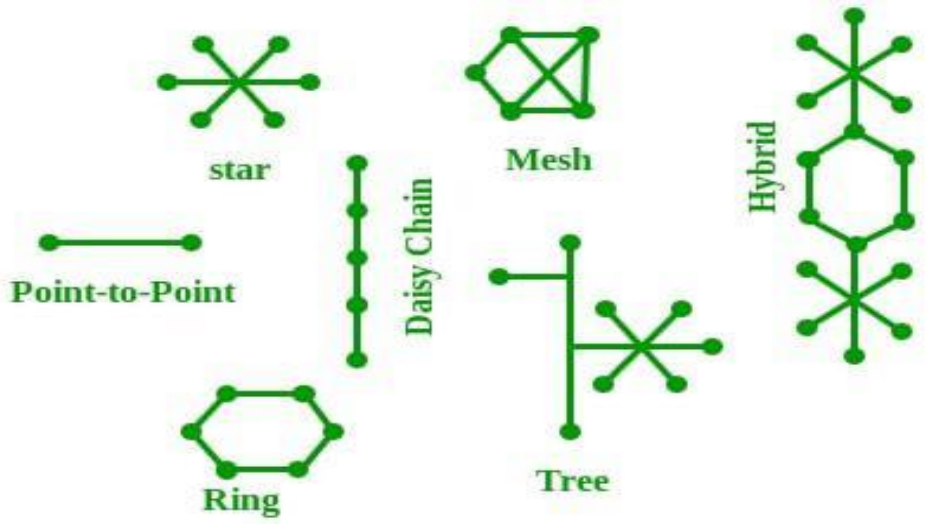
Network Devices

Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



Network Topology:

The Network Topology is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



Types of Computer Network Architecture:

- **Client-Server Architecture:** Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behavior.
- **Peer-to-Peer Architecture:** In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

Classification of Computer Networks:

- **LAN:** A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.
- **WAN:** A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.
- **Cloud Networks:** Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

Applications of Computer Network:

- **Business applications:** Computer networks are widely used in businesses to improve communication, share resources, and enable remote access.
- **Educational applications:** Computer networks are used extensively in educational institutions to facilitate distance learning, provide access to educational resources, and enable collaboration among students and teachers.
- **Healthcare applications:** Computer networks are used in healthcare to store and share patient information, enabling healthcare professionals to provide more personalized care.
- **Entertainment applications:** Computer networks are used for entertainment purposes such as online gaming, streaming movies and music, and social media.
- **Military applications:** Computer networks are used in military applications to provide secure communication and information sharing among military personnel.
- **Scientific applications:** Computer networks are used in scientific research to facilitate collaboration among researchers and share data and information.
- **Transportation applications:** Computer networks are used in transportation to manage traffic, track vehicles, and improve transportation efficiency.
- **Banking and finance applications:** Computer networks are used in banking and finance to process transactions, share information, and provide secure access to financial services.

INTERNET CONCEPTS & APPLICATIONS

Internet overview

The Internet is a giant network of networks.

• A network may include PCs, and other devices like servers or printers.

• A network is connected through a communication channel.

• Early research was performed by the US Department of Defense in 1962. This research group established ARPAnet (Advanced Research Project Agency) in order to connect the US Defense Department network.

What did the Internet come from?

• Original aim was to create a network that would allow users of a research computer at one university to be able to 'talk to' research computers at other universities.

• A side benefit of ARPAnet's design was that, because messages could be routed or rerouted in more than one direction, the network could continue to function even if parts of it were destroyed in the event of a military attack or other disaster.

• The users of the Internet took a direction of their own.

History of the Internet

• The first long distance communication took place in 1965 between a computer in MIT and California.

• In 1969, four computers clients were connected together via ARPAnet.

How old is the Internet ?

• Leonard Kleinrock is accredited with the idea of packet switching, which describes how data can be sent across a network. The Ethernet was developed by Xerox during this period. This was inspired by Robert Metcalfe's PhD on 'packet networks'.

• An Ethernet is a protocol for describing how computers can be connected in a LAN (Local Area network). Through the use of Ethernet and ARPAnet the US were able to develop a working network.

• In the late 1970s and early 1980s other networks were developed, e.g. CSNET, USNET and BITNET. In 1973 Vint Cerf and Bob Kahn created the TCP/IP communication protocols.

• TCP/IP: Transfer Control Protocol/Internet Protocol is a set of rules that describe how computers can communicate over a network.

• To send information over the Internet, a computer packs data into Internet Protocol (IP) packets and labels them with the correct address. They are then sent across a packet switched interconnected network.

Application of Internet

- Communication
- Job Searches
- Finding books & Study materials
- Health & Medicine
- Travel
- Entertainment
- Shopping
- Stock market updates
- Research
- Business

WWW

What is WWW?

WWW stands for World Wide Web and is commonly known as the Web. The WWW was started by CERN in 1989. WWW is defined as the collection of different websites around the world, containing different information shared via local servers (or computers).

Web pages are linked together using hyperlinks which are HTML-formatted and, also referred to as hypertext, these are the fundamental units of the Internet and are accessed through Hyper Text Transfer Protocol(HTTP).

Features of WWW

- WWW is open source.
- It is a distributed system spread across various websites.
- It is a Hypertext Information System.
- It is Cross-Platform.
- Uses Web Browsers to provide a single interface for many services.
- Dynamic, Interactive and Evolving.

Components of the Web

There are 3 components of the web:

- **Uniform Resource Locator (URL):** serves as a system for resources on the web.
- **Hyper Text Transfer Protocol (HTTP):** specifies communication of browser and server.
- **Hyper Text Markup Language (HTML):** defines the structure, organization and content of a web page.

WEB BROWSER

- **Web Browser Definition:** A software application used to access information on the World Wide Web is called a Web Browser. When a user requests some information, the web browser fetches the data from a web server and then displays the webpage on the user's screen.

History of Web Browser

- **"World Wide Web"** was the first web browser created by Tim Berners Lee in 1990. This is completely different from the World Wide Web we use today
- In 1993, the **"Mosaic"** web browser was released. It had the feature of adding images and an innovative graphical interface. It was the "the world's first popular browser"
- After this, in 1994, Marc Andreessen (leader of Mosaic Team) started working on a new web browser, which was released and was named **"Netscape Navigator"**
- In 1995, **"Internet Explorer"** was launched by Microsoft. It soon overtook as the most popular web browser
- In 2002, **"Mozilla Firefox"** was introduced which was equally as competent as Internet Explorer
- Apple too launched a web browser in the year 2003 and named it **"Safari"**. This browser is commonly used in Apple devices only and not popular with other devices
- Finally, in the year 2008, Google released "Chrome" and within a time span of 3 years it took over all the other existing browsers and is one of the most commonly used web browsers across the world

Functions of Web Browser

- The main function is to retrieve information from the World Wide Web and making it available for users
- Visiting any website can be done using a web browser. When a URL is entered in a browser, the web server takes us to that website
- To run Java applets and flash content, plug ins are available on the web browser
- It makes Internet surfing easy as once we reach a website we can easily check the hyperlinks and get more and more useful data online

- Browsers user internal cache which gets stored and the user can open the same webpage time and again without losing extra data
- Multiple web pages can be opened at the same time on a web browser
- Options like back, forward, reload; stop reload, home, etc. are available on these web browsers, which make using them easy and convenient.

Types of Web Browser

1. World Wide Web
- The first web browser ever
- Launched in 1990
- It was later named "Nexus" to avoid any confusion with the World Wide Web
- Had the very basic features and less interactive in terms of graphical interface
- Did not have the feature of bookmark

2. Mosaic
- It was launched in 1993
- The second web browser which was launched
- Had a better graphical interface. Images, text and graphics could all be integrated
- It was developed at the National Center for Supercomputing Applications
- The team which was responsible for creating Mosaic was lead by Marc Andreessen
- It was named "the world's first popular browser"

3. Netscape Navigator
- It was released in 1994
- In the 1990s, it was the dominant browser in terms of usage share
- More versions of this browser were launched by Netscape
- It had an advanced licensing scheme and allowed free usage for non-commercial purposes

4. Internet Explorer
- It was launched in 1995 by Microsoft
- By 2003, it has attained almost 95% of usage share and had become the most popular browsers of all
- Close to 10 versions of Internet Explorer were released by Microsoft and were updated gradually
- It was included in the Microsoft Windows operating system
- In 2015, it was replaced with "Microsoft Edge", as it became the default browser on Windows 10

5. Firefox
- It was introduced in 2002 and was developed by Mozilla Foundation
- Firefox overtook the usage share from Internet Explorer and became the dominant browser during 2003-04
- Location-aware browsing was made available with Firefox
- This browser was also made available for mobile phones, tablets, etc.

6. Google Chrome
- It was launched in 2008 by Google
- It is a cross-platform web browser
- Multiple features from old browsers were amalgamated to form better and newer features
- To save computers from malware, Google developed the ad-blocking feature to keep the user data safe and secure
- Incognito mode is provided where private searching is available where no cookies or history is saved
- Till date, it has the best user interface

Apart from these, Opera Mini web browser was introduced in 2005 which was specially designed for mobile users. Before the mobile version, the computer version "Opera" was also released in 1995. It supported a decent user interface and was developed by Opera Software.

SEARCH ENGINE:

A software program used to do web searches is known as a search engine. A search engine is a specific type of website where a user can do an information search and have the relevant results displayed on the screen.

Difference Between Web Browser and Search Engine	
Web Browser	**Search Engine**
A web browser is a software application used to retrieve data from webpages or HTML files present in servers.	Search Engine is kind of a website where a user can search for information and the results based on the same are displayed on the screen.
A web browser used Graphical Interface to help users experience an interactive online session on the World Wide Web	A search engine has three main components: • Search index • Crawler • Search algorithm
No database of its own. Only comprises a memory to store cache and cookies	It has its own database
Multiple Web Browsers can be installed on a single device	You do not need to install a search engine in your system
Examples of Web Browser are: • Chrome • Firefox • Mosaic • Internet Explorer • Opera	Examples of Search Engine include: • Google • Yahoo • Bing • Ask

MESSAGING

Online messaging apps are those apps which allow one to send and receive a message instantly. Popular messaging apps include Telegram, WhatsApp, Facebook Messenger, Google Chats, WeChat and Viber. They come with multiple features like location sharing, contact sharing, photo sharing, document sharing, and video and audio calls. These messaging apps can be installed on your smart phone, tablet or laptop for free.

EMAIL

An email is an electronic medium of exchanging and transmitting digital files and messages through the internet- by using various electronic devices like smart phones, tablets, desktops, laptops, etc. A user can operate Email across the Internet. Email Writing - Format and Samples

Emails are modern-age letters. This article explains the format of email writing and also gives you sample emails for students of Class 8 to Class 12 and working professionals.

How to Write an Email?

Email writing is an essential part of professional communication. It is not easy to get people to respond to your emails if they do not feel interested in your message or proposal. This is exactly the reason why you

should learn to write good emails. Be bold. Get to the point right away. The best email communication is the one that is simple and clear.
When you start writing an email,

- Make sure you type in the right email ID. Always check with the receiver for the exact **email address** because even a full stop that is not part of the email address can land your email with the wrong person, or the mail would simply bounce.
- The **Subject** line is the next most important factor you should carefully consider because that is the first thing anyone receiving the email would see. It also determines if the receiver would want to open the mail. 'The from line is what recipients use to determine whether to delete an email. The subject line is what motivates people to actually open the email.' said Loren McDonald. Spend double the time you spend on drafting the body to draft the subject.
- See to it that your **Salutation or Greeting** is appropriate to the receiver/s. The greeting builds a rapport.
- The **Body** of the email states what the email is about. Be clear with what you want your receiver to know. Make sure you have everything you want to convey drafted in simple terms. Do not use colloquial language or long unwinding sentences. Try not to repeat words or use cliched terms. Make your message positive, even if you're turning down an offer. If you have to follow, do it before they remind you to. Keep it short. Use standard font style and size. Do a final spelling/grammar check/proofread.
- Finally, **Sign off** the email on a polite note and proofread it before hitting send. The closing should feel genuine; only then will the receiver want to respond.

SOCIAL MEDIA

Social media has a profound influence especially on young people. Its impact and negative effects are often seen in the news; hence the topic's relevance for the UPSC Mains.

Social Media and Its Impact On Society

Context

1. Social media has been accused of polarizing society due to the inflammatory nature of certain posts.
2. World over concerns has been raised over social media being used for surveillance, election meddling, etc.

Background

1. Social media has become ubiquitous. As per a UN report, 47 % of the global population is online and among them, the percentage of social media users is rising steadily.
2. It does not have a steep learning curve and compared to other traditional websites offers content in the local language.
3. The barriers to entry are quite low and there is a large and well development ecosystem in place for users which is unavailable in traditional TV media. The positives of social media.
4. Social media offers a variety of entertainment that offers an escape from the conventional scripted entertainment industry funded by established studios.
5. It offers people-to-people interaction that breaks barriers and forges a true human connection.
6. It also has been instrumental in pro-democracy fights in many oppressive regimes.
7. Social media also played an important role in bringing out stories of 'Metoo' victims.
8. Social media is also playing a crucial role in disaster relief, blood donation drives, etc.

COMPUTER BASED INFORMATION SYSTEM

Definition:

Computer Based Information System (CBIS) is an information system in which the computer plays a major role. **Computer Based Information System (CBIS)** is an information system in which the computer plays a major role. CBIS include data, information, systems, information systems and computer base.

Components of CBIS (Computer Based Information System):

- People (end users and CBIS specialists)
- Hardware (Physical computer equipment and associated devices, machines, and media)
- Software (programs and procedures)
- Database, and
- Networks (communications media and network support)

Significance of CBIS:

1. Efficiency Improvement: CBIS streamline operations by automating routine tasks, reducing the time and effort required for data processing and management, leading to significant efficiency improvements.

2. Enhanced Decision Making: With accurate and timely data provided by CBIS, managers can make more informed decisions. The availability of comprehensive data analytics and reporting tools supports strategic planning and problem-solving.

