Computer History

Our journey begins here. Let's go back in time to learn about computer history

In 1834, Charles Babbage announces the analysis engine

British mathematics teacher **Charles Babbage** woke up one morning to start creating the analytical machine!. A modern general-purpose computer that was a major breakthrough in the history of computer science.

Its general purpose was a machine that could be programmed by the user, capable of executing the desired instructions and commands. It was mechanical in nature, and already had many parts of a modern computer. It could store **1000 numbers of 50 digits each**, and although it could never be built by its inventor, Babbage, because the necessary technology was not yet available, it was one of the first milestones of computer science.

1943: The birth of Mark I Colossus

The Colossus machines were the first electronic calculating devices. They were used by the British to read German encrypted communications during World War II. This means that the Colossus, originally designed by Tommy Flowers, was one of the first digital computers.

1954: First prototype of desktop calculators

Back in 1954, **IBM** presented the world's first electronic calculator in the United States, made with transistors, something highly revolutionary and technological for the time. It was quite large and could cost around **$80,000**. But, after a short time, more commercial models were launched, which thanks to the development were more reliable and affordable.

1969: The creation of ARPANET

ARPANET was just a small network of computers that was created on behalf of the United States Department of Defense. They did so as a way of communication for the various agencies in the country. We are witnessing the seminal net that would become what we now know as the **Internet**. In 1990, ARPANET ended its existence.

1971: The first e-mail is sent

The first e-mail was sent by **Ray Tomlinson**. As a curiosity, he used for the first time the @ symbol between the user name and the machine. This fact is now a thing of the past, as you can imagine. He chose this symbol because, he explained, **"it certainly wasn't in a real name"**.

1981: IBM launches a PC

IBM achieved a milestone in the history of humanity in general and of computing in particular: with the commercialization of the personal computer, or PC, it managed to turn computing from being a hidden mystery for the majority, to becoming something useful and practical for everyone.

I assure you that **neither prophets nor seers** could have imagined the revolution that this would entail today.

1990: Tim Berners-Lee writes the first website

It was exactly on December 20, 1990, when **Berners-Lee**, a British scientist, uploaded this page to CERN's servers, with the mission of explaining the basic principles of what the modern web was going to be.

As you can see, it is a simple page with rudimentary text and hyperlinks. This is a modest guide on how his project would work.

1997: The machine defeats the man, in chess

Such a prick to our ego resonated beyond the limits of the board, to spread beyond the confines of the pedestal on which the human being thought he was standing.

The event took place in two parts, the first in Philadelphia on February 10, 1996, where the IBM **Deep Blue** supercomputer faced the then champion, Garry Kasparov. In the first game, after an initial fright, the great master ended up winning. Humanity could continue to breathe in peace. But IBM prepared the rematch. It was held shortly thereafter in New York City in 1997. In that historic duel the machine won. Though by an adjusted outcome, man's intellectual supremacy on Earth was defeated.

1998: Google was founded

In 1995, **Larry Page and Sergey Brin** met as colleagues at Stanford. Already as computer students, they collaborated on a search engine called BackRub that operated on Stanford's servers until it was too bandwidth-intensive to cope with the university.

In 1997, they decided that the **BackRub** search engine needed a new look and feel and considered some ideas, including a game of the word "googol", a mathematical term represented by the number 1 followed by 100 zeros.

In 1998, the then co-founder of Sun, **Andy Bechtolsheim**, prepared a check for about $100,000 for a newly registered company, a certain **Google Inc.** that would make us all happy.

2018: You get to meet Pandora FMS

Pandora FMS is a flexible monitoring software, which is capable of monitoring devices, infrastructures, applications, services and business processes.

Computer

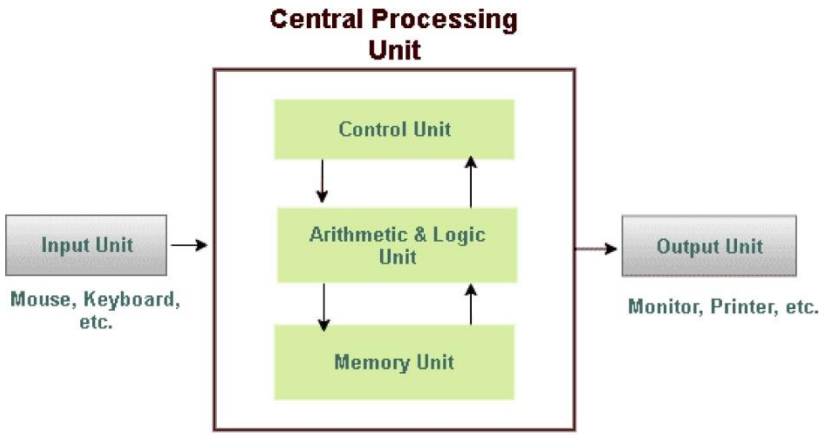
Computer : Computer is an electronic device that is designed to work with Information. *The term computer* is *derived from the Greek term* '**compute**', this means to *calculate* or *programmable machine*. **Computer can not do anything without a Program**. It represents the decimal numbers through a string of binary digits. The Word 'Computer' usually refers to the Center Processor Unit plus Internal memory.

