What is a Computer Network?

A computer network is a system that connects many independent computers to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily. A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

Uses of Computer Networks

- Communicating using email, video, instant messaging, etc.
- Sharing devices such as printers, scanners, etc.
- Sharing files.
- Sharing software and operating programs on remote systems.
- Allowing network users to easily access and maintain information.

Types of Computer Networks

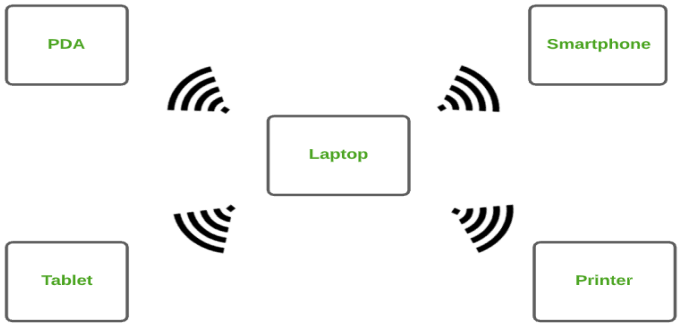
There are mainly five types of Computer Networks

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Campus Area Network (CAN)
4. Metropolitan Area Network (MAN)
5. Wide Area Network (WAN)

Types of Computer Networks

1. Personal Area Network (PAN)

PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. This uses Bluetooth**,** IrDA**,** and Zigbee as technology. Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.



Personal Area Network (PAN)

Types of PAN

- **Wireless Personal Area Networks:** Wireless Personal Area Networks are created by simply utilising wireless technologies such as WiFi and Bluetooth. It is a low-range network.

- **Wired Personal Area Network:** A wired personal area network is constructed using a USB.

Advantages of PAN

- PAN is relatively flexible and provides high efficiency for short network ranges.
- It needs easy setup and relatively low cost.
- It does not require frequent installations and maintenance
- It is easy and portable.
- Needs fewer technical skills to use.

Disadvantages of PAN

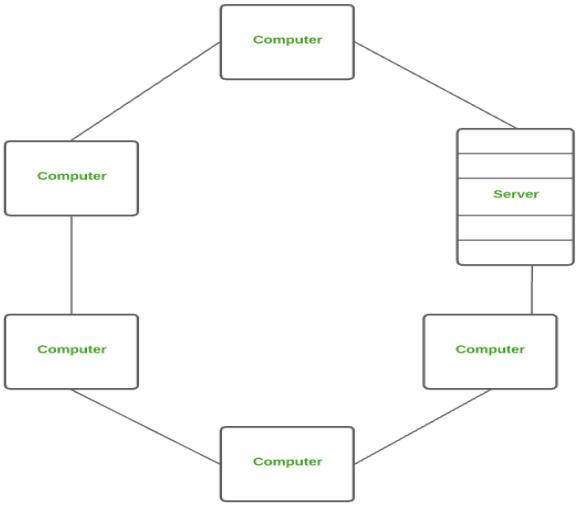
- Low network coverage area/range.
- Limited to relatively low data rates.
- Devices are not compatible with each other.
- Inbuilt WPAN devices are a little bit costly.

Applications of PAN

- Home and Offices
- Organizations and the Business sector
- Medical and Hospital
- School and College Education
- Military and Defense

2. Local Area Network (LAN)

LAN is the most frequently used network. A LAN is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



Local Area Network (LAN)

Advantages of a LAN

- **Privacy:** LAN is a private network, thus no outside regulatory body controls it, giving it a privacy.
- **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
- **Supports different transmission mediums:** LAN support a variety of communications transmission medium such as an Ethernet cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.
- **Inexpensive and Simple:** A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

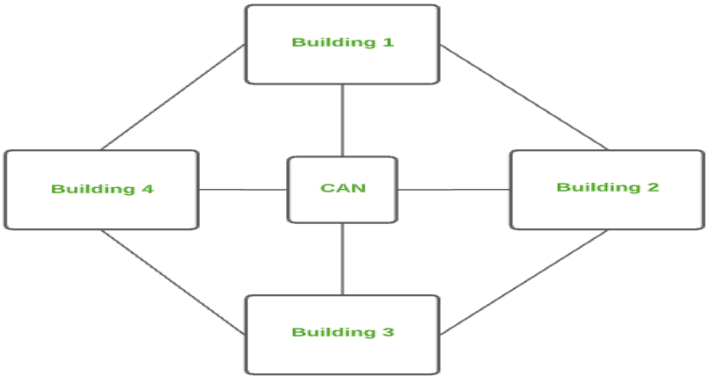
Disadvantages of LAN

- The initial setup costs of installing Local Area Networks is high because there is special software required to make a server.
- Communication devices like an ethernet cable, switches, hubs, routers, cables are costly.
- LAN administrator can see and check personal data files as well as Internet history of each and every LAN user. Hence, the privacy of the users are violated
- LANs are restricted in size and cover only a limited area

- Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, can cause a serious data security threat.

3. Campus Area Network (CAN)

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range from 1km to 5km. Its transmission speed is very high with a moderate maintenance cost and moderate cost. Examples of CAN are networks that cover schools, colleges, buildings, etc.



Campus Area Network (CAN)

Advantages of CAN

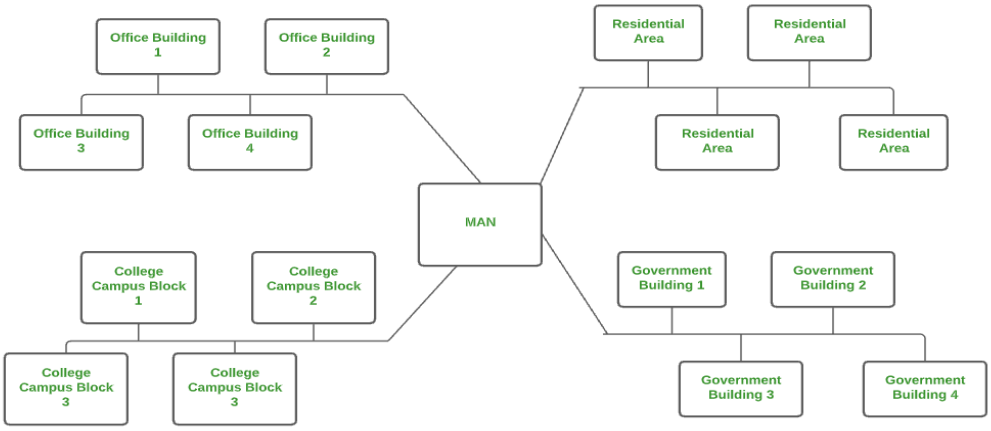
- **Speed:** Communication within a CAN takes place over Local Area Network (LAN) so data transfer rate between systems is little bit fast than Internet.

- **Security:** Network administrators of campus take care of network by continuous monitoring, tracking and limiting access. To protect network from unauthorized access firewall is placed between network and internet.

- **Cost effective:** With a little effort and maintenance, network works well by providing fast data transfer rate with multi-departmental network access. It can be enabled wirelessly, where wiring and cabling costs can be managed. So to work with in a campus using CAN is cost-effective in view of performance

4. Metropolitan Area Network (MAN)

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.



