UNIT V: ESSENTIALS OF COMPUTER SCIENCE:

Milestones of computer evolution - Internet, history, Internet Service Providers, Types of Networks, IP, Domain Name Services, applications.

Ethical and social implications: Network and security concepts- Information Assurance Fundamentals, Cryptography-Symmetric and Asymmetric, Malware, Firewalls, Fraud Techniques-Privacy and Data Protection

1. Milestones of computer evolution

The history of the computer dates back to several years. There are five prominent generations of computers. Each generation has witnessed several technological advances which change the functionality of the computers. This results in more compact, powerful, robust systems which are less expensive.

The brief history of computers is discussed below –

- First Generation: (1940-1956)
  Used vacuum tubes, were large, and had limited processing power
- Second Generation: (1956-1963)
  Used transistors, were smaller and more reliable
- Third Generation: (1964-1971)
  Used integrated circuits, reduced size and power consumption
- Fourth Generation: (1971-Present)
  Used microprocessors, personal computers emerged
- Fifth Generation: (1990-Present)
  i) Used artificial intelligence
  ii) Highly interconnected and intelligent systems.

2000 B.C.: Abacus first used in computation

1642 A.D.: Blaise Pascal creates a mechanical adding machine for tax computations

1670: Gottfried von Leibniz creates a more reliable adding machine that adds, subtracts, multiplies, divides, and calculates square roots

1842: Charles Babbage designs analytical engine to perform calculations automatically; Ada, countess of Lovelace, programs this machine

1890: Herman Hollerith designs census recording system that uses punched cards; starts a company that later becomes IBM

1946: J. Presper Eckert and John Mauchly design and build the ENIAC; considered the first modern computer, used vacuum tubes

1946: John von Neumann proposes stored program architecture that bears his name

1951: Eckert & Mauchly build the first general-purpose computer, the UNIVAC I

1957: John Backus and his IBM team complete the first Fortran compiler

1958: IBM introduces the 7090 series, first to use transistors

1964: IBM announces the 360, first to use integrated circuitry (IC)

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.

1971: The first e-mail is sent

1975: The Altair, the first microcomputer, is introduced

1975: The Cray-1, the first supercomputer, is announced

1977: Steve Wozniak and Steve Jobs found Apple Computers

1981: IBM introduces its own PC

1984: Apple introduces the Macintosh
1990: Tim Berners-Lee writes the first website
1994 Netscape Navigator 1.0 is released; the WWW takes off
1995: Sun releases Java 1.0; object-oriented programming takes off
1997: The machine defeats the man, in chess
1998: Google was founded
2000s – Broadband internet: The 21st century has seen the mass adoption of broadband internet across the developed world.
2000s – Connected living: Today's homes are rapidly transforming into spaces where traditional computers dovetail alongside newer pieces of technology, from smartphones and smart TVs to virtual assistants and tablets.

2. Internet

The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). The U.S. Department of Defense laid the foundation of the Internet roughly 30 years ago with a network called ARPANET. But the general public didn't use the Internet much until after the development of the World Wide Web in the early 1990s.
Definition: The Internet is a worldwide network of interconnected computer systems.
Components: The Internet is made up of many smaller networks, including domestic, academic, business, and government networks.
IP address: Each computer on the Internet has a unique IP address, which is a set of numbers.
Services: The World Wide Web is one of the Internet's biggest services.

- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 192.168.1.14) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name **https://www.google.co.in** to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.

3. History of internet

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:

- The origin of Internet devised from the concept of Advanced Research Project Agency Network (ARPANET).
- ARPANET was developed by United States Department of Defense.
- Basic purpose of ARPANET was to provide communication among the various bodies of government.
- Initially, there were only four nodes, formally called Hosts.
- In 1972, the ARPANET spread over the globe with 23 nodes located at different countries and thus became known as Internet.
- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc.,Internet provided a medium to publish and access information over the web.

4. Internet Service Providers

ISP stands for **Internet Service Provider** which is a term used to refer to a company that provides internet access to people who pay the company or subscribe to the company for the same. For their services, the customers have to pay the internet service provider a nominal fee which varies according to the amount of data they actually use or the data plan which they purchase. An Internet Service Provider is also known as an Internet Access Provider or an online service provider. An Internet Service Provider is a must if one wants to connect to the internet.