3. Cost Reduction: By automating processes and reducing the need for manual intervention, CBIS can significantly lower operational costs. They help in optimizing resource allocation and reducing waste.

4. Data Accuracy and Reliability: CBIS ensure that data collected and processed is accurate and reliable, minimizing errors that can occur in manual processes. This is crucial for financial reporting, inventory management, and other critical business operations.

5. Improved Customer Service: CBIS enable organizations to better understand and meet their customers' needs through advanced data analysis, leading to improved customer satisfaction and loyalty.

6. Enhanced Communication: They facilitate better communication within an organization and with external stakeholders by providing platforms for sharing information quickly and efficiently.

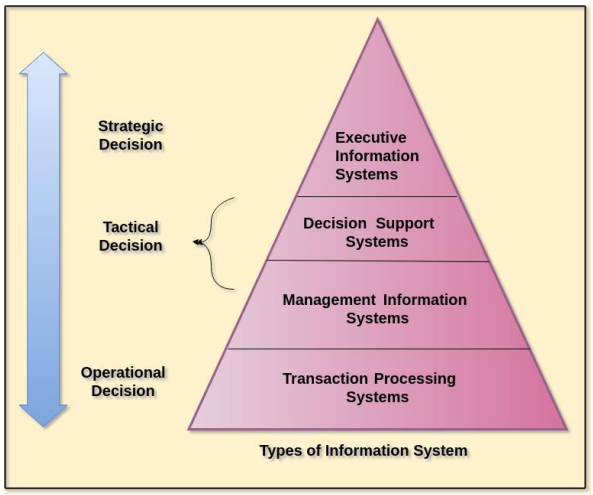
7. Competitive Advantage: Organizations that effectively use CBIS can gain a competitive edge by identifying market trends, optimizing operations, and offering superior customer service.

8. Regulatory Compliance: CBIS help organizations comply with legal and regulatory requirements by ensuring that data is accurately recorded, stored securely, and can be retrieved as needed.

9. Scalability: CBIS are scalable, allowing organizations to adjust their systems as they grow or as their needs change, ensuring that the information system continues to support organizational goals effectively.

10. Innovation Facilitation: By providing tools for data analysis and modeling, CBIS can facilitate innovation within an organization, enabling the development of new products, services, and business models.

Types of Computer Based Information Systems:



1. Transaction Processing System (TPS)

Transaction processing is essential to helping businesses perform daily operations. Transactions are defined as any activity or event that affects the company, and include things like deposits, withdrawals, shipping, billing customers, order entry, and placing orders. TPS supports these business transactions

.

2. Management Information System (MIS)

Middle managers handle much of the administrative chores for day-to-day routines and performance monitoring, ensuring that all the work is aligned with the organization's needs. That's why MIS is such a valuable tool. Management Information Systems are specially designed to help middle managers and supervisors make decisions, plan, and control the workflow. The MIS pulls transactional data from various Transactional Processing Systems, compiles the information, and presents it in reports and displays.

Additionally, these reports can be produced monthly, quarterly, or annually, although MIS can have more immediate reports (e.g., hourly, daily).

3. Decision Support System (DSS)

The DSS is a management-level, interactive computer-based information system that helps managers to make decisions. The Decision Support System specifically gives middle managers the information necessary to make informed, intelligent decisions.

Decision Support Systems use different decision models to analyze or summarize large pieces of data into an easy-to-use form that makes it easier for managers to compare and analyze information. Often, these summaries come in the form of charts and tables.

4. Executive Support System (ESS)

The ESS is like the MIS but for executive-level decision-making. The decisions involve company-wide matters, so the stakes are higher. Consequently, they demand more insight and judgment. The ESS provides greater telecommunication, better computing capabilities, and more efficient display options than the DSS. Executives use ESS to make effective decisions through summarized internal data taken from DSS and MIS and external sources. In addition, executive support systems help monitor performances, track competitors, spot opportunities, and forecast future trends.

E COMMERCE

What is E-Commerce?

E-Commerce is defined as the buying and selling of goods and services including digital products over digital and electronic networks. Electronic commerce (E-commerce) draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

Types of E-Commerce Models

There are mainly four types of E-Commerce Models which are followed in India:

- **Business to Business (B2B) –** The selling of products between the manufacturer, retailers and wholesalers is called the B2B model of e-commerce. Here the customer is not involved in the transfer of products or goods
- **Business to Consumer –** This is the generally used online portals where the e-commerce company sells directly to the consumer
- **Consumer to Consumer (C2C) –** The best example of this is OLX, where consumer can upload their old products and resale them directly to the buyer. There is no interference of the manufacturers or retailers
- **Consumer to Business –** When a person designs or creates something new, they can sell it to the e-commerce company for further sales. This is called the Consumer to Business model

Benefits of E-Commerce:

- Business can be done from anywhere can the products can be sold both within the country as well as Internationally
- One can promote their work and sell their products directly to the consumers without the interference of middlemen
- Goods can be delivered to the doorstep from any part of the country or the world
- Reduced the investment cost since in many cases money can be saved on buying a storeroom for the display of products
- 24×7 facility to order products online. The only requirement is an internet connection
- Through the four different models of electronic commerce in the country, businessmen can choose their target consumers and sell directly to the customers or to other retailers as well.

DIGITAL MARKETING

Marketing plays a major role in creating awareness about a business, increasing customer base, growing sales and building brand. Marketing is one of the most important parts of any business and without effective marketing, growing business becomes almost impossible.

There are two types of marketing

- Traditional Marketing
- Digital marketing

Traditional Marketing

1. Communication is unidirectional in traditional marketing, which means, an organization communicates about its services with its audiences
2. Medium of communication in traditional marketing is generally phone calls, emails,and letters.
3. Campaign in Traditional marketing takes more time as designing, preparing, and launching are involved.
4. It is best for reaching local audience.
5. It is almost impossible to measure the effectiveness of a traditional marketing campaign

Digital Marketing

1. Communication is bidirectional in Digital Marketing as businesses can communicate with customers and customers can ask queries or make suggestions to businesses as well.
2. Medium of communication is more powerful and involves social media websites, chats, apps and Email.
3. Digital marketing campaigns can be developed quite rapidly and with digital tools, channelizing Digital Marketing campaigns is easier.
4. It is very effective for reaching global audiences.
5. Digital Marketing lets you measure the effectiveness of a digital marketing campaign through analytics

What Is Digital Marketing?

- Digital marketing is the use of websites, apps, mobile devices, social media, search engines, and other digital means to promote and sell products and services.
- Digital marketing started to become popular with the widespread adoption of the internet in the 1990s.
-

- Digital marketing promotes products and services through channels such as websites, mobile devices, and social media platforms.
- Digital marketers have a number of tools to measure the effectiveness of their campaigns.
- One of the biggest challenges digital marketers face is how to set themselves apart in a world that is oversaturated with digital ads and other distractions.

Digital Marketing Concepts:

Search Engine Optimization (SEO):

One of the most specialized and sought after tools, SEO focuses on making your business website rank top in the search engines such as Google, Yahoo, etc.

Email Marketing:

It comprises building a subscribers list and sending emails to the target audience.

Content Optimization:

Some digital marketing experts say that content is the silver bullet of digital marketing. Whether it is a website, social media platforms or emails, the quality, consistency, relevance and frequency of updation of content plays a crucial role.

Marketing Analytics:

Marketing analytics play a very important role in evaluating data to design the complete strategy of marketing.

Benefits of digital marketing:

Global reach

A website allows you to find new markets and trade globally for only a small investment.

Lower cost

A properly planned and well-targeted digital marketing campaign can reach the right customers at a much lower cost than traditional marketing methods.

Trackable, measurable results

Measuring your online marketing with web analytics and other online metric tools makes it easier to establish how effective your campaign has been. You can obtain detailed information about how customers use your website or respond to your advertising.

Personalisation

If your customer database is linked to your website, then whenever someone visits the site, you can greet them with targeted offers. The more they buy from you, the more you can refine your customer profile and market effectively to them.

Openness

By getting involved with social media and managing it carefully, you can build customer loyalty and create a reputation for being easy to engage with.

Social currency

Digital marketing lets you create engaging campaigns using content marketing tactics. This content (images, videos, articles) can gain social currency - being passed from user to user and becoming viral.

Improved conversion rates

If you have a website, then your customers are only ever a few clicks away from making a purchase. Unlike other media which require people to get up and make a phone call, or go to a shop, digital marketing can be seamless and immediate.

Unit III

Digital India& E-Governance :

Digital India is a campaign launched by the Government of India to ensure that Government services are made available to citizens electronically by improved online infrastructure and by increasing Internet connectivity or by making the country digitally empowered in the field of technology.

Initiative

Government of India launched National e-Governance Plan (NeGP) in 2006. 31 Mission Mode Projects covering various domains were initiated.viz. agriculture, land records, health, education, passports, police, courts, municipalities, commercial taxes, treasuries etc.

Despite the successful implementation of many e-Governance projects across the country, e-Governance as a whole has not been able to make the desired impact and fulfill all its objectives. It has been felt that a lot more thrust is required to ensure e-Governance in the country to promote inclusive growth that covers electronic services, products, devices and job opportunities.

Considering the shortcomings in National e-Governance Plan that included lack of integration amongst Government applications and databases, low degree of government process reengineering, scope for leveraging emerging technologies like mobile, cloud…etc, Government of India launched Digital India Programme on 1 July 2015 by Prime Minister Narendra Modi.Digital India is an ambitious programme of Government of India.. This programme has been envisaged and coordinated by the Department of Electronics and Information Technology (DeitY) in collaboration with various Central Ministries/Departments and State Governments. The Prime Minister as the Chairman of Monitoring Committee on Digital India, activities under the Digital India initiative is being carefully monitored. All the existing and ongoing e-Governance initiatives have been revamped to align them with the principles of Digital India.

VISION OF DIGITAL INDIA

The vision of Digital India programmeis to transform India into a digitally empowered society and knowledge economy. Governance and Services on Demand. Digital Empowerment of Citizens. Digital India is an initiative to transform the country into a digitally empowered society through infrastructural upgrades, increased digital literacy and the promotion of e-services. The campaign increased internet access, expanded digital infrastructure, enhanced e-government services.It is centred on three key areas:

- **Digital Infrastructure as a Core Utility to Every Citizen**
- **Governance & Services on Demand**
- **Digital Empowerment of Citizens**

Digital Infrastructure

Another significant effect of the programme has been the expansion of India's digital infrastructure. The government has made significant investments such as the BharatNet project, which linked over 1.15 lakh Gramme Panchayats through a 2,74,246-kilometer optical fibre network, improving high speed internet networks, access in rural areas and creating new prospects for digital entrepreneurship.

Pillars of Digital Infrastructure

• High speed internet : Broadband connectivity in all Urban and Rural area

• Unique digital identity : Uses of Aadhaar and biometric database

• Mobile Connectivity :Universal access to phones and mobile network connectivity including in hilly and remote areas.

• Access to a Common Service Centre : Viable, multi functional e-services delivery outlets closer to the doorsteps of citizen

• Private space on Cloud : Meghraj cloud platform to accelerate delivery of e-services.

• Secure cyber-space : Cyber Swachhta Kendra (Botnet cleaning and Malware analysis centre) to create a secure cyber space.

SERVICES *&* *EMPOWERMENT* FOR DIGITAL INDIA INITIATIVE

In line with the government's Digital India initiative and with the popularity of Smartphones, the craze for downloading mobile apps increased, the government leveraged this scenario to promote the Digital India initiative through mobile apps. Various ministry launched a number of mobile apps, web-based platforms and services to gain access to digital content.

Some of the important apps and services project that Govt. of India has taken to become Digital India

1. **MyGov** : MyGov is Government of India's innovative citizen engagement platform for direct citizen participation in governance. It provides an avenue for channelizing the ideas, comments and creative suggestions of the citizens by connecting them to central ministries and associated organizations. Citizens can participate in policy formulation and programme implementation to usher in an era of direct participatory democracy. After creating a login id on this feature-rich app, a citizen can easily access numerous government initiative sites.
2. **BHIM App** : The Government of India's mobile payment app BHIM (Bharat Interface for Money), the app developed by National Payments Corporation of India (NPCI) was launched by Prime Minister Narendra Modi aims to promote digital transactions and tackle the various stumbling blocks, like payment to service providers, in country's way to become a cashless economy. The app is a rebranded version of UPI (Unified Payment Interface) and USSD (Unstructured Supplementary

Service Data). As UPI is built on top of Immediate Payment Service (IMPS), this means transactions that you will do on BHIM app will take only seconds.

3. **Bharat QR Code** : Bharat QR Code is a common QR code built for ease of payments. It is a standard that will support Visa, MasterCard and Rupay cards for wider acceptance. However, Bharat QR code will enable the merchants to accept digital payments without the Point of Sale (PoS) swiping machine. It will allow customers of any bank to use their smartphone app to make payment using their debit card. In terms of benefits, merchants will no longer need to invest in buying the PoS machine. With no PoS machine, merchants will also be able to do away with the transaction fees charged by the banks for using the PoS terminal.
4. **DigiLocker App**: DigiLocker is one of the key initiatives under the Digital India Programme. This was released by the Department of Electronics and Information Technology (DeitY), Government of India as a service to provide a secure dedicated personal electronic space for storing the documents of resident Indian citizens. The storage space is linked to the Unique Identification Authority of India (Aadhaar number) of the user. The space can be utilized for storing personal documents like University certificates, Permanent account number (PAN) cards, voter id cards, etc., and the URIs of the e-documents issued by various issuer departments. There is also an associated facility for e-signing documents. The service is intended to minimize the use of physical documents and to provide authenticity of the e-documents. It will also provide secure access to government issued documents. It is also intended to reduce administrative expenses of government departments and agencies and to make it easy for the residents to receive services.
5. **Swachh Bharat Abhiyaan:** Prime Minister Narendra Modi had launched a new initiative called Swachh Bharat Abhiyaan on 2nd October 2014 to create awareness about cleanliness, and encourage citizens become more active participants in such drives across the country. With this app, citizens can track the progress made by this campaign as well as tag people to take up the challenge for the mission.