Metropolitan Area Network (MAN)

Advantages of MAN

- MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
- The security level in MAN is high and strict as compared to WAN.
- It support to transmit data in both directions concurrently because of dual bus architecture.
- MAN can serve multiple users at a time with the same high-speed internet to all the users.
- MAN allows for centralized management and control of the network, making it easier to monitor and manage network resources and security.

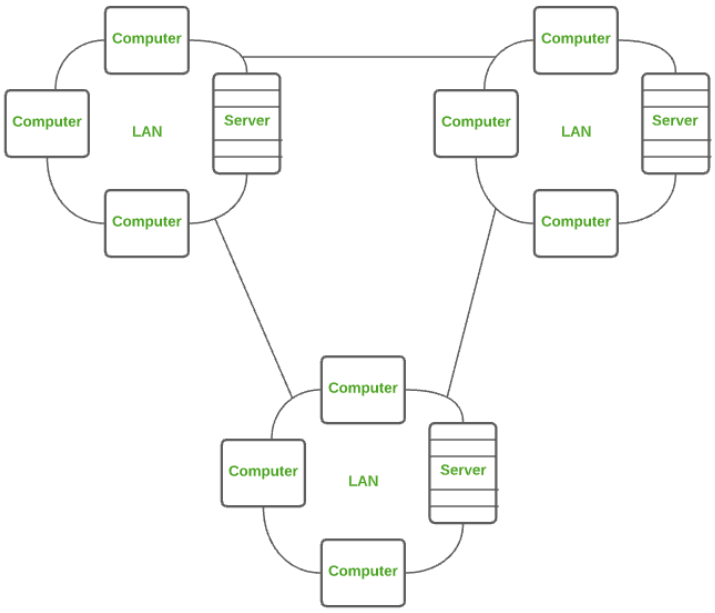
Disadvantages of MAN

- The architecture of MAN is quite complicated hence, it is hard to design and maintain.
- This network is highly expensive because it required the high cost to set up fiber optics.
- It provides less fault tolerance.

- The Data transfer rate in MAN is low when compare to LANs.

5. Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.



Wide Area Network (WAN)

Advantages of WAN

- It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.

- The data can be stored in centralised manner because of remote access to data provided by WAN.

- The travel charges that are needed to cover the geographical area of work can be minimised.
- WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

Disadvantages of WAN

- Traffic congestion in Wide Area Network is very high.
- The fault tolerance ability of WAN is very less.
- Noise and error are present in large amount due to multiple connection point.
- The data transfer rate is slow in comparison to LAN because of large distances and high number of connected system within the network.

Common Types of Networking Devices and Their Uses

Network devices work as a mediator between two devices for transmission of data, and thus play a very important role in the functioning of a computer network. Below are some common network devices used in modern networks:

- Access Point
- Modems
- Firewalls
- Repeater
- Hub
- Bridge
- Switch
- Routers
- Gateway
- Brouter

- NIC

Access Point

An access point in networking is a device that allows wireless devices, like smartphones and laptops, to connect to a wired network. It creates a Wi-Fi network that lets wireless devices communicate with the internet or other devices on the network. Access points are used to extend the range of a network or provide Wi-Fi in areas that do not have it. They are commonly found in homes, offices, and public places to provide wireless internet access.

Modems

Modems is also known as modulator/demodulator is a network device that is used to convert digital signal into analog signal of different frequencies and transmits these signal to a modem at the receiving location. These converted signals can be transmitted over the cable systems, telephone lines, and other communication mediums. A modem is also used to convert analog signal back into digital signal. Modems are generally used to access internet by customers of an Internet Service Provider (ISP).

Types of Modems

There are four main types of modems:

- **DSL Modem**: Uses regular phone lines to connect to the internet but it is slower compared to other types.
- **Cable Modem**: Sends data through TV cables, providing faster internet than DSL.
- **Wireless Modem**: Connects devices to the internet using Wi-Fi relying on nearby Wi-Fi signals.
- **Cellular Modem**: Connects to the internet using mobile data from a cellular network not Wi-Fi or fixed cables.

Firewalls

A firewall is a network security device that monitors and controls the flow of data between your computer or network and the internet. It acts as a barrier, blocking unauthorized access while allowing trusted data to pass through. Firewalls help protect your network from hackers, viruses, and other online threats by filtering traffic based on security rules. Firewalls can be physical devices (hardware), programs (software), or even cloud-based services, which can be offered as SaaS, through public clouds, or private virtual clouds.

Repeater

A repeater operates at the physical layer. Its main function is to amplify (i.e., regenerate) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Hub

A hub is a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

- **Passive Hub:** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

- **Intelligent Hub:** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Bridge

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It typically connects multiple network segments and each port is connected to different segment. A bridge is not strictly limited to two ports, it can have multiple ports to connect and manage multiple network segments. Modern multi-port bridges are often called Layer 2 switches because they perform similar functions.

Types of Bridges

- **Transparent Bridges:** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

- **Source Routing Bridges:** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Switch

A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Types of Switch

- **Unmanaged Switches:** These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.

- **Managed Switches:** These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.

- **Smart Switches:** These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.

- **Layer 2 Switches:** These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.

- **Layer 3 switches:** These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.

- **PoE Switches**: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
- **Gigabit switches:** These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
- **Rack-Mounted Switches:** These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
- **Desktop Switches:** These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
- **Modular Switches**: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

Router

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

Gateway

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers.

Brouter

It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.

NIC

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

What is an IP Address?

Imagine every device on the internet as a house. For you to send a letter to a friend living in one of these houses, you need their home address. In the digital world, this home address is what we call an **IP (Internet Protocol) Address**. It's a unique string of numbers separated by periods (IPv4) or colons (IPv6) that identifies each device connected to the internet or a local network.

Here's the definition:

What is an IP Address?

An IP address, or Internet Protocol address, is a unique string of numbers assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as an identifier that allows devices to send and receive data over the network, ensuring that this data reaches the correct destination.

Types of IP Address

IP addresses can be classified in several ways based on their structure, purpose, and the type of network they are used in. Here's a breakdown of the different classifications of IP addresses:

1. Based on Addressing Scheme (IPv4 vs. IPv6)

IPv4:

This is the most common form of IP Address. It consists of four sets of numbers separated by dots. For example, 192.158.1.38. Each set of numbers can range from 0 to 255. This format can support over 4 billion unique addresses. Here's how the structure is broken down:

- **Four Octets**: Each octet represents eight bits, or a byte, and can take a value from 0 to 255. This range is derived from the possible combinations of eight bits (2^8 = 256 combinations).

- **Example of IPv4 Address**: 192.168.1.1
  - **192** is the first octet
  - **168** is the second octet
  - **1** is the third octet
  - **1** is the fourth octet

Each part of the IP address can indicate various aspects of the network configuration, from the network itself to the specific device within that network. In most cases, the network part of the

address is represented by the first one to three octets, while the remaining section identifies the host (device).

IPv4 Address Format

IPv6:

IPv6 addresses were created to deal with the shortage of IPv4 addresses. They use 128 bits instead of 32, offering a vastly greater number of possible addresses. These addresses are expressed as eight groups of four hexadecimal digits, each group representing 16 bits. The groups are separated by colons.