Characteristics

- **E-mail Account:** Many Internet Service Providers offer an e-mail address to their consumers.
- **User Support:** Professionals and an increasing number of lay users prefer an ISP that can provide them with customer support so that they have someone they can refer to if things go awry.
- **Access to high-speed internet:** Probably the most obvious item on this list as this feature of an Internet Service Provider lies literally in its name.
- **Spam Blocker:** An Internet Service Provider that hinders its customers' productivity by way of not blocking spam and displaying frequent ads is not something that is generally favoured in the market today.
- **Web Hosting:** Some of the ISPs offer web hosting services to their clientele as well.

Different types of ISP connections

- DSL
- Wi-Fi broadband
- mobile broadband
- fibre optic broadband
- cable broadband

List of ISP

- Reliance Jio
- Vodafone Idea
- Airtel
- BSNL

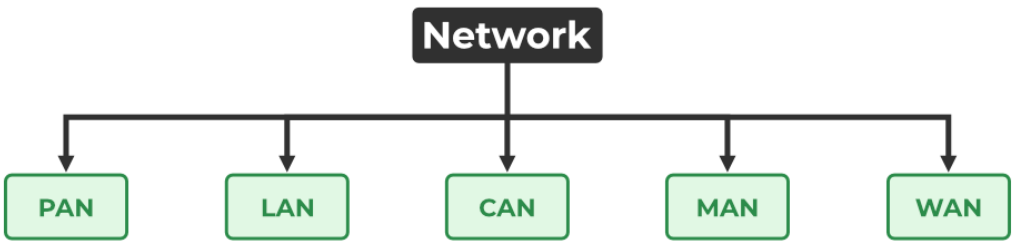
5. Types of Networks

A computer network is a cluster of computers over a shared communication path that works to share resources from one computer to another, provided by or located on the network nodes.

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)

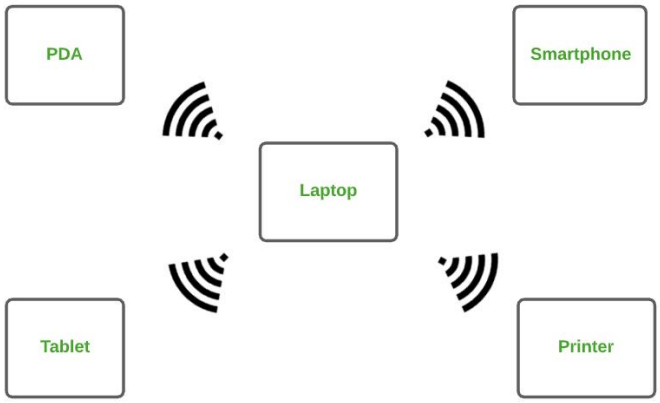


1. Personal Area Network (PAN)

PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centered only on an individual's workspace. 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.

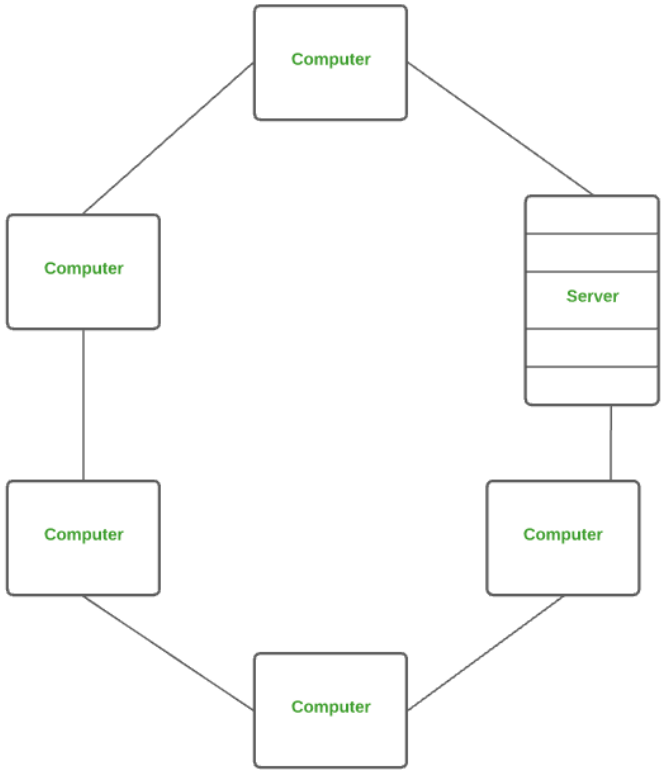
Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.