6. **mPassportSeva** : This app aims at providing all the Passport-related services to all the Indian citizens in a convenient and transparent manner. This is one of the largest projects under the National e-Governance Plan (NeGP). 'mPassport Seva' app offers a wide array of services such as passport application status tracking, locating the Passport Seva Kendra (PSK) and other information related to a Passport.

7. **Government e-Marketplace (GeM)**: It basically intends to eliminate the human interface in vendor registration by providing an online platform to them. The tenders for the goods and services that the government wishes to procure would be available on this platform and the suppliers can evince their

interest after going through the terms and conditions of the procurement. GeM is one of the many initiatives taken by the GoI to digitise the way in which business transactions happen. It would effectively reduce the time required for vendor registration as all the details would be fed online. GeM would enable easy order placement and payment processing thus increasing the efficiency of the system in place. It would also check the leakage in terms of costs involved in a transaction where human interaction is maximized. This policy can go a long way in ensuring that the government officials are also at place with the ongoing digital revolution so that this can further be integrated into other departments as well. GeM would eventually offer hundreds of products such as laptop computers and photocopiers and services such as cab hiring and housekeeping to government departments which currently buy them through rate contracts or yearly tenders handed out to vendors and service providers after competitive bidding.

Digital Financial Tools

Digital Finance:
Digital finance can be defined as financial services delivered over digital infrastructure-including mobile and internet—with low use of cash and traditional bank branches

The major types of Digital Financial Services are as follows

1. **Unified Payments Interface (UPI)**
2. Aadhaar Enabled Payment System
3. **Credit /Debit Cards**
4. Unstructured Supplementary Service Data (USSD)
5. E-Wallet
6. Internet Banking (NEFT, RTGS/IMPS)

Unified Payments Interface (UPI)

Unified Payments Interface (UPI) is a system that powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood. It also caters to the "Peer to Peer" collect request which can be scheduled and paid as per requirement and convenience.

Unified Payments Interface is a system for instant, electronic payments through user's smart phone. It is an advanced version of Immediate Payment Service (IMPS) which was used to transfer money between bank accounts.
Like IMPS, UPI will facilitate round-the-clock funds transfer service. It authenticates the identity of the user like a debit card does using the phone as a tool instead of a separate card.

Advantages for using UPI

- Round the clock availability
- Single Application for accessing different bank accounts
- Use of Virtual ID is more secure, no credential sharing
- Single click authentication
- Raise Complaint from Mobile App directly

Steps for Registration:

- User downloads the UPI application from the App Store/Banks website
- User creates his/her profile by entering details like name, virtual id (payment address), password etc.
- User goes to "Add/Link/Manage Bank Account" option and links the bank and account number with the virtual id

Generating UPI – PIN:

- User selects the bank account from which he/she wants to initiate the transaction
- User clicks one of the option -

Change UPI PIN

- User receives OTP from the Issuer bank on his/her registered mobile number
- User now enters last 6 digits of Debit card number and expiry date
- User enters OTP and enters his preferred numeric UPI PIN(UPI PIN that he would like to set) and clicks on Submit
- After clicking submit, customer gets notification (successful or decline)
- User enters his old UPI PIN and preferred new UPI PIN (UPI PIN that he would like to set) and clicks on Submit
- After clicking submit, customer gets notification (successful or failure)

Performing a UPI Transaction:

- Send Money
    - User logs in to UPI application
    - After successful login, user selects the option of Send Money/Payment
    - User enters beneficiary's/Payee virtual id, amount and selects account to be debited
    - User gets confirmation screen to review the payment details and clicks on Confirm
    - User now enters UPI PIN
    - User gets successful or failure message

AEPS (Aadhaar Enabled Payment System):

In order to facilitate the financial inclusion objectives of the Government of India leveraging Aadhaar authentication through the Business Correspondent channel, NPCI has developed the Aadhaar enabled Payment System (AePS)

It is a payment service empowering a bank customer to use Aadhaar as his/her identity to access his/her respective Aadhaar enabled bank account and perform basic banking transactions. It allows bank-to-bank transaction at PoS (MicroATM) with the help of Banking Correspondent (BC) The user has to seed his/her

account with their Aadhar number at bank or with the help of BC. User can do as many transactions at any AEPS point without any PIN or password.
Any resident of India having an Aadhaar number linked to a bank account - referred to as an Aadhaar Enabled Bank Account (AEBA) - can utilise the AePS service.

Types of banking transactions with Aadhaar Enable Payment System:

- Balance Enquiry
- Cash Withdrawal
- Cash Deposit
- Aadhaar to Aadhaar Fund Transfer
- Mini Statement
- Purchase

To use AePS, **you** need to:

1. Provide KYC (Know Your Customer) information to open a new account
2. Link your Aadhaar number to your bank account
3. Present your Aadhaar and bio-metrics (finger and/or iris)
4. At the PoS machine, enter your Aadhaar number
5. Select the transaction type and specify the bank's name
6. Enter the transaction amount
7. Provide biometric authentication (fingerprint or iris scan) to confirm the payment
8. Upon successful completion, a receipt will be issued for the transaction

Advantages of AePS

For a customer: It allows the customer to have doorstep banking and do basic banking transactions without the need to visit any bank branch, carry cards or remember PIN/passwords.

USSD [Unstructured Supplementary Service Data]:

- USSD (Unstructured Supplementary Service Data) is a communication technology used by mobile service providers to offer menu-based services to mobile phone users.
- USSD can be used for mobile banking, checking account balance, or recharging mobilecredit by dialing specific codes.
- It is offered through a National Unified USSD Platform (NUUP) on a short code *99#.

Credit Card

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle. Following are the actors in the credit card system.

- **The card holder** − Customer
- **The merchant** − seller of product who can accept credit card payments.
- **The card issuer bank** − card holder's bank

- **The acquirer bank** − the merchant's bank
- **The card brand** − for example , visa or Mastercard.

Credit Card Payment Proces

Step	Description
Step 1	Bank issues and activates a credit card to the customer on his/her request.
Step 2	The customer presents the credit card information to the merchant site or to the merchant from whom he/she wants to purchase a product/service.
Step 3	Merchant validates the customer's identity by asking for approval from the card brand company.
Step 4	Card brand company authenticates the credit card and pays the transaction by credit. Merchant keeps the sales slip.
Step 5	Merchant submits the sales slip to acquirer banks and gets the service charges paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 6	Now the card brand company asks to clear the amount from the issuer bank and the amount gets transferred to the card brand company.

Debit Card

Debit card, like credit card, is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between a debit card and a credit card is that in case of payment through debit card, the amount gets deducted from the card's bank account immediately and there should be sufficient balance in the bank account for the transaction to get completed; whereas in case of a credit card transaction, there is no such compulsion.

Debit cards free the customer to carry cash and cheques. Even merchants accept a debit card readily. Having a restriction on the amount that can be withdrawn in a day using a debit card helps the customer to keep a check on his/her spending.

E-Wallet:

Electronic wallet is a type of electronic card which is used for transactions made online through a computer or a smartphone. The utility of e-wallet is same as a credit or debit card. An e-wallet needs to be linked with the individual's bank account to make payments. The main objective of e-Wallet is to make paperless money transaction easier.

E-wallets are classified as Prepaid Payment Instruments (PPIs) per Indian regulation. PPIs are payment instruments that facilitate the purchase of goods and services, including funds transfer, against the value stored

in them. PPIs can be issued as smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets, paper vouchers, and any such instrument that can be used to access the pre-paid amount.

A mobile wallet is the digital equivalent to the physical wallet that we have in our pockets today. It is a vault to store digitized valuables for authorization. It is an online platform which allows a user to undertake various transactions without physical money transactions. It provides mobile-based financial services to the unbanked and those living in the remote geographical locations.

Internet Banking

Internet banking, also known as online banking or e-bankingor Net Banking is a facility offered by banks and financial institutions that allow customers to use banking services over the internet. Customers need not visit their bank's branch office to avail each and every small service. Not all account holders get access to internet banking. If you would like to use internet banking services, you must register for the facility while opening the account or later. You have to use the registered customer ID and password to log into your internet banking account.

Advantages of Internet Banking

Availability: You can avail the banking services round the clock throughout the year. Most of the services offered are not time-restricted; you can check your account balance at any time and transfer funds without having to wait for the bank to open.

Easy to Operate: Using the services offered by online banking is simple and easy. Many find transacting online a lot easier than visiting the branch for the same.

Convenience: You need not leave your chores behind and go stand in a queue at the bank branch. You can complete your transactions from wherever you are. Pay utility bills, recurring deposit account instalments, and others using online banking.

Time Efficient: You can complete any transaction in a matter of a few minutes via internet banking. Funds can be transferred to any account within the country or open a fixed deposit account within no time on netbanking.

Activity Tracking: When you make a transaction at the bank branch, you will receive an acknowledgement receipt. There are possibilities of you losing it. In contrast, all the transactions you perform on a bank's internet banking portal will be recorded. You can show this as proof of the transaction if need be.

Features of Online Banking

- Check the account statement online.
- Open a fixed deposit account.
- Pay utility bills such as water bill and electricity bill.
- Make merchant payments.
- Transfer funds.
- Order for a cheque book.

- Buy general insurance.
- Recharge prepaid mobile/DTH.

Internet banking provides facilities like NEFT, RTGS, and IMPS as fund transfer options and all you must do is pick one of these options, basis your requirements:

NEFT: National Electronic Funds Transfer is the most popular method of electronic money transfer across banks in the country. NEFT works on a deferred settlement basis. NEFT payments are made in hourly instalments. NEFT is the most affordable and secure method of money transfer.

RTGS: Real-time Gross Settlement is the preferred method of settlement for transactions that require immediate gratification. This system guarantees immediate fund transfers with no wait time. Generally used for transactions of greater value, RTGS ensures rapid and secure funds transfers within the banking system, improving efficiency for individuals and businesses.

IMPS: With Immediate Payment Service, you can do instant transactions 24/7. Whether you need to send a friend some money, pay your bills quickly, or make a quick purchase, IMPS makes it easy to transfer funds right away. Thanks to UPI, IMPS has become a part of the digital world, making it super convenient for people who are always on the move.IMPS allows users to make 24/7 fund transfers through mobile phones, internet banking, ATMs, or designated agents.

Online Bill Payment:

- Online bill payment enables users to pay their utility bills, such as electricity, water, telephone, or internet bills, through digital platforms.
- Userscanmakepaymentsusingnetbanking, UPI, eWallets, or other digital payment methods.

Online bill pay is a service that allows users to make bill payments through a website or app, often from a bank account. It can be used to make one-time or recurring payments, and users may also be able to schedule future payments.

Online bill pay can save time, and help users avoid late fees. It can also simplify finances by eliminating the need to write out checks or count and distribute paper currency.

Point of Sale (POS)

POS refers to the point where a customer makes a payment, and goods or services are exchanged. It ensures that transactions run smoothly. POS systems have components like hardware, cash registers, barcode scanners, payment terminals, and software that process transactions and record sales data. Whether a credit card swipe, mobile payment, or cash payment, POS payment is where the transaction happens. These components work together seamlessly to ensure a hassle-free transaction for a customer.

- PoS (Point of Sale) refers to the location or device where a customer makes a payment for goods or services.
- PoS systems can be traditional card swipe machines or modern contactless payment terminals like NFC-enabled devices or QR code scanners.

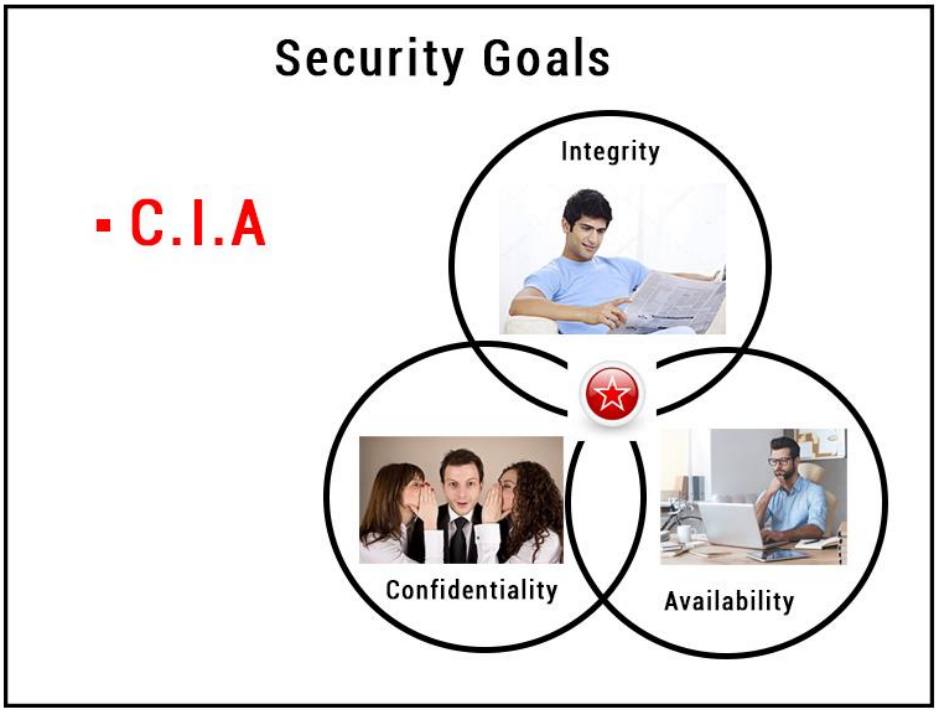
Cyber Security

Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access.

Cyber Security Goals

Cyber security can be measured by at least one of three goals-

1. Protect the confidentiality of data.
2. Preserve the integrity of data.
3. Promote the availability of data for authorized users.