Charles Babbage is called the **Father** of the modern computer. The **First mechanical computer designed by Charles Babbage** was called **Analytical Engine.** It uses read-only memory in the form of punch cards.

The computer is an electronic device that takes input from the user and processes these data under the control of a set of instructions (called program) and gives the result (output) and saves future use. It can process both numerical and non-numerical (arithmetic and logical) calculations.

Block Diagram of Computer

A Block diagram of a computer displays a structural representation of a computer system. The block diagram gives you a quick overview of the working process of a computer from inputting the data to retrieving the desired results.
A computer system is a combination of three components:



- Input Unit
- *CPU (Central Processing Unit)*
- Output Unit

Input Unit

The Input Unit consists of input devices such as a mouse, keyboard, scanner, joystick, etc. These devices are used to input information or instruction into the computer system. Like other electronic machines, a computer takes inputs as raw data (binary data) and performs necessary processing giving out processed data. Therefore, the input unit is the medium of communication that takes data from us to the computer in an organized manner for processing.

The Input Unit performs the following major functions:

- The input unit converts the inputted data or instructions into binary form for further processing.
- Input Unit transmits the data to the main memory of the computer.

Central Processing Unit

CPU or Central Processing Unit is known as the brain of the computer system t is an electronic hardware device that processes all the operations (e.g., arithmetic and logical operations) of the computer. In other words, all the major calculations, operations or comparisons are performed inside the CPU. It is also responsible for handling the operations of several other units.

In the above diagram, the Control Unit (CU) and **Arithmetic & Logic Unit (ALU)** are jointly called the **Central Processing Unit (CPU).**

Let's discuss all the parts displayed in the above diagram one by one:

Control Unit

As the name suggests, the control unit of a CPU controls all the activities and operations of the computer. It is also responsible for controlling input/output, memory, and other devices connected to the CPU.

The control unit acts like the supervisor which determines the sequence in which

computer programs and instructions are executed. It retrieves instructions from memory decodes the instructions, interprets the instructions and understands the sequence of tasks to be performed accordingly. It further transmits the instructions to the other parts of the computer system to

execute them. In short, the control unit determines the sequence of operations to execute the given instructions.

Arithmetic & Logic Unit

The data inputted through input devices is stored in the primary storage unit. The Arithmetic Logic Unit (ALU) performs arithmetic and logical operations.

The arithmetic unit controls simple operations such as **addition, subtraction, division,** and

multiplication.

On the other side, the logical unit controls the logical operations such as AND, OR, Equal, greater than, and less than, etc. Apart from it, the logic unit also responsible for performing several other operations such as comparing, selecting, matching, and merging data.

Memory Unit

Memory Unit is an essential part of the computer system which is used to store data and instructions before and after processing. The memory unit transmits the information to other units of the computer system when required.

There are two types of memory units:

Primary Memory

The primary memory cannot store a vast amount of data. The data stored in the primary memory is temporary. The data will be lost if they are disconnected from the power supply. The primary memory usually stores the input data and immediate calculation results. The primary memory is also known as the Main Memory or **temporary memory. Random Access Memory** (RAM) is an example of primary

memory.

Secondary Memory

The use of primary memory is not possible to store data permanently for future access. Therefore, there are some other options to store the data permanently for future use, which is known as secondary memory or **auxiliary** storage or permanent storage. The data stored in the secondary memory is safe even when there is a power failure or no power supply. Hard Disk is usually considered a secondary memory.

The Central Processing Unit performs the following major functions:

- The CPU controls all components, software and data processing of the computer system.

- The CPU takes data from input devices, executes the data, and sends output to the output devices.
- The CPU processes all the operations, including all the arithmetical and logical operations.

Output Unit

The output unit consists of devices that are used to display the results or output of processing. The output data is first stored in the memory and then displayed in human-readable form through output devices. Some of the widely used output devices are Monitor, Printer, and Projector.

The Output Unit performs the following major functions:

- The output unit accepts the data or information in binary form from the main memory of the computer system.