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.

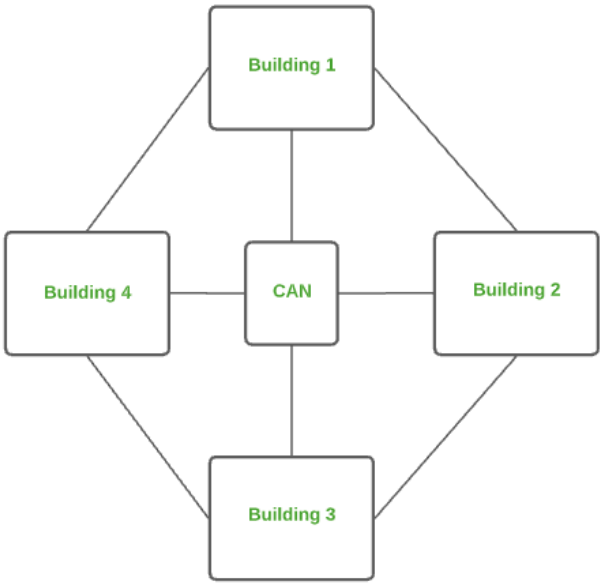
Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



Local Area Network (LAN)

3. Campus Area Network (CAN)

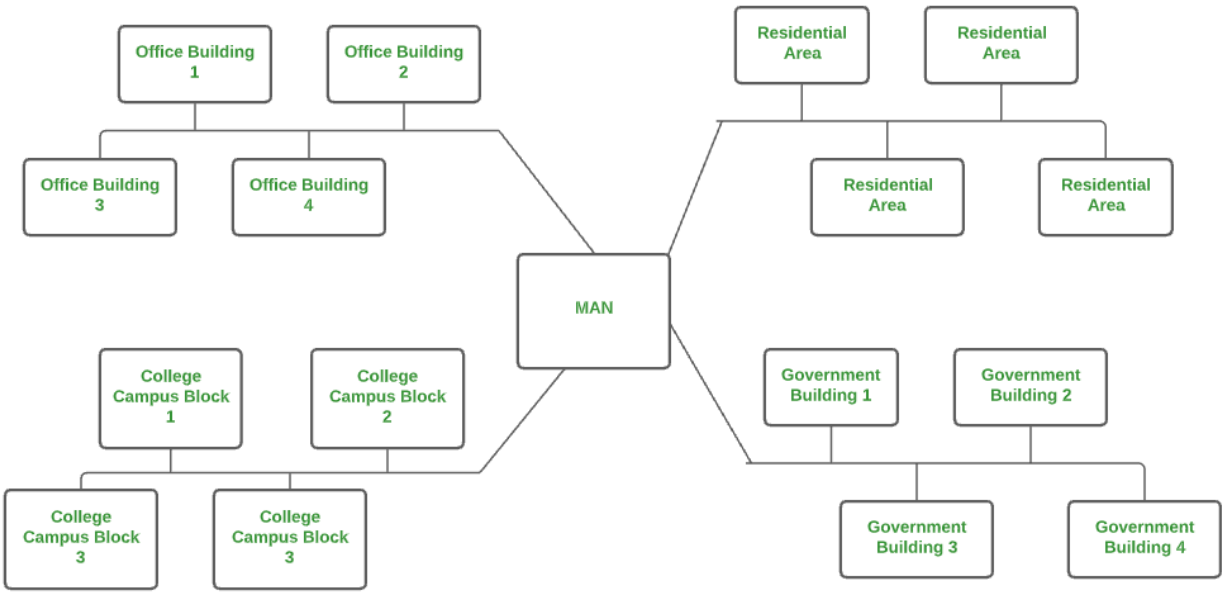
CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range 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)

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.