CIA Triad

Confidentiality

Confidentiality is roughly equivalent to privacy and avoids the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it. It prevents essential information from reaching the wrong people while making sure that the right people can get it. Data encryption is a good example to ensure confidentiality.

Integrity

Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not been altered in an unauthorized way, and that source of the information is genuine.

Availability

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Significance of Cyber security:

Protecting Sensitive Data:

With the increase in digitalization, data is becoming more and more valuable. Cyber security helps protect sensitive data such as personal information, financial data, and intellectual property from unauthorized access and theft.

Prevention of Cyber Attacks:

Cyber attacks, such as **Malware infections**, **Ransomware**, **Phishing**, and **Distributed Denial of Service** (DDoS) attacks, can cause significant disruptions to businesses and individuals. Effective cyber security measures help prevent these attacks, reducing the risk of data breaches, financial losses, and operational disruptions.

Safeguarding Critical Infrastructure:

Critical infrastructure, including power grids, transportation systems, healthcare systems, and communication networks, heavily relies on interconnected computer systems. Protecting these systems from cyber threats is crucial to ensure the smooth functioning of essential services and prevent potential disruptions that could impact public safety and national security.

Maintaining Business Continuity:

Cyber attacks can cause significant disruption to businesses, resulting in lost revenue, damage to reputation, and in some cases, even shutting down the business. Cyber security helps ensure business continuity by preventing or minimizing the impact of cyber attacks.

Compliance with Regulations:

Many industries are subject to strict regulations that require organizations to protect sensitive data. Failure to comply with these regulations can result in significant fines and legal action.

Protecting National Security:

Cyber attacks can be used to compromise national security by targeting critical infrastructure, government systems, and military installations. Cyber security is critical for protecting national security and preventing cyber warfare.

Preserving Privacy:

In an era where personal information is increasingly collected, stored, and shared digitally, cyber security is crucial for preserving privacy. Protecting personal data from unauthorized access, surveillance, and misuse helps maintain individuals' privacy rights and fosters trust in digital services.

Challenges of Cyber security

Constantly Evolving Threat Landscape:
Cyber threats are constantly evolving, and attackers are becoming increasingly sophisticated. This makes it challenging for cyber security professionals to keep up with the latest threats and implement effective measures to protect against them.

Lack of Skilled Professionals:
There is a shortage of skilled cyber security professionals, which makes it difficult for organizations to find and hire qualified staff to manage their cyber security.

Limited Budgets:
Cyber security can be expensive, and many organizations have limited budgets to allocate towards cyber security initiatives. This can result in a lack of resources and infrastructure to effectively protect against cyber threats.

Insider Threats:
Insider threats can be just as damaging as external threats. Employees or contractors who have access to sensitive information can intentionally or unintentionally compromise data security.

Complexity of Technology:
With the rise of cloud computing, IoT, and other technologies, the complexity of IT infrastructure have increased significantly. This complexity makes it challenging to identify and address vulnerabilities and implement effective cyber security measures.

Computer Security Threats

A security threat is a threat that has the potential to harm computer systems and organizations. The cause could be physical, such as a computer containing sensitive information being stolen. It's also possible that the cause isn't physical, such as a viral attack.

Types of Threats:
The threads can be commonly caused by:

(i) Malware: Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge. Malware tries to go unnoticed by either hiding or not letting the user know about its presence on the system. You may notice that your system is processing at a slower rate than usual.

(ii) Virus: It is a program that replicates itself and infects your computer's files and programs, rendering them inoperable. It is a type of malware that spreads by inserting a copy of itself into and becoming part of another program. It spreads with the help of software or documents. They are embedded with software and documents and then transferred from one computer to another using the network, a disk, file sharing, or infected e-mail. They usually appear as an executable file.

(iii) Spyware: Spyware is a type of computer program that tracks, records, and reports a user's activity (offline and online) without their permission for the purpose of profit or data theft. Spyware can be acquired from a variety of sources, including websites, instant chats, and emails. A user may also unwittingly obtain spyware by adopting a software program's End User License Agreement.
Adware is a sort of spyware that is primarily utilized by advertising. When you go online, it keeps track of your web browsing patterns in order to compile data on the types of websites you visit.

(iv) Worms: Computer worms are similar to viruses in that they replicate themselves and can cause exact similar damage. Unlike viruses, which spread by infecting a host file, worms are freestanding programs that do not require a host program or human assistance to proliferate. Worms don't change programs; instead, they replicate themselves over and over. They just eat resources to make the system down.

(v) Trojan: A Trojan horse is malicious software that is disguised as a useful host program. When the host program is run, the Trojan performs a harmful/unwanted action. It is malicious malware or software that appears to be legal yet has the ability to take control of your computer. A Trojan is a computer program that is designed to disrupt, steal, or otherwise harm your data or network.

(vi) Denial Of Service Attacks: A Denial of Service attack is one in which an attacker tries to prohibit legitimate users from obtaining information or services. An attacker tries to make a system or network resource unavailable to its intended users in this attack. The web servers of large organizations such as banking, commerce, trading organizations, etc. are the victims.

(vii) Phishing: Phishing is a type of attack that is frequently used to obtain sensitive information from users, such as login credentials and credit card details. They deceive users into giving critical information, such as bank and credit card information, or access to personal accounts, by sending spam, malicious Web sites, email messages, and instant chats.

(viii) Key-Loggers: Keyloggers can monitor a user's computer activity in real-time. Keylogger is a program that runs in the background and records every keystroke made by a user, and then sends the data to a hacker with the intent of stealing passwords and financial information.

Cyber Attack-Precautions

In order to keep your system data secure and safe, you should take the following measures:

1. Always keep a backup of your data.

2. Install firewall software and keep it updated every time.

3. Make use of strong and difficult to crack passwords (having capital & small alphabets, numbers, and special characters).

4. Install antivirus/ anti-spyware and keep it updated every time.

5. Timely scan your complete system.

6. Before installing any program, check whether it is safe to install it (using Antivirus Software).

7. Take extra caution when reading emails that contain attachments.

8. Always keep youroperating system updated.

Cyber Attack-Safety Measures

1. Use an Internet Security Suite:
We may use an antivirus program combined with an internet security program, its help you in:

- Avoiding malicious downloads done by mistake.
- Avoiding malicious installs done by mistake.
- Preventing from being a victim to Man In The Middle Attack(MITM)
- Protection from phishing.
- Protection from damage that Trojan horses may cause.

2. Use Strong Passwords:
Your password should be strong enough to be practically unbreakable. A strong password is one that is 12+ characters long and contains a diverse use of alphabets(both cases), numbers and symbols (and spaces). Setting a really unbreakable password should not be difficult specially when there are help available as random password generator applications.

3. Keep Your Software Up-to-Date: we should update our Operating System, Antivirus and other softwares which we used in our computer or Mobile devices

4. Avoid Identity Theft:
Identity theft is when someone else uses your personal information to impersonate you on any platform to gain benefits in your name ,identity theft can cause you to damage more serious than financial losses. The most common reason for identity theft is improper management of sensitive personal data. There are some things to be avoided when dealing with personally identifiable data:

- Never share your Aadhaar/PAN number(In India) with anyone whom you do not know/trust.
- Do not post sensitive data on social networking sites.
- Do not make all the personal information on your social media accounts public.
- Please never share an Aadhaar OTP received on your phone with someone over a call.
- Make sure that you do not receive unnecessary OTP SMS about Aadhaar(if you do, your Aadhaar number is already in the wrong hands)
- Do not fill personal data on the website that claim to offer benefits in return.

5. Be careful with links and attachments:
Be careful when clicking on links or attachments in emails, even if they seem to be from a trusted source. It's always best to verify the authenticity of the email and the link or attachment before clicking on them.

- Verify the authenticity of the email: Before clicking on any links or attachments in an email, verify that the email is legitimate and that it comes from a trusted source.
- Check the sender's email address: Phishers often use email addresses that are similar to, but not exactly the same as, the email address of a trusted source. Be sure to check the sender's email address carefully.
- Look for suspicious links: If an email contains a link, hover your cursor over the link to see where it leads. If the link is suspicious, do not click on it.
- Be wary of unsolicited attachments: If you receive an attachment from an unknown sender or that is unexpected, be wary of opening it. Malicious attachments can contain malware that can infect your computer.

6. Take appropriate actions if you have been a Victim:
There are few things that should be done as soon as you realize you have been hacked:

- File a formal complaint with the police and inform the other relevant authorities, Report to www.cybercrime.gov.in or use a toll free number 1930.
- Try regaining access to your compromised accounts by utilizing secondary contacts.
- Reset the password for other accounts and websites that were using the same password as the account that was compromised.
- Perform a factory reset and proper formatting of your devices that are affected(assuming you have your data backed up already).
- Stay aware of the current data breaches and other incidents of the cyber world to prevent such incidents from happening again and staying safe online.

Cyber Security Tools

Cyber security tools are a set of systems and techniques that protect an organization's networks, applications, code repositories, and other critical systems from known and unknown threats by monitoring, identifying, remediating, and mitigating them.

1.Firewall

Firewalls are security systems within networks that monitor the flow of both incoming and outgoing data. They evaluate the data moving along their borders and use a set of predetermined rules to decide what data can and cannot pass through the barrier.

2. Anti-Malware

It is a type of software-based cyber security tool that prevents malware (malicious software) from infecting a computer and removes existing malware from devices and systems. There are three common types of anti-malware software, each with its own method for identifying and removing malware

4.Anti-Virus
It is another one of the tools for cyber security that is used to prevent and protect our computer systems from computer virus infection. It's generally recommended that everyone install some sort of anti-virus software on their devices to keep dangerous software from infecting it.

4. Penetration Testing Software

It is a cyber security technique that simulates a cyberattack on a system. This may also be known as a pen test or ethical hacking. The test is designed to identify weaknesses within a system and determine the likelihood of a breach.

5.Network Monitoring Software

Through the use of network monitoring software, administrators can determine if a network is running optimally and proactively identify deficiencies. Network monitoring provides a clear picture of all the connected devices on a network, allowing system administrators to see how data is moving between them and quickly correct any flaws that could undermine network performance or lead to outages.

Computer Ethics:

Cyber Ethics governs rules that individuals must be polite and responsible when they use the internet. Cyberethics aim to protect the moral, financial, social behavior of individuals. Cyberethics engages the users to use the internet safely and use technology responsibly and sensibly. Cyberethicsempathizes the behavior that must be adopted while using cyber technology.

Some of the breaches of cyberethics are listed below:

- **Cyber Bullying:** Cyberbullying is a form of bullying carried out via internet technology such as social media where individuals are mocked on their physical appearance, lifestyle, preferences, etc. The teenage generation or say youngsters are the major victims of this form of cyber ethic breach. Cyberbullying affects the emotional ethics of individuals and can cause mental disturbance to individuals.
- **Hacking:** Stealing a user's personal or organizational information without authorized permission is

not considered a good practice. It is one of the riskiest cyber breaches to data leak. Data leak includes passing of sensitive information such as passwords, bank details of the user to a third-party user who is not authorized to access the information.

- **Copywriting:** Claiming of another individual as one's own is another type of cyber ethic breach that must be eradicated. Never engage in copywriting another person's content or document and claim as it is your own. It leads to a serious problem called plagiarism, which is a punishable offense and considered a legal crime. It is always advisable to follow general cyberethics, while using the internet or say any kind of technology.

Cyber Ethics focuses on the following:

1. Privacy:

- The content that is available on the internet should not hurt any moral, emotional, or personal ethics of individuals.
- Users should have the right to protect any information which they don't want to share openly.
- Private information like user's contact details, address, security-related information like bank details, credit card/debit card details, are all included in basic cyber ethics of user privacy and must not be breached in any case.
- Any breach of privacy is theft/fraud of user identity and user personal information, which is punishable as per the rules of law.

2. IPR:

- IPR stands for Intellectual Property Rights.
- IPR defines that the owners have the complete right to the content that is posted on the internet.
- The entire content is solely a belonging of the originator and no individual is allowed to claim that content published by the original creator as its own.
- Unauthorized distribution of someone else's work should never be adopted as it's ethically incorrect to not give creation and monetary benefits to the creator of the work.

3. Security:

- Security on the internet is the most basic ethical right that every user must be accessible.
- Users of the internet should feel safe while they surf the net.
- Security, in general means only authorized users to have access to the content on the computer.
- And confidential information is safe, without any risk of loss of information/content.

4. Accuracy:

- The content available on the internet is accessed by billions of users.
- If there is no reliability of the information that is posted online, then it would mislead the masses.
- Cyberethics assert the importance of posting content on the internet that is correct in all aspects.
- Users trust the content of the internet and rely heavily on the internet for facts, therefore it is highly needed that the asked information is correct and reliable.

Best policies that individuals must adopt while using the internet or any kind of technology should include the following:

- Being Polite and not using harsh words.
- Avoid clicking on unknown links.
- Wisely opening Emails from known senders only.
- Not mocking anyone on Social Media.
- Not copying any individual's work and claiming it as their own. Always cite that you have used someone else's work.
- Be careful and research before installing any free software.
- Never intrude on another person's privacy.
- Don't contribute to any malpractice that can lead to the leak of data of an individual or organization.

- Never engage in Cyberbullying.
- Never compromise with the safety of your system. Always install an anti-virus on your system.

Legal issues in Cyber Security

Acts related to information technology

The Government has created certain acts to protect against fraud and illegal activities happening in the cyber space.

Cyber Laws of India

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

- The Computer as a Target :- using a computer to attack other computers.
  e.g. Hacking,Virus/Worm attacks, DOS attack etc.
- computer as a weapon :- using a computer to commit real world crimes.
  e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Difference between Ethics and law

Ethics	**Laws**
These are unwritten principles.	These are formal, well-documented principles.
These are defined by individuals and may vary	These are created by the

depending on personal choice.	Government and court.
These cannot be applied to everyone. Most of the time, the ethics of different companies will be different.	Laws are applicable to everyone.