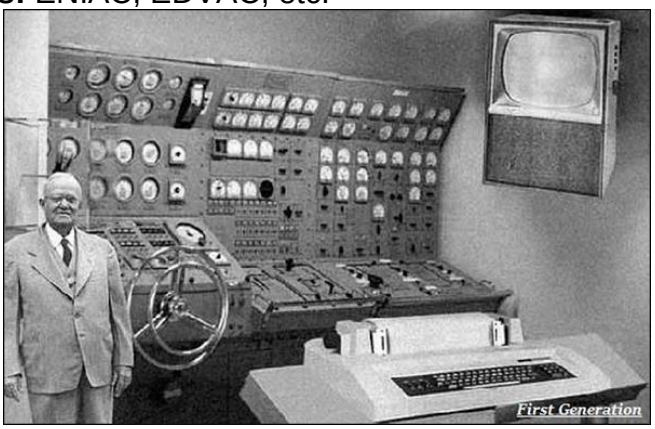
The output unit converts the binary data into a human-readable form for better understanding.

Computer Generations

Let us now discuss the development in Computer Technology over the different generations.

First Generation

- The period 1940 to 1956, roughly considered as the First Generation of Computer.
- The first generation computers were developed by using vacuum tube or thermionic valve machine.
- The input of this system was based on punched cards and paper tape; however, the output was displayed on printouts.
- The first generation computers worked on binary-coded concept (i.e., language of 0-1). **Examples:** ENIAC, EDVAC, etc.



Second Generation

- The period 1956 to 1963 is roughly considered as the period of Second Generation of Computers.
- The second generation computers were developed by using transistor technology.
- In comparison to the first generation, the size of second generation was smaller.
- In comparison to computers of the first generation, the computing time taken by the computers of the second generation was lesser.

Third Generation

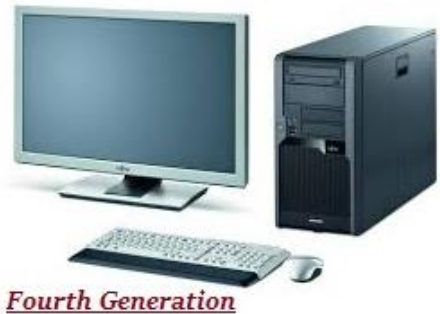
- The period 1963 to 1971 is roughly considered as the period of Third Generation of computers.
- The third generation computers were developed by using the Integrated Circuit (IC) technology.

Third Generation

- In comparison to the computers of the second generation, the size of the computers of the third generation was smaller.
- In comparison to the computers of the second generation, the computing time taken by the computers of the third generation was lesser.
- The third generation computer consumed less power and also generated less heat.
- The maintenance cost of the computers in the third generation was also low.
- The computer system of the computers of the third generation was easier for commercial use.

Fourth Generation

- The period 1972 to 2010 is roughly considered as the fourth generation of computers.
- The fourth generation computers were developed by using microprocessor technology.



Fourth Generation

- By coming to fourth generation, computer became very small in size, it became portable.
- The machine of fourth generation started generating very low amount of heat.
- It is much faster and accuracy became more reliable.
- The production cost reduced to very low in comparison to the previous generation.
- It became available for the common people as well.

Fifth Generation

- The period 2010 to till date and beyond, roughly considered as the period of fifth generation of computers.
- By the time, the computer generation was being categorized on the basis of hardware only, but the fifth generation technology also included software.

- The computers of the fifth generation had high capability and large memory capacity.
- Working with computers of this generation was fast and multiple tasks could be performed simultaneously.
- Some of the popular advanced technologies of the fifth generation include Artificial intelligence, Quantum computation, Nanotechnology, Parallel processing, etc.

Internet

Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.

It is believed that the internet was developed by "Defense Advanced Projects Agency" (DARPA) department of the United States. And, it was first connected in 1969.

Uses of the internet

Generally speaking, the Internet may be used to exchange information with people all over the world, communicate across great distances, and locate information or answers fast on almost any subject.

Here are some examples of specific uses for the Internet:

- Using social media and content sharing.
- Instant messaging, video conferencing, Internet Relay Chat (IRC), Internet telephony, and email are all examples of electronic communication. These all are used through the Internet.
- Access to online degree programs, courses, and workshops for education and self-improvement.
- Searching for jobs: To advertise available positions, submit job applications, and hire candidates identified on social networking sites like LinkedIn, both employers and applicants use the Internet.

Other examples include:

- Online dating
- Online gaming
- Research
- Reading electronic newspapers and magazines
- Online shopping, or e-commerce.
- Online discussion groups and forums

Advantages of the Internet:

- **Instant Messaging:** You can send messages or communicate to anyone using internet, such as email, voice chat, video conferencing, etc.
- **Get directions:** Using GPS technology, you can get directions to almost every place in a city, country, etc. You can find restaurants, malls, or any other service near your location.