- **Example of IPv6 Address**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
    - Each group (like **2001**, **0db8**, **85a3**, etc.) represents a 16-bit block of the address.

For detailed information, refer to this article – **IPv4 vs. IPv6**

2. Based on Usage (Public vs. Private)

Public IP Addresses

A Public IP address is assigned to every device that directly accesses the internet. This address is unique across the entire internet. Here are the key characteristics and uses of public IP addresses:

- **Uniqueness:** Each public IP address is globally unique. No two devices on the internet can have the same public IP address at the same time.
- **Accessibility:** Devices with a public IP address can be accessed directly from anywhere on the internet, assuming no firewall or security settings block the access.
- **Assigned by ISPs:** Public IP addresses are assigned by Internet Service Providers (ISPs). When you connect to the internet through an ISP, your device or router receives a public IP address.
- **Types:** Public IP addresses can be static (permanently assigned to a device) or dynamic (temporarily assigned and can change over time).

Example Use: Public IP addresses are typically used for servers hosting websites, email servers, or any device that needs to be accessible from the internet. For instance, if you host a website on your own server at home, your ISP must assign a public IP address to your server so users around the world can access your site.

Private IP Addresses

Private IP addresses are used within private networks (such as home networks, office networks, etc.) and are not routable on the internet. This means that devices with private IP addresses

cannot directly communicate with devices on the internet without a translating mechanism like a router performing Network Address Translation (NAT). Key features include:

- **Not globally unique:** Private IP addresses are only required to be unique within their own network. Different private networks can use the same range of IP addresses without conflict.
- **Local communication:** These addresses are used for communication between devices within the same network. They cannot be used to communicate directly with devices on the internet.
- **Defined ranges:** The Internet Assigned Numbers Authority (IANA) has reserved specific IP address ranges for private use:
    - **IPv4:** 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, 192.168.0.0 to 192.168.255.255
    - **IPv6:** Addresses starting with FD or FC

Domain Name System (DNS)

Domain Name System (DNS) is a system that translates human-readable domain names, like www.google.com, into machine-readable IP addresses, such as 142.250.190.14, enabling computers to locate and communicate with each other on the internet. It operates as a distributed database, working through a hierarchical structure of servers.

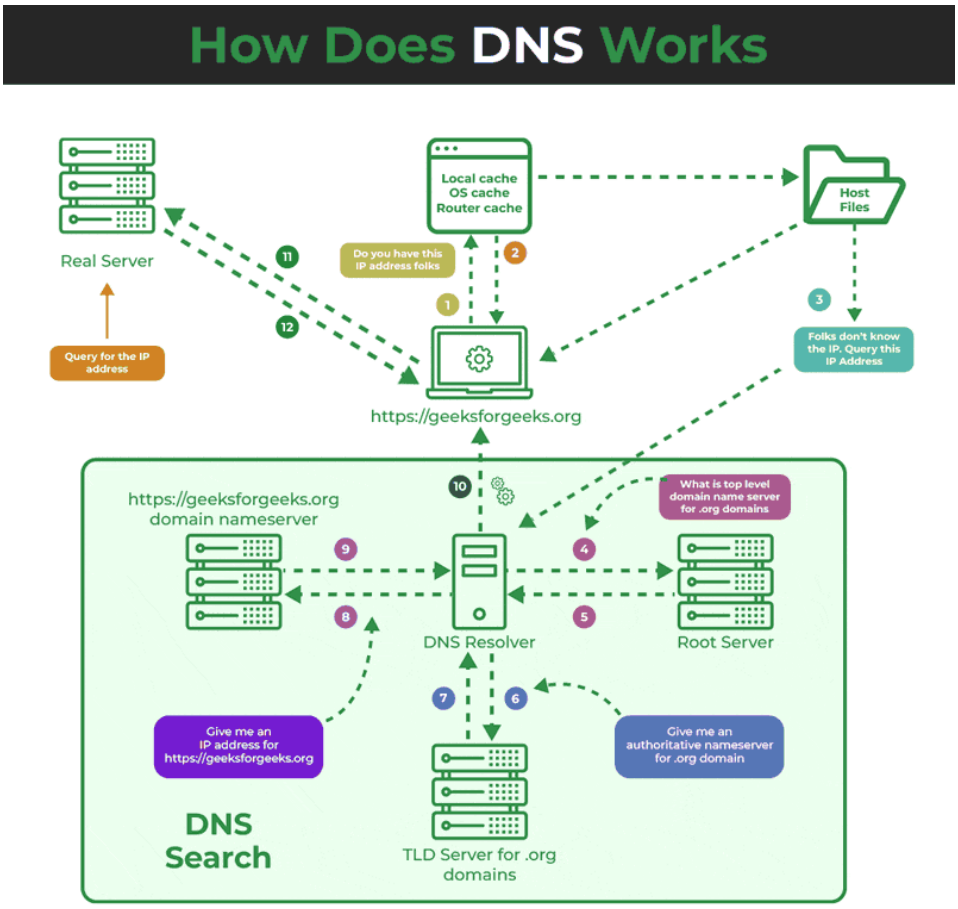
When a user requests a domain, the query passes through multiple levels—starting with the Root server, then the Top-Level Domain (TLD) server and finally the authoritative server that holds the specific IP address for the domain. This seamless process ensures users can access websites using easy-to-remember names instead of numerical IP addresses.

How Does DNS Work?

- When we type a website like https://www.geeksforgeeks.org in our browser, our computer tries to find the IP address.
- First, it checks the local cache (our browser, operating system, or router) to see if it already knows the IP address.
- If the local cache doesn't have the IP, the query is sent to a DNS resolver to find it.

- DNS resolver may check host files (used for specific manual mappings), but usually, it moves on.
- Resolver sends the query to a Root DNS server, which doesn't know the exact IP address but points to the TLD server (e.g., .org server for this example).
- TLD server then directs the resolver to the authoritative nameserver for geeksforgeeks.org.
- Authoritative nameserver knows the exact IP address for geeksforgeeks.org and sends it back to the resolver.
- Resolver passes the IP address to our computer.
- Our computer uses the IP address to connect to the real server where the website is hosted.
- The website loads in our browser.