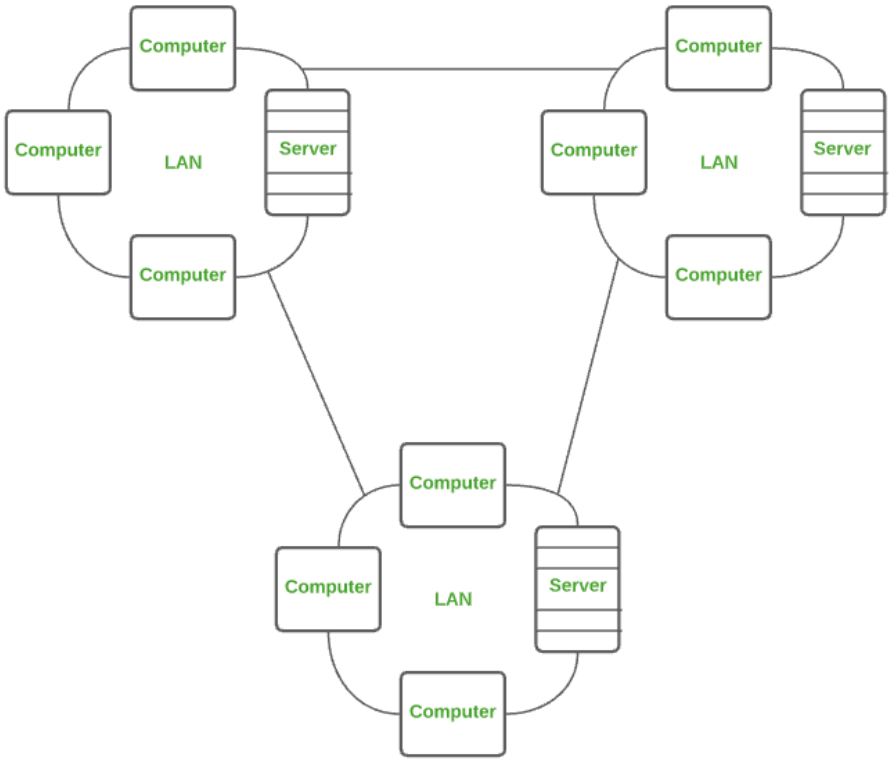


5. Wide Area Network (WAN)

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.



6. IP-Internet Protocol

- P stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.
- An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.
- The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.
- The first major version of the internet protocol was IPv4, which was version 4. This protocol was officially declared in RFC 791 by the Internet Engineering Task Force (IETF) in 1981.
- After IPv4, the second major version of the internet protocol was IPv6, which was version 6. It was officially declared by the IETF in 1998. The main reason behind the development of IPv6 was to replace IPv4. There is a big difference between IPv4 and IPv6 is that IPv4 uses 32 bits for addressing, while IPv6 uses 128 bits for addressing.

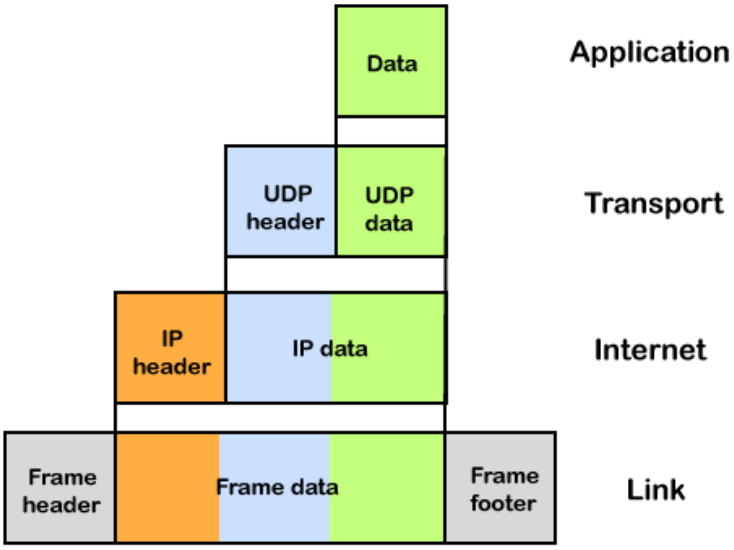
The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more IP networks. In order to achieve these functionalities, internet protocol provides two major things which are given below.

An internet protocol defines two things:

- Format of IP packet
- IP Addressing system

IP packet

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.



An IP header contains lots of information about the IP packet which includes:

- Source IP address: The source is the one who is sending the data.
- Destination IP address: The destination is a host that receives the data from the sender.
- Header length
- Packet length
- TTL (Time to Live): The number of hops occurs before the packet gets discarded.
- Transport protocol: The transport protocol used by the internet protocol, either it can be TCP or UDP.

There is a total of 14 fields exist in the IP header, and one of them is optional.

Payload: Payload is the data that is to be transported.

IP Addressing

An IP address is a unique identifier assigned to the computer which is connected to the internet. Each IP address consists of a series of characters like 192.168.1.2. Users cannot access the domain name of each website with the help of these characters, so DNS resolvers are used that convert the human-readable domain names into a series of characters. Each IP packet contains two addresses, i.e., the IP address of the device, which is sending the packet, and the IP address of the device which is receiving the packet.