UNIT IV

Cloud Computing

Cloud computing is an emerging technology that is becoming more and more popular. This is due primarily to its elastic nature, users can acquire and release resources on-demand, and pay only for the resources they need (pay-per-use or pay-as-you-go model). Cloud computing offers real-time delivery of products, services and solutions over the Internet that is highly scalable and highly available distributed computing services. Cloud computing provides opportunities for organizations to become more cost-effective, productive, and flexible in order to rapidly deliver new capabilities.

Cloud Computing as a service model

Cloud computing is the next stage of the Internet evolution. A typical cloud have several distinct properties: elasticity and scalability, multi-tenancy, self-managed function capabilities, service billing and metering functions, connectivity interfaces and technologies. In addition, a cloud supports large scale user accesses at distributed locations over the Internet, offers on-demand application services at anytime, and provides both virtual and/or physical computing resources for customers.

There are three types of clouds:

Private clouds: Built, operated and managed by an organization for its internal use only to support its business operations exclusively. It is based on a private network behind a firewall that provides hosted services to a limited number of people.

Public clouds: Provided by a designated service provider for general public under a utility based pay-per-use consumption model. The cloud resources are hosted generally on the service provider premises. Popular example of public cloud are Amazon's AWS, Rackspace Cloud Suite, and Microsoft's Azure Service Platform, which are the clouds with public accessible services over the Internet; the main benefits of using a public cloud service are easy and inexpensive setup, scalability to meets needs, no wasted resources because you pay for what you use.

Hybrid clouds: which are made of different types of clouds, including public and private clouds.Organization provides and manages some resources in-house and has others provided externally.

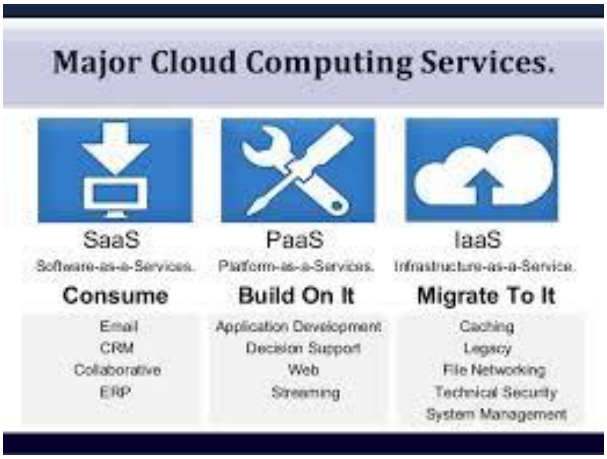
The selection of a deployment model depends on the opportunities to increase earnings and reduce costs.

Service Model

Infrastructure-as-a-Service (IaaS): Offers virtualized resources (computation, storage, and communication) on demand is known as IaaS. IaaS designates the provision of IT and network resources such as processing, storage and bandwidth as well as management middleware.

Platform-as-a-Service (PaaS):Designates programming environments and tools supported by cloud providers that can be used by consumers to build and deploy applications onto the cloud infrastructure. Examples of PaaS include Amazon, Google App Engine , and Microsoft Windows Azure .

Software-as-a-Service (SaaS): Designates hosted vendor applications. For example, Google Apps (such as Google Docs, Google Calendar or Google Sites).



Source: http://www.slideshare.net/

Cloud computing allows the user to increase capacity or add capabilities on the fly without investing in new infrastructure, training personnel, or licensing new software. Cloud Computing encompasses any subscription-based or pay-per-use service that, in real time over the internet, extends IT's capabilities.

Big Data

What is Big Data?

Big data refers to extremely large and diverse collections of structured, unstructured, and semi-structured data that continues to grow exponentially over time. These datasets are so huge and complex in volume, velocity, and variety, that traditional data management systems cannot store, process, and analyze them.

Types of Big Data:

Big Data falls into three main categories:

Structured Data

Any data that can be stored, accessed, and processed in a fixed format is known as structured data. Businesses can get the most out of this type of data by performing analysis. Advanced technologies help generate data-driven insights to make better decisions from structured data.

Unstructured Data

Data that has an unknown structure or form is unstructured data. Processing and analyzing this type of data for data-driven insights can be a difficult and challenging task as they are under different categories and putting them together in a box will not be of any value. A combination of simple text files, images, videos, etc., is an example of unstructured data.

Semi-structured data

Semi-structured data, as you may have already guessed, has both structured and unstructured data. Semi-structured data may seem structured in form, but it is not exactly well-defined with table definition in relational DBMS. Web applications have unstructured data such as transaction history files, log files, etc.

Characteristics of Big Data

These are essentially called the characteristics of big data and are termed as volume, velocity, variety, veracity and value giving rise to the popular name 5Vs of big data

Characteristics of Big Data	Details
Volume	Organizations have to constantly scale their storage solutions since big data requires a large amount of space to be stored.
Velocity	Since big data is being generated every second, organizations need to respond in real time to deal with it.
Variety	Big data comes in a variety of forms. It could be structured or unstructured, or even in different formats such as text format, videos, images, and more.
Veracity	Big data, as large as it is, can contain wrong data too. Uncertainty of data is something organizations have to consider while dealing with big data.
Value	Just collecting big data and storing it is of no consequence unless the data is analyzed and a useful output is produced.

Applications of Big Data

There are many real-life Big Data applications in various industries. Let’s discuss some of them in brief.

- **Fraud Detection**

Big data helps in risk analysis, management, fraud detection, and abnormal trading analysis.

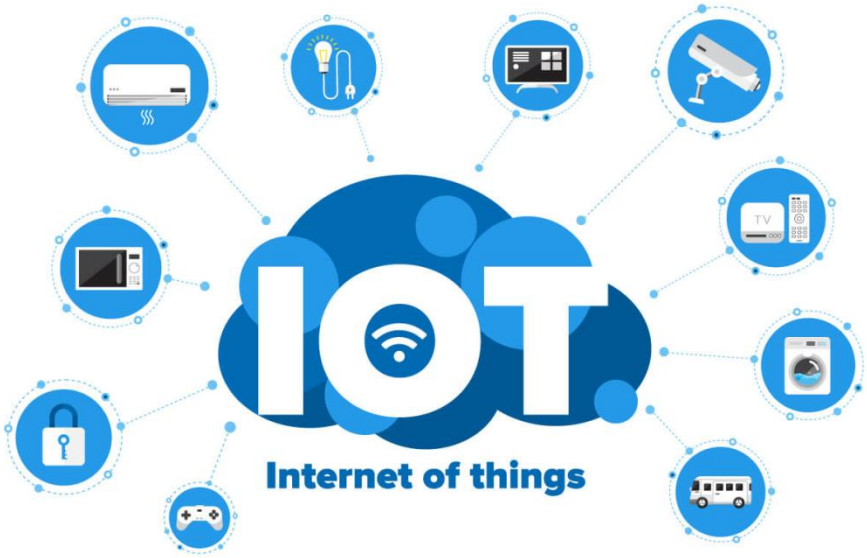
- **Advertising and Marketing**

Big data helps advertising agencies understand the patterns of user behavior and then gather information about consumers' motivations.

- **Agriculture**

Big data can be used to sensor data to increase crop efficiency. This can be done by planting test crops to record and store the data about how crops react to various environmental changes and then using that data for planning crop plantation, accordingly.

Internet of Things (IoT)



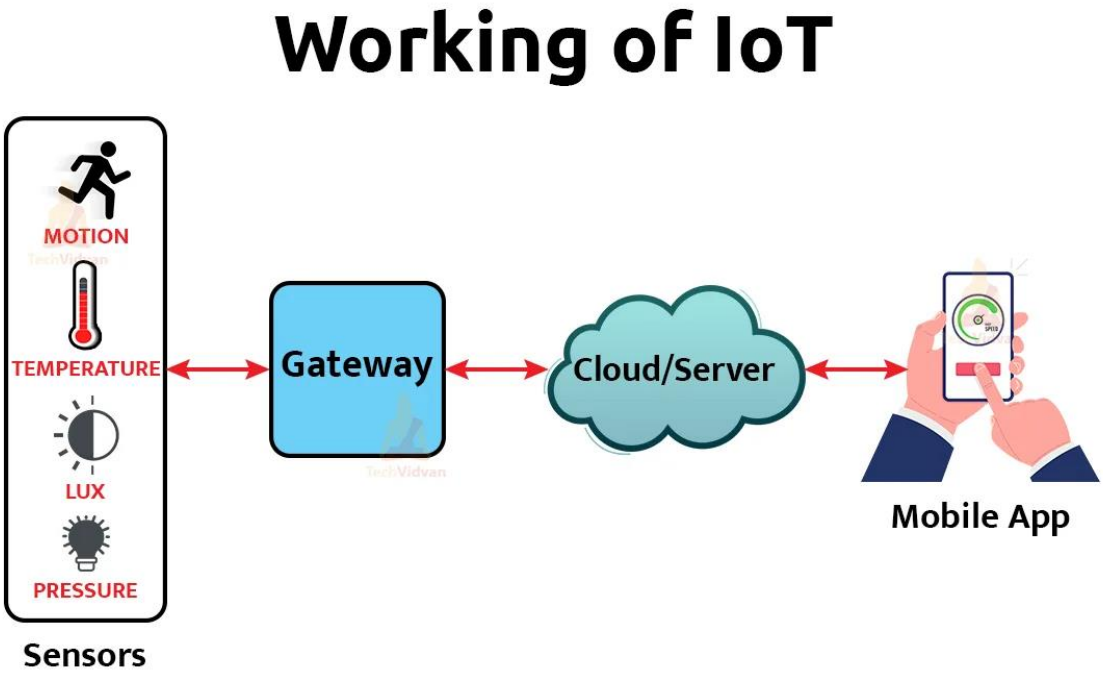
Introduction to Internet of Things (IoT)

-

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment.IOT is a system of interrelated things, computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers. And the ability to transfer the data over a network requiring human-to-human or human-to-computer interaction.

Over 9 billion 'Things' (physical objects) are currently connected to the Internet, as of now. In the near future, this number is expected to rise to 20 billion.

Key Components and Working Steps of IoT:



1) Sensors/Devices

First, sensors or devices collect data from their environment. This data could be as simple as a temperature reading or as complex as a full video feed.In this first step data is being collected from the environment by *something*.

2) Connectivity

Next, that data is sent to the cloud, but it needs a way to get there, the sensors/devices can be connected to the cloud through a variety of methods including: cellular, satellite, WiFi, Bluetooth, low-power wide-area networks (LPWAN), connecting via a gateway/router or connecting directly to the internet via ethernet

3) Data Processing

Once the data gets to the cloud, software performs some kind of processing on it. This could be very simple, such as checking that the temperature reading is within an acceptable range. Or it could also be very complex, such as using computer vision on video to identify objects (such as intruders on a property).

4) User Interface

Next, the information is made useful to the end-user in some way. This could be via an alert to the user (email, text, notification, etc). For example, a text alert when the temperature is too high in the company's cold storage.
Depending on the IoT application, the user may also be able to perform an action and affect the system. For example, the user might remotely adjust the temperature in the cold storage via an app on their phone.
And some actions are performed automatically. Rather than waiting for you to adjust the temperature, the system could do it automatically via predefined rules. Rather than just call you to alert you of an intruder, the IoT system could also automatically notify security teams or relevant authorities.

Application of IoT :

Application type	Description

Application type	Description
Smart Thermostats	Helps you to save resource on heating bills by knowing your usage patterns.
Activity Trackers	Helps you to capture heart rate pattern, calorie expenditure, activity levels, and skin temperature on your wrist.
Parking Sensors	IoT technology helps users to identify the real-time availability of parking spaces on their phone.
Connect Health	The concept of a connected health care system facilitates real-time health monitoring and patient care. It helps in improved medical decision-making based on patient data.
Smart City	Smart city offers all types of use cases which include traffic management to water distribution, waste management, etc.
Smart home	Smart home encapsulates the connectivity inside your homes. It includes smoke detectors, home appliances, light bulbs, windows, door locks, etc.

Virtual Reality

Virtual reality (VR) is a computerized recreation of an engaging, three-dimensional world. It can be experienced through specialized electronic devices, like a virtual reality headset, and interacted with in real time. The virtual setting might be a duplicate of reality or wholly made up.

Virtual reality (VR) offers users a sensation of presence and immersion in a virtual environment. It may pique their senses of sight, hearing, touch, and even smell, making for a singular and captivating experience. Users may explore and interact with virtual items and characters, the environment can react to their activities in real-time, giving them the impression that they are physically present there.

Types of Virtual Reality

Virtual reality (VR) technologies come in a variety of forms and are actively being used or developed. Some of the types are listed below:

Non-Immersive VR

The most basic type of virtual reality (VR) employs a computer screen or projection device to show a virtual environment. A mouse, keyboard, or other input device can be used by users to interact with the environment. This kind of VR is frequently utilized in instruction and training.

Semi-Immersive VR

A larger projection screen or numerous displays are used in semi-immersive VR, a more advanced type of VR, to produce a more immersive experience. To interact with the environment, users often wear 3D glasses and use handheld input devices.

Fully Immersive VR

The most advanced form of virtual reality (VR) employs a head-mounted display (HMD) to provide an immersive experience. The HMD usually includes a screen and sensors that track the movement of your eyes. This sort of VR is ordinarily utilized in gaming, diversion, and the virtual travel industry.

WebVR

With WebVR, users may access virtual worlds directly from a web browser without the need for an additional program. In marketing and e-commerce, this kind of VR is rising in popularity.

Augmented Reality (AR)

A kind of virtual reality called augmented reality superimposes virtual components on the actual environment. Users often use special glasses or a smartphone or tablet screen to view the virtual pieces. AR is often employed in industries including advertising, retail, and education.

Difference between Augmented Reality and Virtual Reality

Virtual Reality Applications

Let’s take a look to know the use cases of virtual reality:

Gaming:

To produce immersive gaming experiences, VR is frequently employed in the gaming business. Virtual reality gaming gives players a degree of contact and engagement that traditional games cannot equal, giving them the impression that they are truly playing the game.