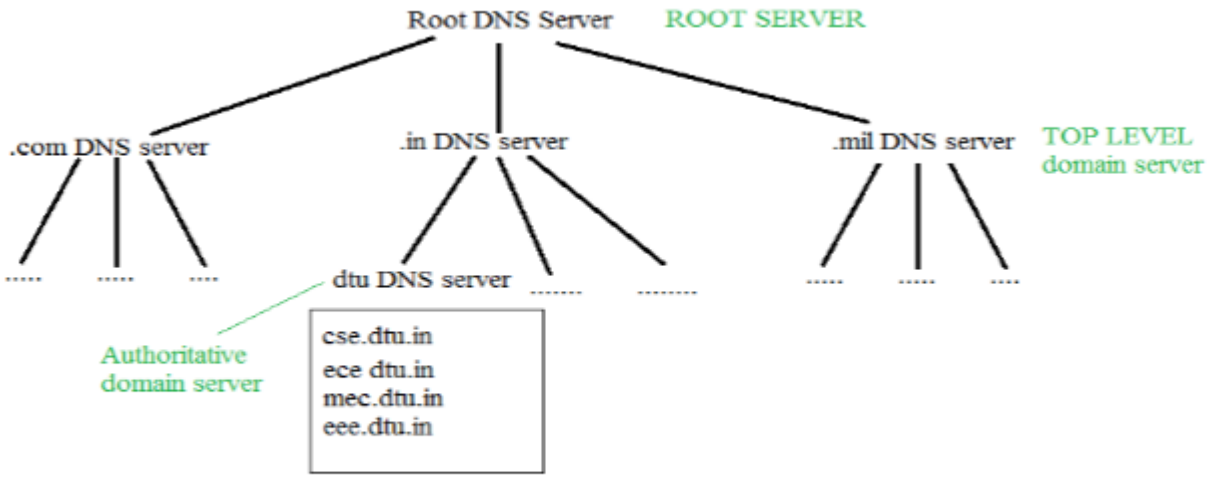
For more, we can refer to [Working of DNS Server]() .



How Does DNS Works?

Structure of DNS

It is very difficult to find out the IP address associated with a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delays for that to happen organization of the database is very important.



Root DNS Server

- **DNS Record:** Domain name, IP address what is the validity? what is the time to live? and all the information related to that domain name. These records are stored in a tree-like structure.
- **Namespace:** Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.
- **Name Server:** It is an implementation of the resolution mechanism.

```
DNS = Name service in Internet – A zone is an administrative unit, and a
domain is a subtree.
```

Types of Domain

There are various kinds of domains:

- **Generic Domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
- **Country Domain:** .in (India) .us .uk
- **Inverse Domain:** if we want to know what is the domain name of the website. IP to domain name mapping. So DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type

Artificial intelligence (AI) refers to computer systems capable of performing complex tasks that historically only a human could do, such as reasoning, making decisions, or solving problems.

- ChatGPT**:** Uses large language models (LLMs) to generate text in response to questions or comments posed to it.
- **Google Translate:** Uses deep learning algorithms to translate text from one language to another.
- **Netflix:** Uses machine learning algorithms to create personalized recommendation engines for users based on their previous viewing history.
- **Tesla:** Uses computer vision to power self-driving features on their cars.

Types of Artificial Intelligence

Artificial Intelligence (AI) has transformed industries, leading to significant advancements in technology, science, and everyday life. To understand AI better, we must first recognize that AI can be categorized into different types based on capabilities and functionalities.

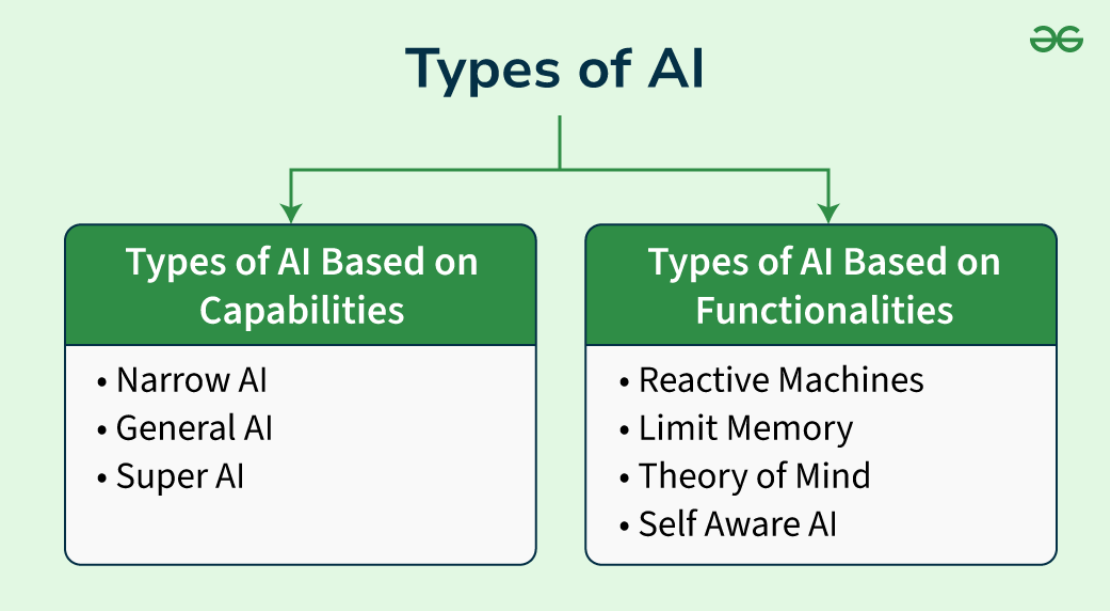
Type 1: Based on Capabilities of AI

- Narrow AI
- General AI
- Super AI

Type 2: Based on the Functionality of AI

- Reactive Machines
- Limited Memory AI

- Theory of Mind
- Self-Aware AI



Types of AI Based on Capabilities

1. Narrow AI (Weak AI)

Narrow AI is designed and trained on a specific task or a narrow range tasks. These Narrow AI systems are designed and trained for a purpose. These Narrow systems performs their designated tasks but mainly lack in the ability to generalize tasks.

Examples:

- Voice assistants like **Siri** or **Alexa** that understand specific commands.
- **Facial recognition** software used in security systems.
- **Recommendation engines** used by platforms like Netflix or Amazon.

Despite being highly efficient at specific tasks, Narrow AI lacks the ability to function beyond its predefined scope. These systems do not possess understanding or awareness.

2. General AI (Strong AI)

General AI refers to AI systems that have human intelligence and abilities to perform various tasks. Systems have capability to understand, learn and apply across a wide range of tasks that are similar to how a human can adapt to various tasks.

While General AI remains a theoretical concept, researchers aim to develop AI systems that can perform any intellectual task a human can. It requires the machine to have consciousness, self-awareness, and the ability to make independent decisions, which is not yet achievable.

Potential Applications:

- Robots that can learn new skills and adapt to unforeseen challenges in real-time.
- AI systems that could autonomously diagnose and solve complex medical issues across various specializations.

3. Superintelligence (Super AI)

Super AI surpasses intelligence of human in solving-problem, creativity, and overall abilities. Super AI develops emotions, desires, need and beliefs of their own. They are able to make decisions of their own and solve problem of its own. Such AI would not only be able to complete tasks better than humans but also understand and interpret emotions and respond in a human-like manner.

While **Super AI** remains speculative, it could revolutionize industries, scientific research, and problem-solving, possibly leading to unprecedented advancements. However, it also raises ethical concerns regarding control and regulation.

Types of Artificial Intelligence Based on Functionalities

AI can also be classified into four types based on how the systems function. This classification is more commonly used to distinguish AI systems in practical applications.

1. Reactive Machines

Reactive machines are the most basic form of AI. They operate purely based on the present data and do not store any previous experiences or learn from past actions. These systems respond to specific inputs with fixed outputs and are unable to adapt.