7. Domain Name Services

DNS is short for **Domain Name System**. It functions as the internet's version of a phone book, converting difficult-to-remember IP addresses into simple names. Cheaper technology and the introduction of desktop computers in the early 1980s facilitated the rapid development of local area networks (LANs). As the number of machines on the network grew, it became impossible to keep track of all the different IP addresses.

The **development of the Domain Name System (DNS)** in 1983 solved this problem. DNS was invented at the University of Southern California by Paul Mockapetris and Jon Postel. It was one of the breakthrough inventions that helped in paving the way for the World Wide Web.

8. Applications of Internet

Internet Applications are online tools that rely on the internet to fetch, share, and display information from servers, enabling their successful operation. The internet has helped people to learn many things irrespective of the field. There are number.
of application of internet in today's world.

Applications of Internet are:

1. Communication
2. Web Browsing
3. Online Shopping
4. Real-Time Update
5. Social Media
6. Job Search
7. Education
8. Travel
9. Stock Market Update
10. Video Conferencing

1. Communication

Communication refers to exchanging ideas and thoughts between or among people to create understanding. The communication process involves the elements of source, encoding, channel, receiver, decoding, and feedback. In organizations, both formal and informal communications simultaneously take place. Formal communications refer to official communications in orders, notes, circulars, agenda, minutes, etc.

2. Web Browsing

Web Browsing is one of the applications of the internet. A web browser is a program that helps the user to interact with all the data in the WWW (World Wide Web). There are many web browsers present in today's world. Some of them are as follows:

Google Chrome
Firefox
Safari
Internet Explorer
Opera
Microsoft Edge
Netscape

3. Online Shopping

The era of the internet took shopping into a new market concept, where many virtual shops are available 24x7. The shops provide all the necessary details of a product on their website, so the user can choose as per their needs.

4. Real-Time Update

The internet makes things easier. One can quickly get an update on the things happening in real-time in any part of the world. For example, sports, politics, business, finance, etc. The internet is very useful in many decisions based on real-time updates.

5. Social Media

The youth of this generation spend the maximum of their free time on social media, all thanks to the internet. Social media is a place where the user can communicate with anyone, like friends, family, classmates, etc. User can promote their businesses on social media as well. You can also post your thoughts, pictures and videos with your friends on social media.

6. Job Search

The internet has brought a revolution in the field of Jobs. The candidate can search for their dream job, apply and get it very easily. Even companies nowadays post their need on the internet and hire candidates as per their skills based on the job role.

There are many platforms which are primarily doing this. Some of them are listed below.

LinkedIn
Monster.com
Naukari.com
Indeed
Glassdoor

7. Education

The Internet has a vital role in the education field. It became an effective tool in both teaching and learning. Teachers can upload their notes or learning videos on the websites with the help of the internet. It made the learning process more diverse and joyful.

8. Travel

Users can easily search for their favourite tourist places worldwide and plan their trips. One can book holiday trips, cabs, hotels, flight tickets, clubs, etc., with the help of the Internet.

Some websites that provide these facilities are as follows:

goibibo.com
makemytrip.com
olacabs.com

9. Stock Market Update

A stock market update refers to the latest information and news related to the financial markets, particularly the stock market. The stock market is where individuals buy and sell publicly traded company shares.

10. Video Conferencing

Video conferencing means using computers to provide a video link between two or more people. It allows users in different locations to hold face-to-face meetings.

9. Ethical and social implications of compter systems:

There are a number of ethical and social impacts of computer use that have become increasingly relevant as technology has become more integrated into our daily lives. Here are a few examples:

1. **Privacy**: One of the most significant ethical and social impacts of computer use is the issue of privacy. With the proliferation of personal data being collected by companies and governments, there is a growing concern about how this data is being used and who has access to it. This includes issues such as data breaches, online tracking, and government surveillance.
2. **Cybersecurity:** The increasing reliance on computers and digital networks has also led to an increased risk of cyberattacks and hacking. This has serious implications for individuals, businesses, and governments, as sensitive information can be compromised or stolen.
3. **Automation:** As computers and artificial intelligence become more advanced, there is a growing concern about the impact on employment. Many jobs that were once performed

by humans are now being automated, which could lead to unemployment and economic inequality.