Education and Training:

In order to produce immersive and engaging learning experiences, VR is employed in education and training. Engineers may use VR to replicate complicated machinery or building projects, and medical students can use it to rehearse intricate medical procedures in a realistic setting.

Tourism and hospitality:

Virtual reality technology is utilized in these sectors to offer tours of hotels, resorts, and tourist attractions. Customers may experience a destination virtually before they go, which helps them make better choices.

Healthcare:

Anxiety, PTSD, and chronic pain are just a few of the illnesses that are treated and managed using VR in the medical field.

Cloud Computing

Cloud computing is the on-demand availability of computing resources (such as storage and infrastructure), as services over the internet. It eliminates the need for individuals and businesses to self-manage physical resources themselves, and only pay for what they use.

Characteristics of Cloud Computing

1. Broad network access
2. Resource pooling
3. On-demand self-service
4. Rapid elasticity
5. Measured service

Types of Clouds

Public Cloud

The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the internet. With a public cloud, all hardware, software, and other supporting infrastructure are owned and managed by the cloud provider. Microsoft Azure is an example of a public cloud.

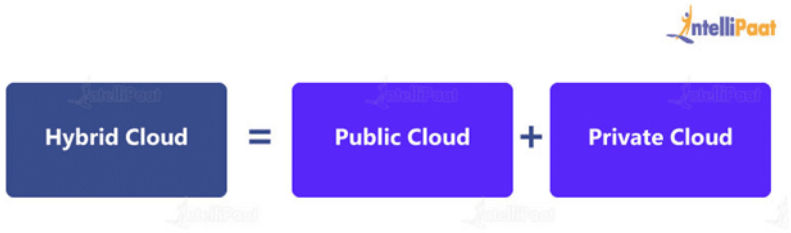
Private Cloud

A private cloud consists of cloud computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization's on-site datacenter, or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization.

Examples of private clouds are – Amazon VPC, HPE, VMware, and IBM.

Hybrid Cloud

The combination of the public and the private cloud models is called a hybrid cloud.



Example: Gmail, Google Drive, Google Apps, AWS, MS Office on the Web, One Drive, etc.

Community Cloud

The community cloud, as the name suggests, allows services and systems to be accessible by a group of organizations to share information between them and a specific community. It can be owned, operated, and managed by multiple organizations in the community, a third party, or a combination of them.

Example: The US-based dedicated IBM SoftLayer cloud for federal agencies, healthcare community cloud, etc.

Cloud Computing Services

Software as a Service (SaaS)

SaaS (also known as cloud application services) mostly runs directly through the web browser without downloading and installing these applications.

Example: Dropbox, Google Apps, Slack, Hubspot, Salesforce, Cisco WebEx, etc.

Platform as a Service (PaaS)

PaaS (also known as cloud platform services) is similar to SaaS, but it provides a platform for software creation.

Example: Windows Azure, Magento Commerce Cloud, Force.com, OpenShift, etc.

Infrastructure as a Service (IaaS)

IaaS (also known as cloud infrastructure services) manages applications' data, runtime environments, and middleware.

Example: Google Compute Engine (GCE), AWS EC2, Cisco Metapod, etc.

Cyber Security

Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access.

Cyber Security Goals

Cyber security can be measured by at least one of three goals-

4. Protect the confidentiality of data.
5. Preserve the integrity of data.
6. Promote the availability of data for authorized users.

Significance of Cyber security:

Protecting Sensitive Data:

Cyber security helps protect sensitive data such as personal information, financial data, and intellectual property from unauthorized access and theft.

Prevention of Cyber Attacks:

Cyber attacks, such as **Malware infections**, **Ransomware**, **Phishing**, and **Distributed Denial of Service** (DDoS) attacks, can cause significant disruptions to businesses and individuals. Effective cyber security measures help prevent these attacks, reducing the risk of data breaches, financial losses, and operational disruptions.

Safeguarding Critical Infrastructure:

Critical infrastructure, including power grids, transportation systems, healthcare systems, and communication networks, heavily relies on interconnected computer systems. Protecting these systems from cyber threats is crucial to ensure the smooth functioning of essential services and prevent potential disruptions that could impact public safety and national security.

Maintaining Business Continuity:

Cyber attacks can cause significant disruption to businesses, resulting in lost revenue, damage to reputation, and in some cases, even shutting down the business. Cyber security helps ensure business continuity by preventing or minimizing the impact of cyber attacks.

Compliance with Regulations:

Many industries are subject to strict regulations that require organizations to protect sensitive data. Failure to comply with these regulations can result in significant fines and legal action.

Protecting National Security:

Cyber attacks can be used to compromise national security by targeting critical infrastructure, government systems, and military installations. Cyber security is critical for protecting national security and preventing cyber warfare.

Preserving Privacy:

cyber security is crucial for preserving privacy. Protecting personal data from unauthorized access, surveillance, and misuse helps maintain individuals' privacy rights and fosters trust in digital services.

Challenges of Cyber security

Constantly Evolving Threat Landscape:

Cyber threats are constantly evolving, and attackers are becoming increasingly sophisticated. This makes it challenging for cyber security professionals to keep up with the latest threats and implement effective measures to protect against them.

Lack of Skilled Professionals:

There is a shortage of skilled cyber security professionals, which makes it difficult for organizations to find and hire qualified staff to manage their cyber security.

Limited Budgets:

Cyber security can be expensive, and many organizations have limited budgets to allocate towards cyber security initiatives. This can result in a lack of resources and infrastructure to effectively protect against cyber threats.

Insider Threats:

Employees or contractors who have access to sensitive information can intentionally or unintentionally compromise data security.

Complexity of Technology:
With the rise of cloud computing, IoT, and other technologies, the complexity of IT infrastructure have increased significantly. This complexity makes it challenging to identify and address vulnerabilities and implement effective cyber security measures.

Computer Security Threats

A security threat is a threat that has the potential to harm computer systems and organizations. The cause could be physical, such as a computer containing sensitive information being stolen. It's also possible that the cause isn't physical, such as a viral attack.

Types of Threats:

The threads can be commonly caused by:

(i) Malware: Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge. Malware tries to go unnoticed by either hiding or not letting the user know about its presence on the system. You may notice that your system is processing at a slower rate than usual.

(ii) Virus: It is a program that replicates itself and infects your computer's files and programs, rendering them inoperable. It is a type of malware that spreads by inserting a copy of itself into and becoming part of another program. It spreads with the help of software or documents. They are embedded with software and documents and then transferred from one computer to another using the network, a disk, file sharing, or infected e-mail. They usually appear as an executable file.

(iii) Spyware: Spyware is a type of computer program that tracks, records, and reports a user's activity (offline and online) without their permission for the purpose of profit or data theft. Spyware can be acquired from a variety of sources, including websites, instant chats, and emails.
Adware is a sort of spyware that is primarily utilized by advertising. When you go online, it keeps track of your web browsing patterns in order to compile data on the types of websites you visit.

(iv) Denial Of Service Attacks: A Denial of Service attack is one in which an attacker tries to prohibit legitimate users from obtaining information or services. An attacker tries to make a system or network resource unavailable to its intended users in this attack. The web servers of large organizations such as banking, commerce, trading organizations, etc. are the victims.

(v) Phishing: Phishing is a type of attack that is frequently used to obtain sensitive information from users, such as login credentials and credit card details. They deceive users into giving critical information, such as bank and credit card information, or access to personal accounts, by sending spam, malicious Web sites, email messages, and instant chats.

(vi) Key-Loggers: Keyloggers can monitor a user's computer activity in real-time. Keylogger is a program that runs in the background and records every keystroke made by a user, and then sends the data to a hacker with the intent of stealing passwords and financial information.

Cyber Attack-Precautions

In order to keep your system data secure and safe, you should take the following measures:

1. Always keep a backup of your data.

2. Install firewall software and keep it updated every time.

3. Make use of strong and difficult to crack passwords (having capital & small alphabets, numbers, and special characters).

4. Install antivirus/ anti-spyware and keep it updated every time.

5. Timely scan your complete system.

6. Before installing any program, check whether it is safe to install it (using Antivirus Software).

7. Take extra caution when reading emails that contain attachments.

8. Always keep your operating system updated.

Cyber Attack-Safety Measures

1. Use an Internet Security Suite:
We may use an antivirus program combined with an internet security program, its help you in:

- Avoiding malicious downloads done by mistake.
- Avoiding malicious installs done by mistake.
- Preventing from being a victim to Man In The Middle Attack(MITM)
- Protection from phishing.
- Protection from damage that Trojan horses may cause.

2. Use Strong Passwords:
A strong password is one that is 12+ characters long and contains a diverse use of alphabets(both cases), numbers and symbols (and spaces). Setting a really unbreakable password should not be difficult specially when there are help available as random password generator applications.

3. Keep Your Software Up-to-Date: we should update our Operating System, Antivirus and other softwares which we used in our computer or Mobile devices

4. Avoid Identity Theft:
Identity theft is when someone else uses your personal information to impersonate you on any platform to gain benefits in your name, identity theft can cause you to damage more serious than financial losses. The most common reason for identity theft is improper management of sensitive personal data. There are some things to be avoided when dealing with personally identifiable data:

- Never share your Aadhaar/PAN number with anyone whom you do not know/trust.
- Do not post sensitive data on social networking sites.
- Do not make all the personal information on your social media accounts public.
- Please never share an Aadhaar OTP received on your phone with someone over a call.
- Make sure that you do not receive unnecessary OTP SMS about Aadhaar (if you do, your Aadhaar number is already in the wrong hands)
- Do not fill personal data on the website that claim to offer benefits in return.

5. Be careful with links and attachments:
Be careful when clicking on links or attachments in emails, even if they seem to be from a trusted source. It's always best to verify the authenticity of the email and the link or attachment before clicking on them.

6. Take appropriate actions if you have been a Victim:
There are few things that should be done as soon as you realize you have been hacked:

- File a formal complaint with the police and inform the other relevant authorities, Report to www.cybercrime.gov.in or use a toll free number 1930.
- Try regaining access to your compromised accounts by utilizing secondary contacts.
- Reset the password for other accounts and websites that were using the same password as the account that was compromised.

- Perform a factory reset and proper formatting of your devices that are affected (assuming you have your data backed up already).

Cyber Security Tools

Cyber security tools are a set of systems and techniques that protect an organization's networks, applications, code repositories, and other critical systems from known and unknown threats by monitoring, identifying, remediating, and mitigating them.

1.Firewall

Firewalls are security systems within networks that monitor the flow of both incoming and outgoing data. They evaluate the data moving along their borders and use a set of predetermined rules to decide what data can and cannot pass through the barrier.

2. Anti-Malware

It is a type of software-based cyber security tool that prevents malware (malicious software) from infecting a computer and removes existing malware from devices and systems.

4.Anti-Virus
It is another one of the tools for cyber security that is used to prevent and protect our computer systems from computer virus infection. It's generally recommended that everyone install some sort of anti-virus software on their devices to keep dangerous software from infecting it.

4. Penetration Testing Software

It is a cyber security technique that simulates a cyberattack on a system. This may also be known as a pen test or ethical hacking. The test is designed to identify weaknesses within a system and determine the likelihood of a breach.

5.Network Monitoring Software

Through the use of network monitoring software, administrators can determine if a network is running optimally and proactively identify deficiencies. Network monitoring provides a clear picture of all the connected devices on a network, allowing system administrators to see how data is moving between them and quickly correct any flaws that could undermine network performance or lead to outages.

Cyber Ethics

Cyber ethics is a set of morally correct rules. It is also a security protocol that decides a code of behaviour. It must be followed and taken care of while using the online environment. A responsible citizen must follow these rules while using the internet.

Cyber ethics helps to create a safe environment in cyberspace.

Some important Ethics are:

Do not ask for, send, or store any offensive content.

Do not access any network or system without permission.

Do not store any data of users even if it is public.

Do not bully, harass, abuse, or stalk anyone over the internet.

Do not spread computer viruses even if it is for fun.

Do not spam any internet user.

Do not violate copyright laws.

Say no to plagiarism. Watch or listen to any form of media only after lawfully purchasing it.

Legal issues in Cyber Security

Acts related to information technology

The Government has created certain acts to protect against fraud and illegal activities happening in the cyber space.

Cyber Laws of India

Cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

- The Computer as a Target :- using a computer to attack other computers.
  e.g. Hacking,Virus/Worm attacks, DOS attack etc.
- computer as a weapon :- using a computer to commit real world crimes.
  e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Difference between Ethics and law

Ethics	**Laws**
These are unwritten principles.	These are formal, well-documented principles.
These are defined by individuals and may vary depending on personal choice.	These are created by the Government and court.
These cannot be applied to everyone. Most of the time, the ethics of different companies will be different.	Laws are applicable to everyone.

UNIT-5

Emerging Technologies in Artificial Intelligence, Machine Learning, Blockchain, Cryptocurrency and Digital Signature

ARTIFICIAL INTELLIGENCE

Introduction:

- Artificial Intelligence is concerned with the design of intelligence in an artificial device. The term was coined by John McCarthy in 1956.
- Intelligence is the ability to acquire, understand and apply the knowledge to achieve goals in the world.
- AI is the study of the mental faculties through the use of computational models
- AI is the study of intellectual/mental processes as computational processes.
- AI program will demonstrate a high level of intelligence to a degree that equals or exceeds the intelligence required of a human in performing some task.
- AI is unique, sharing borders with Mathematics, Computer Science, Philosophy, Psychology, Biology, Cognitive Science and many others.