Examples:

- **IBM's Deep Blue**, which defeated the world chess champion Garry Kasparov in 1997. It could identify the pieces on the board and make predictions but could not store any memories or learn from past games.

- **Google's AlphaGo**, which played the board game Go using a similar approach of pattern recognition without learning from previous games.

2. Limited Memory in AI

Limited Memory AI can learn from past data to improve future responses. Most modern AI applications fall under this category. These systems use historical data to make decisions and predictions but do not have long-term memory. Machine learning models, particularly in autonomous systems and robotics, often rely on limited memory to perform better.

Examples:

- **Self-driving cars**: They observe the road, traffic signs, and movement of nearby cars, and make decisions based on past experiences and current conditions.

- **Chatbots** that can remember recent conversations to improve the flow and relevance of replies.

3. Theory of Mind

Theory of Mind AI aims to understand human emotions, beliefs, intentions, and desires. While this type of AI remains in development, it would allow machines to engage in more sophisticated interactions by perceiving emotions and adjusting behavior accordingly.

Potential Applications:

- **Human-robot interaction** where AI could detect emotions and adjust its responses to empathize with humans.

- **Collaborative robots** that work alongside humans in fields like healthcare, adapting their tasks based on the needs of the patients.

4. Self-Awareness AI

Self-Aware AI is an advanced stage of AI that possesses self-consciousness and awareness. This type of AI would have the ability to not only understand and react to emotions but also have its own consciousness, similar to human awareness.

While we are far from achieving self-aware AI, it remains the ultimate goal for AI development. It opens philosophical debates about consciousness, identity, and the rights of AI systems if they ever reach this level.

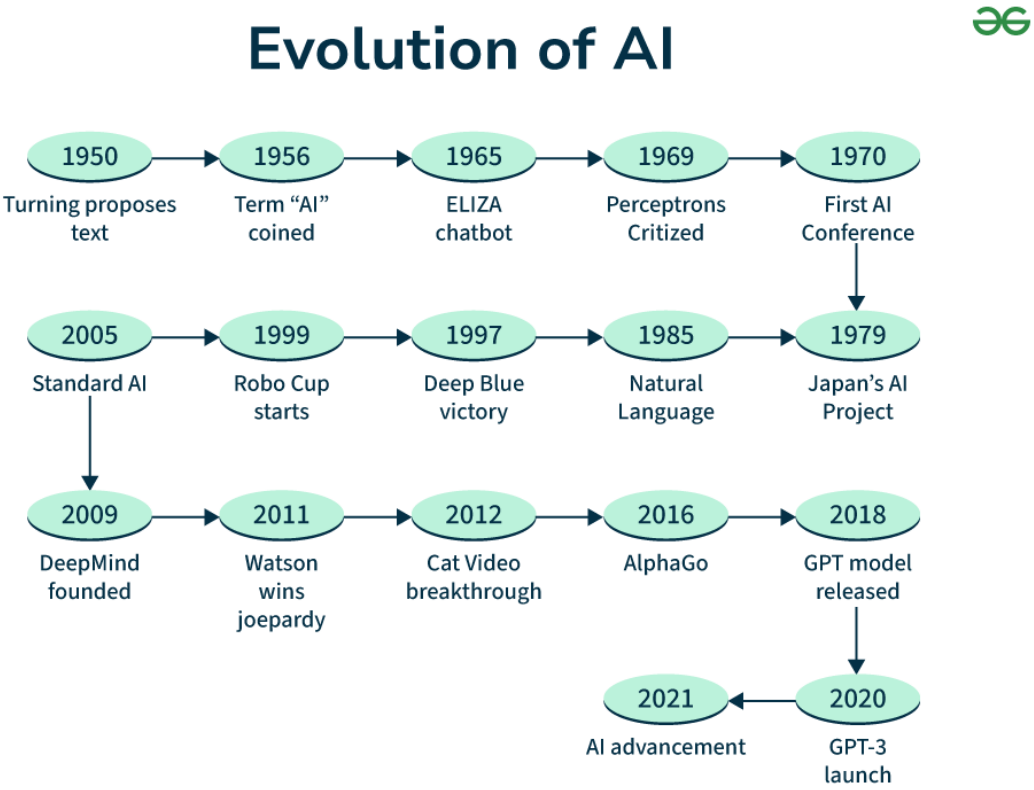
Potential Applications:

- Fully autonomous systems that can make moral and ethical decisions.

- AI systems that can independently pursue goals based on their understanding of the world around them.

History of AI

The term ***Artificial Intelligence (AI)*** is already widely used in everything from smartphones to self-driving cars. AI has come a long way from science fiction stories to practical uses. Yet ***What is artificial intelligence and how did it go from being an idea in science fiction to a technology that reshaping our world?***



Evolution of AI

This article examines the intriguing development of Artificial Intelligence from, its inception to its present state of development and promising prospects.

Envision a device with human-like cognitive abilities to learn, think, and solve issues. That is AI's central tenet. AI research aims to create intelligent machines that can replicate human cognitive functions. It has been a long and winding road filled, with moments of tremendous advancement, failures, and moments of reflection.

Fundamentally, Artificial Intelligence is the process of building machines that can replicate human intelligence. These machines can learn, reason, and adapt while carrying out activities that normally call for human intelligence. With artificial intelligence (AI) this world of natural language comprehension, image recognition, and decision making by computers can become a reality.

The Dawn of Artificial Intelligence (1950s-1960s)

The 1950s , which saw the following advancements , are considered to be the birthplace of AI :

- **1950 :** In 1950 saw the publication of Alan Turing's work ,**"Computing Machinery and Intelligence "** which introduced the Turing Test—a measure of computer intelligence.
- **1956:** A significant turning point in AI research occurs in 1956 when, **John McCarthy** first uses the phrase ***"Artificial Intelligence"*** at the Dartmouth Workshop.
- **1950s–1960s:** The goal of early artificial intelligence (AI) research was to encode human knowledge into computer programs through the use of symbolic reasoning, and logic-based environments.
- **Limited Advancement:** Quick advances are hampered by limited resources and computing-capacity.
- **Early AI systems:** This made an effort to encode human knowledge through the use of logic, and symbolic thinking. The development of early artificial intelligence (AI) systems that, depended on symbolic thinking and logic was hampered by a lack of resources, and processing capacity , which caused the field to advance slowly in the beginning.

AI’s Early Achievements and Setbacks (1970s-1980s)

This age has seen notable developments as well as difficulties :

- **1970:** The 1970s witnessed the development of expert systems , which were intended to capture the knowledge of experts in a variety of domains. Data Scientists created rule-based systems that , could use pre-established guidelines to address certain issues.
- **Limitations:** Due to their inability to handle ambiguity and complicated circumstances , these systems had a limited range of applications.
- **The Artificial Intelligence Winter(1970–1980):** A period of inactivity brought on by a lack of funding , and un-met expectations.