- **Online Shopping:** It allows you to shop online such as you can be clothes, shoes, book movie tickets, railway tickets, flight tickets, and more.
- **Pay Bills:** You can pay your bills online, such as electricity bills, gas bills, college fees, etc.
- **Online Banking:** It allows you to use internet banking in which you can check your balance, receive or transfer money, get a statement, request cheque-book, etc.
- **Online Selling:** You can sell your products or services online. It helps you reach more customers and thus increases your sales and profit.
- **Work from Home:** In case you need to work from home, you can do it using a system with internet access. Today, many companies allow their employees to work from home.
- **Entertainment:** You can listen to online music, watch videos or movies, play online games.
- **Cloud computing:** It enables you to connect your computers and internet-enabled devices to cloud services such as cloud storage, cloud computing, etc.
- **Career building:** You can search for jobs online on different job portals and send you CV through email if required.

Disadvantages of the Internet

- **Time wastage:** Although, Internet has a lot of advantages, it also contains some limitations. Time wasting is one of among them. It can decrease your productivity if you are spending too much time on the Internet using social media apps while doing nothing. Rather than squandering time, one should use that time to do something useful and even more productive.
- **Bad impacts on health:** You can get health related issues if you spend too much time online; your body needs outside activities, exercise, and many other things. If you look at the screen for a long time, it causes negative effects on the eyes.
- **Cyber Crimes:** These days, crimes including cyberbullying, spam, viruses, hacking, and data theft are increasing day by day. Cybercriminals can quickly break into your system, which store all of your private information.

- **Effects on children:** The constant watching of videos and playing games on the Internet by young children is bad for their social and overall personality development.
- **Bullying and spreading negativity:** Social media applications have provided a free tool to all those people who regularly attempt to spread negativity with really repulsive and humiliating comments and try to bully each other, which is wrong and does bad impact on society.

History of the Internet

- The forerunner of the Internet, the ARPANet, went live for the first time in **1969**. The TCP/IP, open networking protocol suite, was adopted by the ARPANet in 1983, and the National Science Foundation Network (NSFN) developed the network to link university computer science departments across the US in 1985.
- When the hypertext transfer protocol (HTTP) was developed in 1989, it enabled different computer platforms to connect to the same Internet sites, which dramatically improved communications over the network. The Mosaic Web browser was developed in **1993**.
- Over the years of its existence, the Internet has remained a constant growth and development. For instance, IPv6 was created to provide for a significant future rise in the number of IP addresses that could be used. In a related development, the Internet of Things (IoT) refers to the rapidly developing environment where nearly any entity or device can be given a unique identifier (UID) and the capability to communicate data automatically over the Internet.

Social impact of the Internet

Both positive and negative effects of the Internet on society can be observed. On the one hand, some people claim that the Internet has raised the risk of withdrawal, social exclusion, alienation, and citing a rise in FOMO, or the fear of missing out, as evidence. On the other hand, some people also believe that the Internet has had the opposite impact on society, increasing sociability, civic participation, and the depth of connections.

The Internet has changed how society communicates and interacts, whether the effects are positive or negative on society. The increased focus on personal growth is one example of change and the fall in a community that is determined by space, job, and family. People increasingly now build social connections on the basis of their unique projects, values, as well as interests. In addition to offline and in person, communities are being created by like-minded people through the Internet and the abundance of online settings it provides and produces. Social networking sites like Facebook and LinkedIn are the preferred platforms for both businesses and individuals wishing to carry out various tasks and connect with others.

Internet service provider

An internet service provider (ISP) is a company that provides access to the internet. ISPs can provide this access through multiple means, including dial-up, DSL, cable, wireless and fiber-optic connections.

A variety of companies serve as ISPs, including cable providers, mobile carriers, and telephone companies. In some cases, a single company may offer multiple types of service (e.g., cable and wireless), while in other cases, a company may focus on just one type of service (e.g., fiber-optic). Without an ISP, individuals and businesses could not reach the internet and the opportunities it provides.