History of AI:

- In 1931, Goedellayed the foundation of Theoretical Computer Science**1920-30s**: He published the first universal formal language and showed that math itself is either flawed or allows for unprovable but true statements.
- In 1936, Turing reformulated Goedel's result and church's extension thereof.
- In 1956, John McCarthy coined the term "Artificial Intelligence" as the topic of the **Dartmouth Conference**, the first conference devoted to the subject.
- In 1957, The **General Problem Solver (GPS)** demonstrated by Newell, Shaw & Simon
- In 1958, John McCarthy (MIT) invented the Lisp language.
- In 1959, Arthur Samuel (IBM) wrote the first game-playing program, for checkers, to achieve sufficient skill to challenge a world champion.
- In 1963, Ivan Sutherland's MIT dissertation on Sketchpad introduced the idea of interactive graphics into computing.
- In 1966, Ross Quillian (PhD dissertation, Carnegie Inst. of Technology; now CMU) demonstrated semantic nets
- In 1967, Dendral program (Edward Feigenbaum, Joshua Lederberg, Bruce Buchanan, Georgia Sutherland at Stanford) demonstrated to interpret mass spectra on organic chemical compounds. First successful knowledge-based program for scientific reasoning.
- In 1967, Doug Engelbart invented the mouse at SRI
- In 1968, Marvin Minsky& Seymour PapertpublishPerceptrons, demonstrating limits of simple neural nets.
- In 1972, Prolog developed by Alain Colmerauer.

- In Mid 80's, Neural Networks become widely used with the Backpropagation algorithm (first described by Werbos in 1974).
- In 1990, Major advances in all areas of AI, with significant demonstrations in machine learning, intelligent tutoring, case-based reasoning, multi-agent planning, scheduling, uncertain reasoning, data mining, natural language understanding and translation, visio n, virtual reality, games, and other topics.
- In 1997, Deep Blue beats the World Chess Champion Kasparov
- In 2002, iRobot, founded by researchers at the MIT Artificial Intelligence Lab, introduced **Roomba**, a vacuum cleaning robot. By 2006, two million had been sold.

Examples of AI:

1. Typing using software: While typing reports using any word-processor, wrong spellings or incorrect grammar is highlighted. We also are exposed to auto-complete options of previously used words, or auto-suggest of commonly used words while typing an e-mail, a SMS message or a social-media post.

2. Shopping online: All of us are now used to shopping online. We are either ordering clothes or gadgets online, or using a streaming service (watching movies/shows online). Depending on the user profile, the system shows ads, products or suggests programs to watch.

The software is constantly monitoring what we are watching or searching online. Previous history of browsing is also looked at. Shopping preferences are noted. Then, appropriate suggestions are displayed. All this is happening invisibly or unknown to us.

3. Chat bots: Chat bots are used universally today on many websites to interact with the human users that arrive on the specific sites. They try to provide them effective communication and explain to the users how the company or industry works while providing detailed instructions and guides with spontaneous replies.

Chat bots are usually used for quick responses to most commonly asked questions on a particular website. They save time as well as reduce human labor and expenditure.

Applications of AI

1. Artificial Intelligence in Healthcare

With AI, natural language is a boon. It helps to respond to the questions that are asked for. It enables workflow assistants who screen the patients, getting preliminary information. This in turn helps the doctors to free up their schedules and also reduce the time and cost by streamlining processes.

Thus, these are the following advantages of using AI in healthcare:

1. It helps to support decision making and research.

2. Help to integrate activities in medical, software and cognitive sciences.

3. Help to offer a content-rich discipline for the future scientific medical communities.

2. Artificial Intelligence in Business

A business relies on real-time reporting, accuracy, and processing of large volumes of quantitative data to make crucial decisions. The adaptive intelligence, Chabot and automation helps to smoothen out the business process.

AI is used in online help centers. If you've visited a website, you must have seen that the chat window pops up. You can then ask questions there directly and they revert to your problem or query in no time.

3. Artificial Intelligence in Education

It must be very tedious for a teacher to evaluate homework and tests for large lecture courses. A significant amount of time is consumed to interact with students, to prepare for class, or work on professional development. But, with AI in education, this will not be the case anymore. Though it can never replace human work, it is pretty close to it. So, with the automated grading system checking multiple-choice questions, fill-in-the-blank testing, grading of students can be done in no time.

4. Artificial Intelligence in Autonomous Vehicles

Long-range radar, cameras, and LIDAR, a lot of advancement has been made in the autonomous vehicle segment. These technologies are used in different capacities and each of them collects different pieces of information. The information is of no use unless it is processed and any form of insights can't be derived.

This is where artificial intelligence is used and where it can be compared to the human brain. Some of their usage in autonomous vehicles is:

• Directing the car to the fuel station or recharge station when it is running low on fuel.

• Adjust the trip's directions based on known traffic conditions to find the quickest route.

• Incorporate speech recognition for advanced communication with passengers.

• Natural language interfaces and virtual assistance technologies.

5. Artificial Intelligence in Social Media

Instagram, Snapchat, Facebook, Twitter, the world today is changing and everyone is using these social media apps to stay connected with the virtual world. But, are you aware of the fact that a majority of your decisions are being influenced by artificial intelligence?

Starting from notifications, to upgradations, everything is managed by AI. It considers all the past web searches, behaviours, interactions, and much more. So, while you visit these websites, your data is being stored and analyzed and thus you are served with a personalized experience.

6. Artificial Intelligence for a Better World

Many people say that technology is snatching away their jobs and with the machine, there is no need for humans. But, do you know that it is these machines that are making the world a better place to live in.

7. Artificial Intelligence in Tourism

Competition in the travel and tourism industry is very high. You must have seen that prices keep on fluctuating and change often.

MACHINE LEARNING

Introduction:

Machine learning is simply a way of achieving AI. Machine learning is a way of "training" an algorithm so that it can learn how. "Training" involves feeding huge amounts of data to the algorithm and allowing the algorithm to adjust itself and improve.

For example, the humans might tag pictures that have a cat in them versus those that do not. Then, the algorithm tries to build a model that can accurately tag a picture as containing a cat or not as well as a human. Once the accuracy level is high enough, the machine has now "learned" what a cat looks like.

Machine Learning Methods:

Supervised Learning:

Supervised learning is commonly used in applications where historical data predicts likely future events. For example, it can anticipate when credit card transactions are likely to be fraudulent or which insurance customer is likely to file a claim.

The most common fields of use for supervised learning are price prediction and trend forecasting in sales, retail commerce, and stock trading. In both cases, an algorithm uses incoming data to assess the possibility and calculate possible outcomes.

Unsupervised Learning:

Unsupervised learning works well on transactional data. For example, it can identify segments of customers with similar attributes who can then be treated similarly in marketing campaigns. Or it can find the main attributes that separate customer segments from each other.

Digital marketing and ad tech are the fields where unsupervised learning is used to its maximum effect. In addition to that, this algorithm is often applied to explore customer information and adjust the service accordingly.

Semi-supervised Learning:

Semi-supervised learning is useful when the cost is too high to allow for a fully supervised process. Examples of this include identifying a person's face on a web cam.

Legal and Healthcare industries, among others, manage web content classification, image, and speech analysis with the help of semi-supervised learning.

Reinforcement Learning:

This is often used for robotics, gaming and navigation. With reinforcement learning, the system discovers through trial and error which actions yield the greatest rewards.

Modern NPCs (non-playing characters) and other video games use this type of machine learning model a lot. Reinforcement Learning provides flexibility to the AI reactions to the player's action

Who uses Machine Learning?

Financial Services:

Banks and other businesses in the financial industry use machine learning technology for two key purposes: to identify important insights in data, and prevent fraud. The insights can identify investment opportunities, or help investors know when to trade. Data mining can also identify clients with high-risk profiles, or use cyber-surveillance to pinpoint warning signs of fraud.

Government Agencies:

Government agencies such as public safety and utilities have a particular need for machine learning since they have multiple sources of data that can be mined for insights. Analyzing sensor data, for example, identifies ways to increase efficiency and save money. Machine learning can also help detect fraud and minimize identity theft.

Healthcare:

Machine learning is a fast-growing trend in the health care industry, thanks to the advent of wearable devices and sensors that can use data to assess a patient's health in real time. The technology can also help medical experts analyze data to identify trends or red flags that may lead to improved diagnoses and treatment.

Retail:

Websites recommending items you might like based on previous purchases are using machine learning to analyze your buying history. Retailers rely on machine learning to capture data, analyze it and use it to personalize a shopping experience, implement a marketing campaign, price optimization, merchandise supply planning, and for customer insights.

Oil and Gas:

Finding new energy sources. Analyzing minerals in the ground. Predicting refinery sensor failure. Streamlining oil distribution to make it more efficient and cost-effective. The number of machine learning use cases for this industry is vast – and still expanding.

BLOCK CHAIN

Introduction:

Blockchain is an emerging technology that will change the way we acquire and share information. It is an online global database that anyone, anywhere at any time, with an internet connection, can use.

The Block chain is defined as the decentralized and distributed ledger technology that provides information to be recorded, maintained and shared by a community.

The name of blockchain came from its structure, i.e. block and chain; individual records, called blocks, are linked together in a series to form the chain. A Blockchain is a Network Protocol like SMTP.

Block chain builds trust through the following **five attributes**:

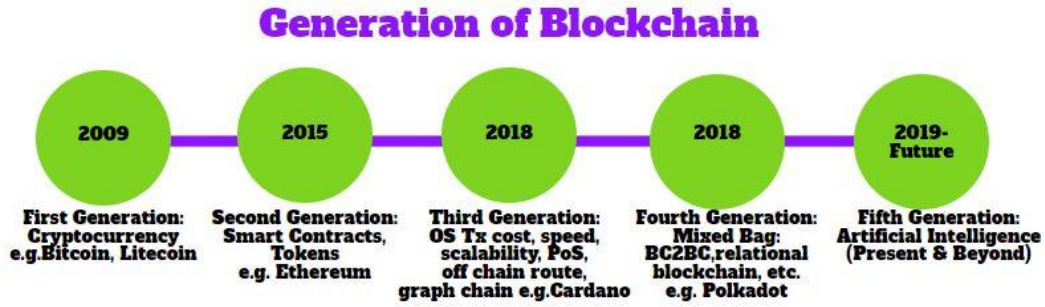
Distributed: The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real-time as there is no central server controlling the data.

Secure: There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.

Transparent: Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.

Consensus-based: All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.

Flexible: Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.



Characteristics:

- **Open**: Anyone can access blockchain.
- **Distributed or Decentralized:** Not under the control of any single authority.
- **Efficient:** Fast and Scalable.
- **Verifiable:** Everyone can check the validity of information because each node maintains a copy of the transactions.
- **Permanent:** Once a transaction is done, it is persistent and can't be altered.

Types of Blockchain

Blockchain can be classified into the following three major types.

1. Public Blockchain
2. Private Blockchain
3. Consortium Blockchain or Hybrid Blockchain

Public Blockchain:

- A public blockchain is one in which anyone can join and participate.
- It meansanyone can be a user or a miner, and anybody can add new blocks.
- It ensurestransparency in public blockchain networks.
- A public blockchain is also called permission less as it permits anyone to take a copy of the blockchain and involve inblock validation.
- Bit coin and Ethereum are examples of a public blockchain.

Private Blockchain:

- A private blockchain is a permissioned blockchain suitable for individualorganizations.
- Here an organization decides who is allowed to participate andmaintain a shared ledger.
- Hyperledger is an example of a private blockchain.

Consortium Blockchain or Hybrid Blockchain:

- A consortium blockchain is a permissioned blockchain where several organizations take responsibility for maintaining the blockchain.
- Consortium blockchain has the privacy benefits of private blockchain and the transparent nature of public blockchain.
- A consortium blockchain is also called a hybrid blockchain.
- Dragon chain is an example of consortium blockchain.

Features of the above three blockchain types are as shown in Table:

	Public	Consortium	Private
Participants	Without permission • Anonymous • Could be malicious	Permissioned • Identified • Trusted	Permissioned • Identified •Trusted
Consensus mechanisms	Proof of work, proof of stake, etc. • Large energy consumption • No finality • 51% attack	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality
Transaction approval freq.	Long Bitcoin: 10 min or more	Short 100× ms	Short 100× ms

Advantages of Blockchain Technology

- Decentralization
- Transparent and Anonymous
- Less transaction fees and no taxes
- Theft resistant

Applications of Blockchain Technology

Financial Application

Banks and other financial institutions are highly susceptible to money laundering, identity theft and digital transfer of funds.

Blockchain Applications in Government

Governments can use Blockchain in the following areas:

- Record management for secure record-keeping of people
- Identity management for proof of identity
- Government services like public safety and welfare
- Payment infrastructures to collect dues, taxes and other payments fast and safe
- Smart property to digitally record assets

Blockchain Applications in Healthcare

Blockchain technology provides data security and integrity. Patients, healthcare providers (hospitals, doctors, lab technicians etc.), data analysts and insurance providers are key stakeholders of healthcare.

The Distributed Ledger Technology/Blockchain technology in healthcare guarantees the security and privacy of healthcare data of all stakeholders. These stakeholders can share information without compromising data security and integrity.

Blockchain Applications in Industry:

Blockchain technology can help in tracking the movements of goods and services efficiently. Almost all business operations, be it purchase management, customer relationship management, supply chain management or operation management, blockchain technology is there to addressbusiness concerns.

Blockchain Application in the Internet of Things (IoT)

In IoT applications, smart devices interact with each other using the internet. Thebiggest concern is the security of data generated by these smart devices within distributed nature of wireless networks.

CRYPTOCURRENCY

Introduction:

- A crypto currency or crypto is a virtual currency secured by cryptography. It is designed to work as a medium of exchange, where individual ownership records are stored in a computerized database.
- It is a **decentralized currency**, meaning it is not controlled by any **government or institution.**
- It is a coded string of data representing a currency unit.
- Peer-to-peer networks called blockchains monitor and organize cryptocurrency transactions, such as buying, selling, and transferring, and also serve as secure ledgers of transactions.