Machine Learning and Data-Driven Approaches (1990s)

The 1990s bring a transformative move in AI :

- **1990s:** A worldview move towards machine learning approaches happens.
- **Rise of Machine-Learning:** Calculations learn from information utilizing strategies like neural systems, choice trees , and bolster vector machines.
- **Neural Organize Insurgency:** Propelled by the human brain, neural systems pick up ubiquity for errands like discourse acknowledgment, stock advertise expectation , and motion picture suggestions.
- **Information Powers AI:** Expanded handling control , and information accessibility fuel the development of data driven AI.
- **Unused Areas Rise:** Proposal frameworks , picture acknowledgment and normal dialect handling (NLP) take root.
- **Brilliant Age of AI:** AI frameworks exceed expectations in dis-course acknowledgment, stock determining, and suggestion frameworks.
- **Improved Execution:** Handling control enhancements and information accessibility drive progressions.

The AI Boom: Deep Learning and Neural Networks (2000s-2010s)

The 21st century , witnesses the rise of profound learning , and neural systems :

- **2000s-2010s:** Profound learning a subset of machine learning imitating the human brain's structure and work , came to the cutting edge.
- **Profound Neural Systems:** Multi-layered neural systems exceeded expectations in ranges such as - picture acknowledgment, NLP and gaming.
- **Innovative Progressions:** Profound learning encouraged advance in discourse acknowledgment, NLP , and computer vision.
- **Corporate Speculation:** Tech monsters like ***Facebook, Google , and OpenAI*** made noteworthy commitments to AI inquire about.
- **Counterfeit Neural Systems:** Complex calculations, based on interconnected neurons control profound learning headways.

Generative Pre-trained Transformers: A New Era (GPT Series)

A novel advancement in recent times is the use of Generative Pre-trained Transformers :

- **GPT Series:** Trained on enormous volumes of textual data , these models have rocked the globe.
- **GPT-3:** This model transforms language processing by producing writing that is similar to that of a human being and translating between languages.
- **Learning from Text:** Large volumes of text are absorbed by GPT models, such as - GPT-3, which help them comprehend syntax, context , and comedy.
- **Beyond Translation:** GPT-3 serves as a portable writing assistant by producing essays, poetry , and even language translations.
- **The Upcoming Generation:** This new wave of models , which can write, translate and generate original material as well as provide insightful responses, is exemplified by models such as Bard, ChatGPT, and Bing Copilot.
- **Pushing Boundaries:** These developments have increased the possible applications of AI showcasing its ability in content production, creative projects and language translation.

Introduction to Internet of Things (IoT) – Set 1

IoT stands for Internet of Things. It refers to the interconnectedness of physical devices, such as appliances and vehicles, that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data. This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.

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. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a few of the categorical examples where IoT is strongly established.

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.

History of IOT

Here you will get to know about how IOT is involved and also from the explanation of each will let you know how IOT plays a role in this innovations !

- 1982 – Vending machine: The first glimpse of IoT emerged as a vending machine at Carnegie Mellon University was connected to the internet to report its inventory and status, paving the way for remote monitoring.

- 1990 – Toaster: Early IoT innovation saw a toaster connected to the internet, allowing users to control it remotely, foreshadowing the convenience of smart home devices.

- 1999 – IoT Coined (Kevin Ashton): Kevin Ashton coined the term “Internet of Things” to describe the interconnected network of devices communicating and sharing data, laying the foundation for a new era of connectivity.

- 2000 – LG Smart Fridge: The LG Smart Fridge marked a breakthrough, enabling users to check and manage refrigerator contents remotely, showcasing the potential of IoT in daily life.

- 2004 – Smart Watch: The advent of smartwatches introduced IoT to the wearable tech realm, offering fitness tracking and notifications on-the-go.

- 2007 – Smart iPhone: Apple’s iPhone became a game-changer, integrating IoT capabilities with apps that connected users to a myriad of services and devices, transforming smartphones into hubs.

- 2009 – Car Testing: IoT entered the automotive industry, enhancing vehicles with sensors for real-time diagnostics, performance monitoring, and remote testing.

- 2011 – Smart TV: The introduction of Smart TVs brought IoT to the living room, enabling internet connectivity for streaming, app usage, and interactive content.

- 2013 – Google Lens: Google Lens showcased IoT’s potential in image recognition, allowing smartphones to provide information about objects in the physical world.

- 2014 – Echo: Amazon’s Echo, equipped with the virtual assistant Alexa, demonstrated the power of voice-activated IoT, making smart homes more intuitive and responsive.

- 2015 – Tesla Autopilot: Tesla’s Autopilot system exemplified IoT in automobiles, introducing semi-autonomous driving capabilities through interconnected sensors and software.

Four Key Components of IOT

- Device or sensor

- Connectivity
- Data processing
- Interface

IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.

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 a whopping 20 billion.

Main Components Used in IoT

- **Low-power embedded systems:** Less battery consumption, high performance are the inverse factors that play a significant role during the design of electronic systems.
- **Sensors:** Sensors are the major part of any IoT application. It is a physical device that measures and detects certain physical quantities and converts it into signal which can be provided as an input to processing or control unit for analysis purpose.

Different types of Sensors

- Temperature Sensors
- Image Sensors
- Gyro Sensors
- Obstacle Sensors
- RF Sensor
- IR Sensor
- MQ-02/05 Gas Sensor
- LDR Sensor
- Ultrasonic Distance Sensor
- **Control Units:** It is a unit of small computer on a single integrated circuit containing microprocessor or processing core, memory and programmable input/output devices/peripherals. It is responsible for major processing work of IoT devices and all logical operations are carried out here.

- **Cloud computing:** Data collected through IoT devices is massive, and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.

- **Availability of big data:** We know that IoT relies heavily on sensors, especially in real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.

- **Networking connection:** In order to communicate, internet connectivity is a must, where each physical object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

Characteristics of IoT

- Massively scalable and efficient

- IP-based addressing will no longer be suitable in the upcoming future.

- An abundance of physical objects is present that do not use IP, so IoT is made possible.

- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.

- A device that is connected to another device right now may not be connected in another instant of time.

- Intermittent connectivity – IoT devices aren't always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

Top Applications of IoT in the World

IoT has made our life easier with its applications. You won't believe all the cool stuff IoT can do! Imagine having a home where the lights turn on by themselves, the TV knows your favorite shows, and even the fridge tells you when you're running out of ice cream! Yum!

In big factories, IoT helps machines work together smoothly, like a team of robots! They can even fix themselves when something is not right. Super smart!

And guess what? In hospitals, doctors can use IoT to check on patients from far away. It's like having a superhero doctor with special powers!

All these can be achieved through top IoT applications. So let's see all these **top applications of IoT** in different facets and industries of the world.

1. Smart Agriculture

Food is an integral part of life without which we cannot survive. However, it is an unfortunate fact that a lot of food is wasted in developed countries like America while people starve in poorer countries like Chad, Sudan, etc. One way to feed everyone is through better agricultural practices which can be enhanced using IoT applications. This can be done by first collecting data for a farm such as soil quality, sunlight levels, seed type, and rainfall density from various sources like farm sensors, satellites, local weather stations, etc. and then using this data with Machine Learning and IoT to create custom recommendations for each farm that will optimize the planting procedure, irrigation levels required, fertilizer amount, etc. All this will result in better yield or crops with a focus on reducing world hunger in the future. This is done very efficiently by SunCulture, a top IoT application, which is an initiative by Microsoft AI for Earth.