Different ways to Connect to the Internet

The various methods for connecting to the Internet are briefly discussed below:

- **Dial-Up:** Users must connect their phone line to a computer system in such connections in order to access the Internet connection. The user is unable to make or receive calls using the tier home phone service while connected.
- **Broadband:** Today's most popular high-speed internet connection, broadband is offered either by cable or phone companies.
- **Wireless Connection:** This category includes Mobile and Wi-Fi services providers. No matter where you are, you can connect to the Internet anywhere because connectivity is made possible by radio waves. Several instances of wireless connections are provided below:
- **Wi-fi:** Without the use of cables, wi-fi or wireless fidelity, enables high-speed internet connectivity.
- **Mobile Phones:** In modern times, all smartphones include an Internet connectivity option that can be availed using Internet packs and coupons. These don't require a wire or external connection as well.
- **Satellite:** Satellites are utilized for wireless Internet connectivity in areas Where broadband connections is not available.

IP Address

IP Address stands for Internet Protocol Address. Every PC/Local machine is having an IP address and that IP address is provided by the Internet Service Providers (ISPs). These are some sets of rules which govern the flow of data whenever a device is connected to the Internet. It differentiates computers, websites, and routers. Just like human identification cards like Aadhaar cards, Pan cards, or any other unique identification documents. Every laptop and desktop has its own unique IP address for identification. It's an important part of Internet technology. An IP address is displayed as a set of four-digit like 192.154.3.29. Here each number on the set ranges from 0 to 255. Hence, the total IP address range from 0.0.0.0 to 255.255.255.255.

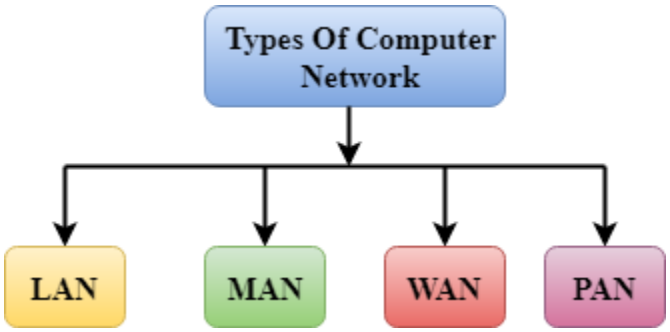
You can check the IP address of your Laptop or desktop by clicking on the Windows start menu -> then right-click and go to network -> in that go to status and then Properties you can see the IP address. There are four different types of IP addresses are available:

1. Static IP Address
2. Dynamic IP Address
3. Private IP Address
4. Public IP Address

Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)

- WAN(Wide Area Network)

LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

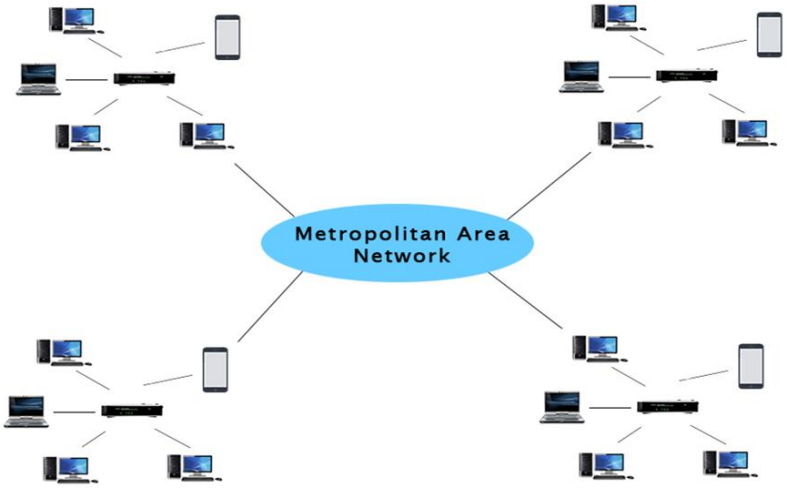
PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.

- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

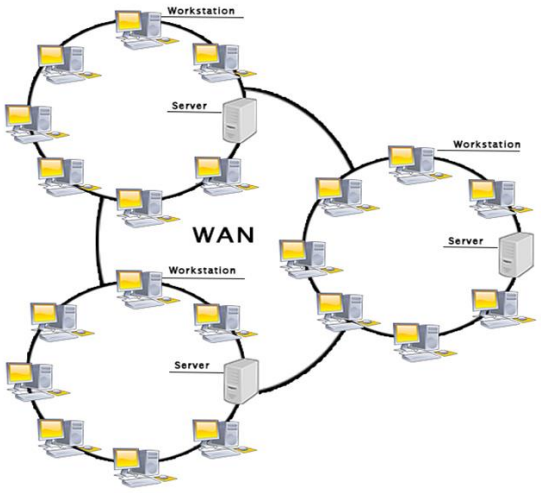


Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.

- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Network Security

Network security is a set of hardware and software solutions that stop unauthorized users from accessing a network and its resources. The goal of network security is to create a safe work platform for devices, users, and programs.