Legal Status of Cryptocurrency:

In India:

- The **legal status of cryptocurrency** in India is currently in a **state of flux.**
- The **Reserve Bank of India (RBI)** has issued several warnings against the use of **cryptocurrencies,** stating that they pose risks to investors and are **not legal tender.**
- **In 2018** the **Supreme Court struck down** a circular of **Reserve Bank of India,** which **bans financial institutions** from dealing in **digital or cryptocurrencies.**
- In **2022**, the **Government of India** mentioned in the **Union budget 2022-23** that-the transfer of any **virtual currency/cryptocurrency** asset will be subject to **30% tax deduction.**
- **The Govt.** has also set up a panel to explore the **potential use of blockchain technology** and the possibility of issuing a **Central Bank Digital Currency (CBDC).**

Elsewhere:

- At present, **El Salvador** and the **Central African Republic (CAR)** are the **only two countries** in the world where **Bitcoin** functions as a **legal currency.**
- However, many countries have taken steps to **recognize and regulate** the use of certain **cryptocurrencies**, such as **Bitcoin.**

- Some countries, such as **Japan** and **South Korea**, have issued regulations for **cryptocurrency exchanges.**
- Nations like **Germany** and **Switzerland,** have recognized **Bitcoin** as a **"legal means of payment."**

- Other countries, such as **China** and **Russia,** have taken a more cautious approach and have **imposed restrictions** on the use of **cryptocurrencies.**

Examples:

1. **Bitcoin:** Bitcoin is the most widely accepted cryptocurrency. Founded in 2009 by Satoshi Nakamoto, it is still the most commonly traded. It is a decentralized digital currency that can be transferred on a peer-to-peer Bitcoin network.
2. **Ether:** Ether is the native cryptocurrency of the Ethereum blockchain network. Each Ethereum account has an ETH balance and may send ETH to any other account. The smallest subunit of Ether is known as Wei.
3. **Litecoin:** Litecoin is a peer-to-peer cryptocurrency and in technical terms, Litecoin is nearly identical to Bitcoin. It uses a script in its proof-of-work algorithm. It is an adaptation of Bitcoin that is intended to make payment easier.
4. **Stablecoins:** These are the class of cryptocurrencies whose values are designed to stay stable relative to real-world assets like the U.S. Dollar.
5. **Solana:** Solana is a competitor of Ethereum whose main emphasis is on speed and cost- effectiveness.

Features:

- **Decentralization:** Cryptocurrencies are decentralized, meaning they operate on a peer-to-peer network and are not controlled by a central authority or government.
- **Security:** Cryptocurrencies use cryptographic techniques to ensure the security and integrity of transactions and to protect against fraud and hacking.
- **Transparency:** Most cryptocurrencies operate on a public ledger called a blockchain, which allows anyone to see all transactions that have occurred on the network.
- **Anonymity:** While most cryptocurrencies are not completely anonymous, they do offer a high degree of privacy and can allow users to transact without revealing their identity.
- **Limited Supply:** Cryptocurrencies are designed with a limited supply to maintain their value and prevent inflation.
- **Global Accessibility:** Cryptocurrencies can be accessed and used from anywhere in the world, as long as there is an internet connection.

Challenges:

- **Volatility:** Cryptocurrency prices are highly volatile, which makes it difficult for businesses to accept it as a form of payment.
- **Regulation:** There is a lack of clear regulation around cryptocurrency, which makes it difficult for businesses and individuals to know how to legally use it.
- **Security:** Cryptocurrency exchanges and wallets are susceptible to hacking attacks, which can result in the loss of funds.

- **Adoption:** Despite its growing popularity, cryptocurrency still has low adoption rates, which makes it difficult for individuals to use it as a form of payment in everyday life.
- **Scalability:** The scalability of cryptocurrencies is limited, which makes it difficult for the technology to handle a large number of transactions.
- **Energy consumption:** The process of verifying transactions in a cryptocurrency network, known as mining, is energy-intensive, and contributes to climate change.

How Does Cryptocurrency Work?

Cryptocurrencies are not regulated or controlled by any central authority hence cryptocurrency works outside the banking system using different types of coins.

1. Mining: Cryptocurrencies are generated through a process called Mining. In this process, the miners are required to solve a mathematical puzzle over a specially equipped computer system to be rewarded with bitcoins in exchange.
2. Buying, selling, and storing: Users can buy cryptocurrencies from central exchanges, brokers, or individual currency owners and sell crypto to them. Cryptocurrencies can be stored in wallets.
3. Investing: Cryptocurrencies can be transferred from one digital wallet to another. Cryptocurrencies can be used for the following purposes:

- Buying goods and services.
- Trade-in them.
- Exchange them for cash.

How To Buy Cryptocurrency?

There are **three** steps involved in buying a cryptocurrency:
1. Choosing a platform: There are two platforms available to choose from:

- **Traditional Brokers:** There are online brokers who offer to buy and sell cryptocurrencies along with stocks, bonds, etc, but they offer lower trading costs and fewer crypto features.
- **Cryptocurrency exchanges:** Different types of cryptocurrency exchanges are available to choose from with different cryptocurrencies, wallet storage, etc.

2. Funding your account: After choosing the platform, the next step is to fund the account. Most crypto exchanges allow users to purchase cryptocurrencies using fiat currency like U.S. Dollar, or the Euro, or using Credit and Debit cards, but this varies from platform to platform. An important factor to consider here is the fees that include the potential deposit and withdrawal transaction fees plus the trading fees.
3. Placing an order: The order can be placed via exchanges or broker's web or mobile platform.

- Select the Buy option.
- Choose the order type.
- Enter the number of cryptocurrencies.
- Confirm the order.

Advantages of Cryptocurrencies

1. **Private and Secure: Blockchain** technology ensures user anonymity and at the same time the use of cryptography in blockchain makes the network secure for working with cryptocurrencies.

2. **Decentralized, Immutable, and Transparent:** The entire blockchain network works on the principle of shared ownership where there is no single regulating authority and the data is available to all the permissioned members on the network and is tamper-proof.
3. **Inflation Hedge:** Cryptocurrencies are a good means of investing in times of inflation as they are limited in supply and there is a cap on mining any type of cryptocurrency.
4. **Faster Settlement:** Payments for most cryptocurrencies settle in seconds or minutes. Wire transfers at banks can cost more and often take three to five business days to settle.
5. **Easy Transactions:** Crypto transactions can be done more easily, in a private manner in comparison to bank transactions. using a simple smartphone and a cryptocurrency wallet, anyone can send or receive a variety of cryptocurrencies.

Disadvantages of Cryptocurrencies:

1. **Cybersecurity issues:** Cryptocurrencies will be subject to cybersecurity breaches and may fall into the hands of hackers. Mitigating this will require continuous maintenance of security infrastructure.
2. **Price Volatility:** Cryptocurrencies are highly volatile in terms of price as they have no underlying value and there is a supply-demand-like equation that is used to determine the price of cryptocurrencies.
3. **Scalability:** Scalability is one of the major concerns with cryptocurrencies. Digital coins and tokens adoption is increasing rapidly but owing to the sluggish nature of the blockchain makes cryptocurrencies prone to transaction delays. Cryptocurrencies cannot compete with the number of transactions that payment giants like VISA, and MasterCard process in a day.
4. **Less awareness:** Cryptocurrency is still a new concept for the people and the long-term sustainability of cryptocurrencies remains to be seen.

DIGITAL SIGNATURE

Introduction:

- A **digital signature** is a mathematical scheme that is used to verify the integrity and authenticity of digital messages and documents.
- It may be considered as a digital version of the handwritten signature or stamped seal.
- The digital signatures use asymmetric cryptography i.e. also known as public key cryptography.
- **Asymmetric key cryptography** also known as public key cryptography uses public and private keys to encrypt and decrypt data.
    1. The public key can be shared with anyone.
    2. The private key is the secret key that is kept a secret.

Whyare Digital Signature Important?

Digital signatures are important to achieve three results:

1. **Data Integrity:** It is preserved by using the hash function in signing and verifying algorithms. Any change in the message will produce a completely different signature. This way Bob can verify that the message sent by Alice was not modified along its way.

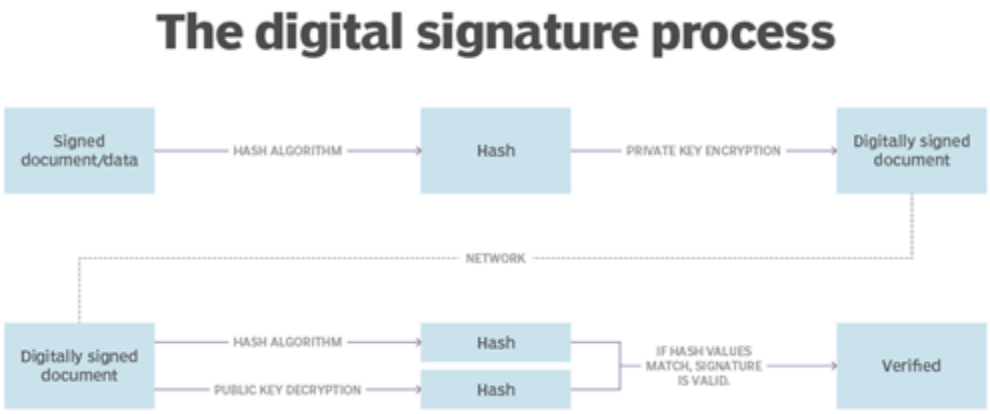
2. **Authenticity:** The message is verified using the public key of the sender. When Alice sends a message to Bob. Bob uses the public key of Alice for verification and Alice's public key cannot create the same signature as Kev's private key.

3. **Message Nonrepudiation:** Once the signature is generated, Alice cannot deny having signed it in the future, unless Alice's private key is compromised.

How do Digital Signatures Work?

1. **Signing the message with the private key:** Digital signature is created using signing software that creates a one-way hash function of the data to be signed. The private key of the sender is used to encrypt the hash value generated. The encrypted hash value along with the hash algorithm constitutes the digital signature. The sender will now send the message along with the encrypted hash value to the receiver. The receiver can only decrypt the hash value using the sender's public key.

2. **Verifying the message with the public key:** At the receiver end, there are two steps, to generate the hash of the message and decryption of the signature. By using the sender's public key, the signature can be decrypted. If the decrypted hash matches the second computed hash value then it proves that the message hasn't been changed since it was signed. If the two hash values don't match then it means that the message has been tampered with along its way.



Classes and types of digital signatures:

There are three different classes of digital signature certificates (DSCs) as follows:

- **Class 1.** This type of DSC can't be used for legal business documents, as they're validated based only on an email ID and username. Class 1 signatures provide a basic level of security and are used in environments with a low risk of data compromise.
- **Class 2.** These DSCs are often used for electronic filing (e-filing) of tax documents, including income tax returns and goods and services tax returns. Class 2 digital signatures authenticate a signer's identity against a pre-verified database. Class 2 digital signatures are used in environments where the risks and consequences of data compromise are moderate.
- **Class 3.** The highest level of digital signatures, Class 3 signatures require people or organizations to present in front of a CA to prove their identity before signing. Class 3 digital signatures are used for e-auctions, e-

tendering, e-ticketing and court filings, as well as in other environments where threats to data or the consequences of a security failure are high.

Applications of Digital Signatures

- **Healthcare:** Digital signatures are used in healthcare to improve the efficiency of administrative and treatment processes to strengthen data security. For example, for prescribing medicines and admissions to hospitals. They can be used to prevent fraudulent prescriptions and medical records.
- **Legal:** Digital signatures can be used to reduce the time to close contracts that require multiple parties to validate and sign them. Due to the immutable nature of the blockchain, the contract validity can be trusted thus allowing parties to sign the contract at their convenience.
- **Government:** Digital signatures are used by the government worldwide for a variety of reasons like processing tax returns, managing contracts, verifying B2G transactions, etc.
- **Financial services:** Digital signatures can be used in expense reports, audits, loan agreements, etc.
- **Manufacturing:** Digital signatures are used in the manufacturing industry to speed up processes like product design, quality assurance, and marketing sales. The use of digital signatures in Manufacturing is governed by organizations like ISO, NIST, and DMC.
- **Cryptocurrencies:** Digital signatures are used in cryptocurrencies to authenticate the blockchain, and manage transaction data associated with the cryptocurrency.
- **Software programs:** Digital signatures are used in software programs like browsers where a secure connection needs to be established over insecure internet.
- **B2B communications and transactions:** Digital signatures can be used to validate the source of the transaction and can only be sent to only intended party without any middlemen.

Benefits of Digital Signatures:

- **Increase security:** Digital signatures are based on the PKI technology through which the signature becomes part of the message and cannot be modified and removed. When a digital signature is created the time and IP location of the user get recorded in the audit trail embedded within the message.
- **Time-saving:** Digital signatures simplify the time-consuming process of paper-based transactions with manual tasks like drafting, printing, signing, scanning, and mailing. Digital signing helps to automate the manual work and reduce the long wait to few hours.
- **Time stamping:** Time stamping is important when timing is critical. Providing date and time of a digital signature helps in time critical jobs like stock trading, legal; proceedings, etc.
- **Cost savings:** By going paperless with the use of digital signature, organizations can save money that was previously being spent on the physical resources like paper, office space, manpower hat are used to manage them.
- **Workflow automation:** Paper process requires annual tracking, accuracy, and coordination when the documents need to be signed in the particular order and at the same time the data confidentiality needs to be protected. There are more chances of error, delays, mistakes but these can be cut out when using a digital tool that makes the workflow standardized, consistent, and error-free.
- **Traceability:** Digital signatures create an audit trail that makes internal record-keeping easier. There are very minor chances of mistake when everything is recorded digitally.
- **Legally compliant:** Digital signatures are enforceable in every developed country worldwide. Digital signatures are generally considered the most secure type of e-signatures and can be used to sign most documents.
- **Satisfied end-user:** Users can sign from any device, from anywhere and at their own pace without physically visiting a branch, office, or store.

Limitations of Digital Signature:

- **Theft of keys:** Lost or theft of keys is one of the major drawbacks of digital signatures. The use of vulnerable storage facilities is one of the other limitations.
- **Additional cost:** To effectively use digital signatures sender and receiver needs to buy digital certificates and verification software at a cost.
- **Need for standard:** There is a strong need for a standard through which these different methods can interact.