2. Smart Vehicles

Smart vehicles or self-driving cars are Iot applications as they can be called are pretty dependent on IoT. These cars have a lot of features that are integrated with each other and need to communicate such as the sensors that handle navigation, various antennas, controls for speeding or slowing down, etc. Here the Internet of Things technology is critical, especially in the sense that self-driving cars need to be extremely accurate and all the parts need to communicate with each other in milliseconds on the road. Tesla Cars are quite popular and working on their self-driving cars. Tesla Motors' cars use the latest advancements in Artificial Intelligence and the Internet of Things. And they are quite popular as well!!! Tesla Model 3 was the most sold plug-in electric car in the U.S. in 2018 with a total yearly sales of around 140,000 cars. This top IoT application has gained a lot of advancement in recent years

3. Smart Home

Maybe one of the most famous applications of IoT is in Smart Homes. After all, who hasn't heard about connecting all the home applications like lighting, air conditioners, locks, thermostat, etc. into a single system that can be controlled from your smartphone? These IoT devices are applications of IoT and becoming more and more popular these days because they allow you complete freedom to personalize your home as you want. In fact, these IoT devices are so popular that every second there are 127 new devices connected to the internet. Some popular ones that you might have heard have, or even have in your home, include Google Home, Amazon Echo Plus, Philips Hue Lighting System, etc. There are also all sorts of other inventions that you can install in your home including Nest Smoke Alarm and Thermostat, Foobot Air Quality Monitor, August Smart Lock, etc. These applications of IoT are getting famous nowadays.

4. Smart Pollution Control

Pollution is one of the biggest problems in most of the cities in the world. Sometimes it's not clear if we are inhaling oxygen or smog! In such a situation, IoT applications can be a big help in controlling pollution levels to more breathable standards. This can be done by collecting data related to city pollution like emissions from vehicles, pollen levels, airflow direction, weather, traffic levels, etc using various sensors in combination with IoT. Using this data, Machine Learning algorithms can calculate pollution forecasts in different areas of the city that inform city officials beforehand where the problems are going to occur. Then they can try to control the pollution levels till it's much safer. An example of this is the Green Horizons project created by IBM's China Research Lab.

5. Smart Healthcare

There are many applications of IoT in the Healthcare Industry where doctors can monitor patients remotely through a web of interconnected devices and machines without needing to be in direct contact with them. This is very useful if the patients don't have any serious problems or if they have any infectious diseases like COVID-19 these days. One of the most common uses of IoT applications in healthcare is using robots. These include surgical robots that can help doctors in performing surgeries more efficiently with higher precision and control. There are also disinfectant robots that can clean surfaces quickly and thoroughly using high-intensity ultraviolet light (which is pretty useful these days!) Other types of robots also include nursing robots that can handle the monotonous tasks that nurses have to perform for many patients day in and day out where there is little risk to the patients.

6. Smart Cities

Cities can be made more efficient so that they require fewer resources and are more energy-efficient. This can be done with a combination of sensors in different capacities all over the city that can be used for various tasks ranging from managing the traffic, controlling handling waste management, creating smart buildings, optimizing streetlights, etc. There are many cities in the world that are working on incorporating IoT applications and becoming smarter such as Singapore, Geneva, Zurich, Oslo, etc. One example of creating smart cities is the Smart Nation Sensor Platform used by Singapore which is believed to be the smartest city in the world. This platform integrates various facets of transportation, streetlights, public safety, urban planning, etc. using sensors in conjugation with IoT.

7. Smart Retail

There is a way to make shopping even more exciting for customers and that's to use the latest tech like IoT of course! Retail stores can make use of IoT applications in a wide range of operations to make shopping a much smoother experience for customers and also easier for employees. IoT can be used to handle inventory, improve store operations, reduce shoplifting and theft, and prevent long queues at the cashiers. A prime example of this application of IoT is the Amazon Go stores which provide an IoT-enabled shopping experience. These stores monitor

all their products using IoT so that customers can pick up any products and just walk out of the store without stopping at the cashier's queue. The total bill amount is automatically deducted from the card associated with the customer's Amazon account after they leave the store.

Modern Applications

- Smart Grids and energy saving
- Smart cities
- Smart homes/Home automation
- Healthcare
- Earthquake detection
- Radiation detection/hazardous gas detection
- Smartphone detection
- Water flow monitoring
- Traffic monitoring
- Wearables
- Smart door lock protection system
- Robots and Drones
- Healthcare and Hospitals, Telemedicine applications
- Security
- Biochip Transponders (For animals in farms)
- Heart monitoring implants (Example Pacemaker, ECG real time tracking)
- Agriculture
- Industry

Advantages of IoT

- Improved efficiency and automation of tasks.
- Increased convenience and accessibility of information.
- Better monitoring and control of devices and systems.
- Greater ability to gather and analyze data.
- Improved decision-making.
- Cost savings.

Disadvantages of IoT

- Security concerns and potential for hacking or data breaches.
- Privacy issues related to the collection and use of personal data.
- Dependence on technology and potential for system failures.
- Limited standardization and interoperability among devices.
- Complexity and increased maintenance requirements.
- High initial investment costs.
- Limited battery life on some devices.
- Concerns about job displacement due to automation.
- Limited regulation and legal framework for IoT, which can lead to confusion and uncertainty.

Challenges in Internet of things (IoT)

Introduction :

The Internet of Things (IoT) refers to the interconnectivity of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to connect and exchange data. The IoT concept involves extending

Internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things. The ultimate goal of IoT is to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications and covers a variety of protocols, domains, and applications.

The Internet of Things (IoT) has fast grown to be a large part of how human beings live, communicate and do business. All across the world, web-enabled devices are turning our global rights into a greater switched-on area to live in.
There are various types of challenges in front of IoT.

Security challenges in IoT :

1. **Lack of encryption –**
   Although encryption is a great way to prevent hackers from accessing data, it is also one of the leading IoT security challenges.
   These drives like the storage and processing capabilities that would be found on a traditional computer.
   The result is an increase in attacks where hackers can easily manipulate the algorithms that were designed for protection.
2. **Insufficient testing and updating –**
   With the increase in the number of IoT(internet of things) devices, IoT manufacturers are more eager to produce and deliver their device as fast as they can without giving security too much of although.
   Most of these devices and IoT products do not get enough testing and updates and are prone to hackers and other security issues.
3. **Brute forcing and the risk of default passwords –**
   Weak credentials and login details leave nearly all IoT devices vulnerable to password hacking and brute force.
   Any company that uses factory default credentials on their devices is placing both their business and its assets and the customer and their valuable information at risk of being susceptible to a brute force attack.
4. **IoT Malware and ransomware –**
   Increases with increase in devices. Ransomware uses encryption to effectively lock out users from various devices and platforms and still use a user's valuable data and info.
   Example –
   A hacker can hijack a computer camera and take pictures.
   By using malware access points, the hackers can demand ransom to unlock the device and return the data.
5. **IoT botnet aiming at cryptocurrency –**
   IoT botnet workers can manipulate data privacy, which could be massive risks for an open Crypto market. The exact value and creation of cryptocurrencies code face danger from mal-intentioned hackers.
   The blockchain companies are trying to boost security. Blockchain technology itself is not particularly vulnerable, but the app development process is.
6. **Inadequate device security :** Inadequate device security refers to the lack of proper measures to protect electronic devices such as computers, smartphones, and IoT devices from cyber attacks,

hacking, data theft, and unauthorized access. This can happen due to outdated software, weak passwords, unpatched vulnerabilities, lack of encryption, and other security risks. It is important to regularly update the software and implement strong security measures to ensure the security and privacy of sensitive information stored on these devices. Many IoT devices have weak security features and can be easily hacked.