Network security has several vital roles within an IT environment:

- Prevent unauthorized access to assets and data.
- Protect network data, infrastructure, and all traffic from external threats.
- Stop threats from spreading through the system.
- Enable secure data sharing between systems and employees.
- Grant users adequate access to resources.
- Detect and respond to suspicious user behavior and software anomalies.

The framework for successful network security has three phases:

- **Protection:** Configure systems and networks correctly and ensure there are no vulnerabilities.
- **Detection:** Identify dangers before the attacker does damage or spreads through the network.
- **Reaction:** Quickly eliminate threats and return the network to a safe state.

Network Security Concepts

1. **Firewall** – A network device that controls network traffic based on predetermined rules. Firewalls can also be software-based or hardware-based, depending on your network requirements.

2. **Intrusion Detection System (IDS)** – A network security system designed to detect malicious activity within a network. IDS systems can be either network-based or host-based and are often used in conjunction with other network security mechanisms such as firewalls.

3. **Intrusion Prevention System (IPS)** – A network security system designed to prevent malicious activity within a network by monitoring network traffic for suspicious patterns and blocking any activities that appear dangerous or potentially malicious.

4. **Access Control List (ACL)** – A list of rules used to control access to resources on a network, including specific IP addresses, users, and ports. ACLs can be configured for either read or write operations on specific network.

5. **Network Access Control (NAC)** – A network security solution that allows administrators to restrict access to a network based on the user's identity, device type, and other criteria.

6. **Virtual Private Networks (VPN)** – An encrypted network connection used to securely connect two or more private networks over a public network such as the Internet.

7. **Cryptography** – The study of how data is protected through encryption algorithms and cryptographic protocols.

8. **SSL/TLS** – Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are network protocols used to secure network traffic.

9. **PKI** – Public Key Infrastructure (PKI) is a network security solution that uses public-key cryptography to authenticate network users and their devices.

10. **NAT** – Network Address Translation (NAT) is a network security technique that allows private networks to use one or more public IP addresses for outgoing traffic.

11. **DDoS** – Distributed Denial of Service attacks are malicious attempts to overwhelm network resources with large amounts of network traffic from multiple sources or locations.

12. **IPSec** – Internet Protocol Security (IPSec) is an internet standard protocol suite for establishing secure, encrypted connections between network devices.

13. **TACACS** – Terminal Access Controller Access Control System (TACACS) is a network security protocol used to authenticate network users and their devices.

14. **RADIUS** – Remote Authentication Dial-In User Service (RADIUS) is a network authentication protocol used to securely connect network users with network services such as VPNs, network access control (NAC), and wireless networks.

15. **WPA/WPA2** – Wi-Fi Protected Access (WPA/WPA2) is the most commonly used wireless network security protocol for encrypting traffic between Wi-Fi access points and clients.

What is Information Assurance (IA)?

Information Assurance (IA) is the practice of managing information-related risks and the steps involved to protect information systems such as computer and network systems.

The US Government's definition of information assurance is:

"measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

The 5 pillars of Information Assurance

Information Assurance (IA) is essentially protecting information systems, and is often associated with the following five pillars:

1. Integrity
2. Availability
3. Authentication
4. Confidentiality
5. Nonrepudiation

The five pillars of information assurance can be applied various ways, depending on the sensitivity of your organization's information or information systems. Currently, these five pillars are used at the heart of the US Government's ability to conduct safe and secure operations in a global environment.

The NIST Cybersecurity Framework is a framework that organizations can use to manage and reduce their cybersecurity risks. ISO 27001 sets out the requirements for a best-practice ISMS (information security management system).

Both frameworks are closely aligned, making ISO 27001 an excellent way to comply with the NIST CSF. Learn how they can benefit your organization in our free paper.

Download now

1. Integrity

Integrity involves assurance that all information systems are protected and not tampered with. IA aims to maintain integrity through anti-virus software on all computer systems and ensuring all staff with access know how to appropriately use their systems to minimize malware, or viruses entering information systems.

IT Governance provides a variety of E-learning courses to improve staff awareness on topics such as phishing and ransomware to reduce the likelihood of systems being breached and data being exposed.

2. Availability

Availability means those who need access to information, are allowed to access it. Information should be available to only those who are aware of the risks associated with information systems.

3. Authentication

Authentication involves ensuring those who have access to information are who they say they are. Ways of improving authentication include methods such as two-factor authentication, strong passwords, biometrics, and other devices. Authentication may also be used to itentify not only users, but also other devices.