4. **Social isolation:** Another potential social impact of computer use is the risk of social isolation. As people spend more time online and less time interacting with others in person, there is a risk of social disconnection and a loss of important social skills.
5. **Bias and discrimination:** Finally, there is a concern about the potential for bias and discrimination in computer algorithms and decision-making processes. If these systems are not designed and implemented fairly, they could perpetuate existing biases and inequalities in society.

10. Network and Security Concepts

10.1 Information Assurance Fundamentals

COMPUTER SECURITY

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

There are three key concepts, known as the **CIA triad**, which anyone who protects an information system must understand**: confidentiality, integrity, and availability**. Information security professionals are dedicated to ensuring the protection of these principals for each system they protect.

Additionally, there are three key concepts that security professionals must understand to enforce the CIA principles properly: **authentication, authorization, and nonrepudiation**.

Confidentiality:

- Information is only available to authorized users.
- Definition: "assurance that information is not disclosed to unauthorized individuals, processes, or devices."
- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.

Integrity:

- Information is accurate and complete.
- Definition: Quality of an IS (Information System) reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software

implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

- Guarding against improper information modification or destruction,including ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

Availability:

- Authorized users have access to information when they need it.
- Definition: "timely, reliable access to data and information services for authorized users."
- Ensuring timely and reliable access to and use of information.
- A loss of availability is the disruption of access to or use of information or an information system.

Authentication

- Authentication is important to any secure system, as it is the key to verifying the source of a message or that an individual is whom he or she claims.
- The NIAG defines authentication as a "security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information."
- There are many methods available to authenticate a person. In each method, the authenticator issues a challenge that a person must answer. This challenge normally comprises requesting a piece of information that only authentic users can supply.

Authorization

- While authentication relates to verifying identities, authorization focuses on determining what a user has permission to do.
- The NIAG defines authorization as "access privileges granted to a user, program, or process."
- After a secure system authenticates users, it must also decide what privileges they have. For instance, an online banking application will authenticate a user based on his or her credentials, but it must then determine the accounts to which that user has access.
- Additionally, the system determines what actions the user can take regarding those accounts, such as viewing balances and making transfers.

Nonrepudiation

- Non-repudiation is a legal concept that ensures the legitimacy of a data transfer or message. It provides evidence of both integrity and authenticity.
- The NIAG defines Nonrepudiation as "assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data."

10.2 Cryptography-Symmetric and Asymmetric

Cryptography

- The English word cryptography derives from Greek and its meaning is "hidden writing."
- 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 remains important to protecting data and users, ensuring confidentiality, and preventing cyber criminals from intercepting sensitive corporate information.

Basic terminology of cryptography

Crypt analysis

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code."

Cryptology

The areas of cryptography and cryptanalysis together are called cryptology

Cipher

Encryption scheme is known as a cryptographic system or a cipher

Plain Text

This is the original intelligible message or data that is fed into the algorithm as input.

Cipher Text

This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.

Secret key

The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

Encryption

The process of converting from plaintext to cipher text

Decryption

The process of restoring the plaintext from the cipher text

Enciphering Algorithm

The encryption algorithm performs various substitutions and transformations on the plaintext

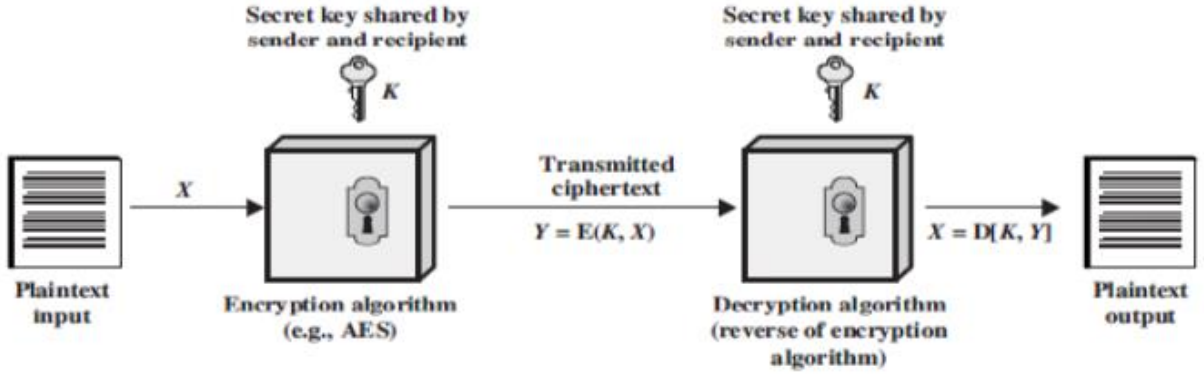
Deciphering Algorithm

This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

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

1. **Symmetric Key Cryptography or private 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.