7. **Lack of standardization:** Lack of standardization refers to the absence of agreed-upon specifications or protocols in a particular field or industry. This can result in different systems, products, or processes being incompatible with each other, leading to confusion, inefficiency, and decreased interoperability. For example, in the context of technology, a lack of standardization can cause difficulties in communication and data exchange between different devices and systems. Establishing standards and protocols can help overcome this and ensure uniformity and compatibility. There is a lack of standardization in IoT devices, making it difficult to secure them consistently.
8. **Vulnerability to network attacks:** Vulnerability to network attacks refers to the susceptibility of a network, system or device to being compromised or exploited by cyber criminals. This can happen due to weaknesses in the network infrastructure, unpatched software, poor password management, or a lack of appropriate security measures. Network attacks can result in data theft, loss of privacy, disruption of services, and financial loss. To reduce vulnerability to network attacks, it's important to implement strong security measures such as firewalls, encryption, and regular software updates, as well as educate users on safe internet practices. IoT devices rely on networks, making them vulnerable to attacks like denial-of-service (DoS) attacks.
9. **Unsecured data transmission:** Unsecured data transmission refers to the transfer of data over a network or the internet without adequate protection. This can leave the data vulnerable to interception, tampering, or theft by malicious actors. Unsecured data transmission can occur when data is transmitted over an unencrypted network connection or when insecure protocols are used. To protect sensitive data during transmission, it is important to use secure protocols such as SSL/TLS or VPN, and to encrypt the data before sending it. This can help to ensure the confidentiality and integrity of the data, even if it is intercepted during transmission. IoT devices often transmit sensitive data, which may be vulnerable to eavesdropping or tampering if not properly secured.
10. **Privacy concerns:** Privacy concerns refer to issues related to the collection, storage, use, and sharing of personal information. This can include concerns about who has access to personal information, how it is being used, and whether it is being protected from unauthorized access or misuse. In the digital age, privacy concerns have become increasingly important as personal information is being collected and stored on an unprecedented scale. To address privacy concerns, individuals and organizations need to implement appropriate security measures to protect personal information, be transparent about how it is being used, and respect individuals' rights to control their own information. Additionally, privacy laws and regulations have been established to provide guidelines and protections for individuals' personal information. The vast amount of data generated by IoT devices raises privacy concerns, as personal information could be collected and used without consent.
11. **Software vulnerabilities:** Software vulnerabilities are weaknesses or flaws in software code that can be exploited by attackers to gain unauthorized access, steal sensitive information, or carry out malicious activities. Software vulnerabilities can arise from errors or mistakes made during the development process, or from the use of outdated or unsupported software. Attackers can exploit these vulnerabilities to gain control over a system, install malware, or steal sensitive

information. To reduce the risk of software vulnerabilities, it is important for software developers to follow secure coding practices and for users to keep their software up-to-date and properly configured. Additionally, organizations and individuals should implement robust security measures, such as firewalls, antivirus software, and intrusion detection systems, to protect against potential threats. IoT devices often have software vulnerabilities, which can be exploited by attackers to gain access to devices and networks.

12. **Insider threats:** Insider threats refer to security risks that come from within an organization, rather than from external sources such as hackers or cyber criminals. These threats can take many forms, such as employees who intentionally or unintentionally cause harm to the organization, contractors who misuse their access privileges, or insiders who are coerced into compromising the security of the organization. Insider threats can result in data breaches, theft of intellectual property, and damage to the reputation of the organization. To mitigate the risk of insider threats, organizations should implement strict access controls, monitor employee activity, and provide regular training on security and privacy policies. Additionally, organizations should have a plan in place to detect, respond to, and recover from security incidents involving insiders. Employees or contractors with access to IoT systems can pose a security risk if they intentionally or unintentionally cause harm.

Most Common Threats to Security and Privacy of IoT Devices

Nowadays, the Internet is growing at a very fast rate with the advancement in technologies and techniques. Some years ago, we did not necessarily require an advanced level security system for our networking devices because the internet is not that much advanced in that era. According to a survey in 2017, 51% of big companies didn't even think about securing their devices because they felt that their devices might not be attacked by hackers and now approx **96%** of companies think that there may be a huge increase in attacks of IoT devices in upcoming years.

As technology is becoming advanced, attacks on internet devices are increasing very rapidly and becoming more and more common. Now, security and privacy have become a very important aspect of any IoT device. In this article, we will discuss some most common threats to the security and privacy of IoT devices.

1. Weak Credentials

Generally, large manufactures ship their products with a username of "admin" and with the password "0000" or "1234" and the consumers of these devices don't change them until they were forced to that by security executive. These kinds of acts make a path for hackers to hack consumer's privacy and let them control the consumer's device. In 2016, the *Mirai botnet Attack* as a result of using weak credentials.

2. Complex Structure of IoT Devices

IoT devices have a very complex structure that makes it difficult to find the fault in devices. Even if a device is hacked the owner of that device will be unaware of that fact. Hackers can force the device to join any malicious botnets or the device may get infected by any virus. We can not directly say that the device was hacked because of its complex structure. A few years ago, a security agency has proved that a smart refrigerator was found sent thousand plus spam mails. The interesting fact was that the owner of that refrigerator even did not know about that.

3. Outdated Software and Hardware

It has been seen that IoT devices are secured when they are shipped. But the issues come here when these devices do not get regular updates. When a company manufactures its device, it makes the devices secure from all the threats of that time but as we discussed earlier, the Internet and technologies are growing at a very fast rate. So after a year or two, it becomes very easy for hackers to find the weakness of old devices with modern technologies. That's why security updates are the most important ones.

4. Rapid increase in Ransomware

With the advancement of the internet, hackers are also getting advanced. In the past few years, there is a rapid increase in malicious software or ransomware. This is causing a big challenge for IoT device manufacturers to secure their devices.

5. Small Scale Attacks

IoT devices are attacked on a very small scale. Manufacturing companies are trying to secure their devices for large scale attacks but no company is paying to attention small attacks. Hackers do small attacks on IoT devices such as baby monitoring devices or open wireless connections and then forced to join botnets.

6. Insecure Data Transfer

It is very difficult to transmit data securely in such a large amount as there are billions of IoT enabled devices. There is always a risk of data leaking or get infected or corrupted.

7. Smart Objects

Smart objects are the main building block of any device. These smart objects should able to communicate with another object or device or a sensor in any infrastructure securely. Even while these devices or objects are not aware of each other's network status. This is also an important issue. Hackers can hack these devices in open wireless networks.