4. Confidentiality

IA involves the confidentiality of information, meaning only those with authorization may view certain data. This step is closely mirrored by the six data processing principles of the General Data Protection Regulation (GDPR), whereby personal data must be processed in a secure manner *"using appropriate technical and oganizational measures" ("integrity and confidentiality").*

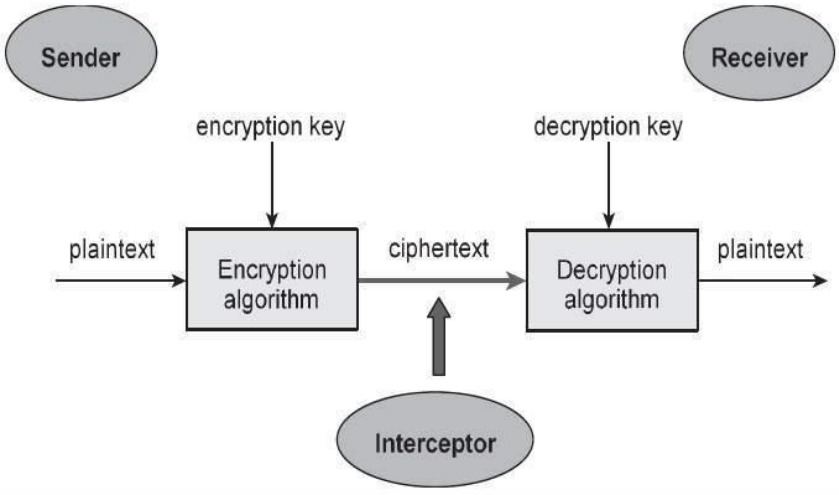
5. Nonrepudiation

The final pillar means someone with access to your organization's information system cannot deny having completed an action within the system, as there should be methods in place to prove that they did make said action.

Cryptography Definition

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.

Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.



Techniques used For Cryptography: In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography: In general there are two types Of cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).

2. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

Malware

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions and monitor end users' computer activity.

Malware can do

Malware can infect networks and devices and is designed to harm those devices, networks and/or their users in some way.

Depending on the type of malware and its goal, this harm may present itself differently to the user or endpoint. In some cases, the effect malware has is relatively mild and benign, and in others, it can be disastrous.

No matter the method, all types of malware are designed to exploit devices at the expense of the user and to the benefit of the hacker -- the person who has designed and/or deployed the malware.

Malware infections happen

Malware authors use a variety of physical and virtual means to spread malware that infects devices and networks. For example, malicious programs can be delivered to a system with a USB drive, through popular collaboration tools and by drive-by downloads, which automatically download malicious programs to systems without the user's approval or knowledge.

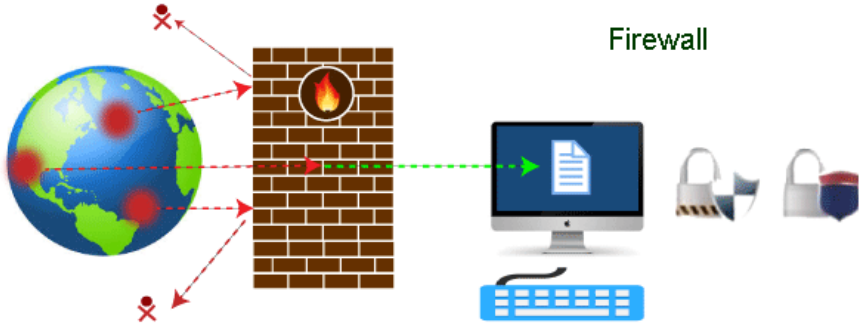
Firewall

Nowadays, it is a big challenge to protect our sensitive data from unwanted and unauthorized sources. There are various tools and devices that can provide different security levels and help keep our private data secure. One such tool is a 'firewall' that prevents unauthorized access and keeps our computers and data safe and secure.