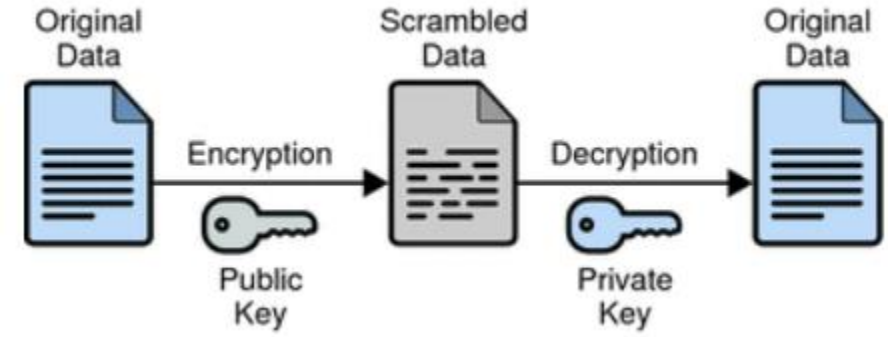


- A symmetric encryption scheme has five ingredients. They are Plain Text, Encryption Algorithm, Secret Key, Decryption Algorithm, Cipher Text
- There are two requirements for secure use of conventional encryption:

- We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more cipher texts would be unable to decipher the cipher text or figure out the key.
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.
- The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).

2. <u>Asymmetric Key Cryptography or public key cryptography:</u>

- Public key cryptography is a method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use.
- The other key is known as the private key.
- Data encrypted with the public key can only be decrypted with the private key.
- 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 knows his private key.
- The most popular asymmetric key cryptography algorithm is RSA algorithm.

11. <u>Malwares</u>

- **Malware** means **malicious software** and refers to any software that is designed to cause harm to computer systems, networks, or users.
- Malware is a program designed to gain access to computer systems, generally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious programs.

<u>Types of Malware</u>

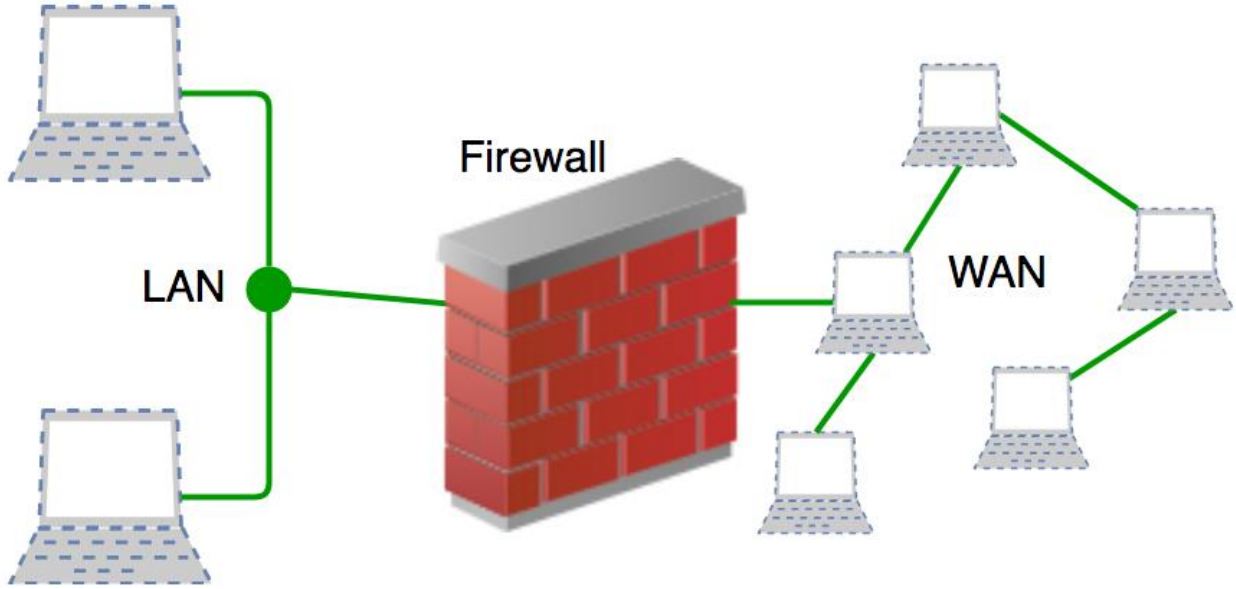
1. **Viruses –** A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.
2. **Worms –** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
3. **Trojan horse –** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.
4. **Ransomware** – Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key that is

unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system

5. **Adware** – It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.
6. **Spyware** – Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.
7. **Logic Bombs –** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.
8. **Rootkits –** A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
9. **Backdoors** – A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.
10. **Keyloggers –** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

12. Firewalls

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic. **Accept :** allow the traffic **Reject :** block the traffic but reply with an "unreachable error" **Drop :** block the traffic with no reply A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



Types of Firewalls

1. Packet Filtering Firewall

One of the oldest types of Firewall

This type of Firewall creates a checkpoint at the traffic router. Only the secure and verified IP address or networks are allowed for the further flow of data

The data packets are not verified, i.e. the information or data is not opened at the Firewall stage

They are easy to use and do not overload the device and do not affect its processing or functioning speed

2. Application Level Gateway Firewall
It is also known as Proxy Firewall
When the user connects with the destination server, it forms a connection with the application gateway
The proxy then connects with the destination server and takes up the decision of forwarding the data packets
It is a bit more secure in comparison to Packet Filtering Firewall
Strong Memory and processors are required for using this Firewall
3. Circuit Level Gateway Firewall
This works as the Sessions layer of the OSI Model
Using this, two Transmission Control Protocol (TCP) connections can be set up together
It can easily let the flow of data packets continue without consuming major computer resources
These Firewalls are not much efficient as they do not check the data packets and incase a data packet comprises malware, it will allow it to pass if the TCP connections are successfully done
4. Stateful Inspection Firewall
It is a combination of data packet inspection and TCP connection. Until both the fields are verified, the information cannot be approved
They are less straining for the computer resources
However, they are a bit slow in comparison to other Firewalls
5. Next-Generation Firewall

The recently launched Firewall systems are known as the Next-Gen Firewalls
Under this, the data packets are also thoroughly checked before being passed on to the destination address
These are still on the platform of improving and evolving and intend to use modern technology for automatic detection of errors and network safety
6. Software Firewall
Any firewall which is installed in a local device or a cloud server is called a Software Firewall
They can be the most beneficial in terms of restricting the number of networks being connected to a single device and control the in-flow and out-flow of data packets
Software Firewall also time-consuming
7. Hardware Firewall
They are also known as Physical-appliance based firewalls
It ensures that the malicious data is stopped before it reaches the endpoint of the network at risk

13. Fraud Techniques

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.

Phishing, Smishing, Vishing, and Mobile Malicious Code
Many phishing attacks against mobile devices use short message service (SMS, or smishing) and voice-over Internet protocol (VoIP, or vishing) to distribute lures and collect personal information.
Phishing by way of mobile phones introduces new challenges for attackers and administrators alike. Many phishing attacks against mobile devices use SMS (smishing) and VoIP (vishing). Attackers often send fraudulent SMS messages to many users attempting to gain private information or distribute malicious files. The messages include a URL or a phone number with themes similar to those of traditional phishing messages. Upon calling a phone number, the user may interact with an actual person or a voicemail system—both of which are risks to the user's personal information.
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.

Denial of service (DoS):
Interrupting access of traffic to an online service, system, or network to cause malicious intent.
Malware:
The use of malicious software to damage or disable users' devices or steal personal and sensitive data.
Ransomware:
It is 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.
Business email compromise (BEC):
It is 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.

14. Privacy and data protection

Privacy and data protection are two related internet governance issues. Data protection is a legal mechanism that ensures privacy. Data privacy is the right to control who can see your personal information.

Techniques to protect your data

- Encryption: Hide sensitive data using a cipher protected by an encryption key.
- Access controls: Allow or deny access to data based on predefined criteria.
- Backup and disaster recovery planning: Regularly assess and update security measures.
- Physical security: Protect your device when it's unattended.
- Use Strong passwords
- Use Multi-factor authentication
- Use Anti-virus and malware protection
- Being aware of your surroundings
- Being wary of suspicious emails
- Using free wi-fi with caution
- Watching out for links and attachments
- Checking to see if the site is secure