Firewall

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

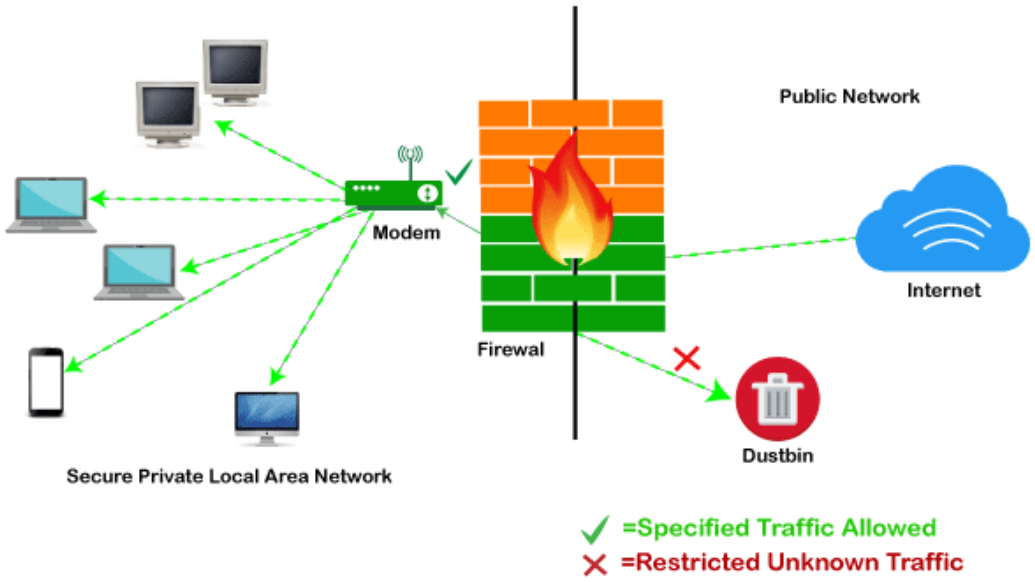


Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

Firewall works

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.



Functions of Firewall

As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

Types of Firewall

Depending on their structure and functionality, there are different types of firewalls. The following is a list of some common types of firewalls:

- Proxy Firewall
- Packet-filtering firewalls

- Stateful Multi-layer Inspection (SMLI) Firewall
- Unified threat management (UTM) firewall
- Next-generation firewall (NGFW)
- Network address translation (NAT) firewalls

Fraud techniques in cyber security

Cyber criminals use a variety of attack vectors and strategies to commit internet fraud. This includes malicious software, email and instant messaging services to spread malware, spoofed websites that steal user data, and elaborate, wide-reaching phishing scams.

Internet fraud can be broken down into several key types of attacks, including:

1. Phishing and spoofing: The use of email and online messaging services to dupe victims into sharing personal data, login credentials, and financial details.
2. Data breach: Stealing confidential, protected, or sensitive data from a secure location and moving it into an untrusted environment. This includes data being stolen from users and organizations.
3. Denial of service (DoS): Interrupting access of traffic to an online service, system, or network to cause malicious intent.
4. Malware: The use of malicious software to damage or disable users' devices or steal personal and sensitive data.
5. Ransomware: A type of malware that prevents users from accessing critical data then demanding payment in the promise of restoring access. Ransomware is typically delivered via phishing attacks.
6. Business email compromise (BEC): A sophisticated form of attack targeting businesses that frequently make wire payments. It compromises legitimate email accounts

through social engineering techniques to submit unauthorized payments.

Data Privacy and Data Protection

1. Data Privacy :

Data Privacy refers to the proper handling of data means how a organization or user is determining whether or what data to be shared with third parties. Data privacy is important as it keeps some data secret from others/third parties. So we can say data privacy is all about authorized access. It is also called as Information privacy.

Example –

In Bank, A lot of customers have their account for monetary transactions. So the bank needs to keeps customers data private, so that customers identity stays safe and protected as much as possible by minimizing any external risks and also it helps in maintaining the reputation standard of banks.

2. Data Protection :

Data Protection refers to the process of keeping safe to important information. In simple it refers protecting data against unauthorized access which leads to no corruption, no compromise, no loss and no security issues of data. Data protection is allowed to all forms of data whether it is personal or data or organizational data.

Example –

A bank has lot of customers, so the bank needs to protect all types of data including self bank records as well as customer information from unauthorized accesses to keep everything safe and to ensure everything is under the control of bank administration.

The terms Data Privacy and Data Security are used interchangeably and seems to be same. But actually they are not same. In reality they can have different meanings depending upon its actual process and use. But it is sure they are very closely interconnected and one complements the other during the entire process. So, now let's know how Data Privacy is different from Data Protection from the below table.

Difference between Data Privacy and Data Protection :

S.No.	Data Privacy	Data Protection
01.	Data Privacy refers maintaining secrecy or keeping control on data access.	Data Protection is the process of protecting data from external risks such corruption, loss etc.
02.	It is all about authorized access means it defines who has authorized	It is all about unauthorized access means if anyone has not access to data

	access to data.	then it keeps the data safe from that unauthorized access.
03.	Data Privacy is a legal process/situation which helps in establishing standards and norms about accessibility.	Data Protection is a technical control system which keeps data protected from technical issues.
04.	Data Privacy is the regulations or policies.	Data protection is the procedures and mechanism.
05.	It can be said as a security from sales means holding the data from shared and sold.	It can be said as s security from hacks means keeping the information away from hackers.