Toppersnotes®
Unleash the topper in you

Rajasthan – CET

Graduate Level

Common Eligibility Test (CET)

Volume - 6

General Science & Computer

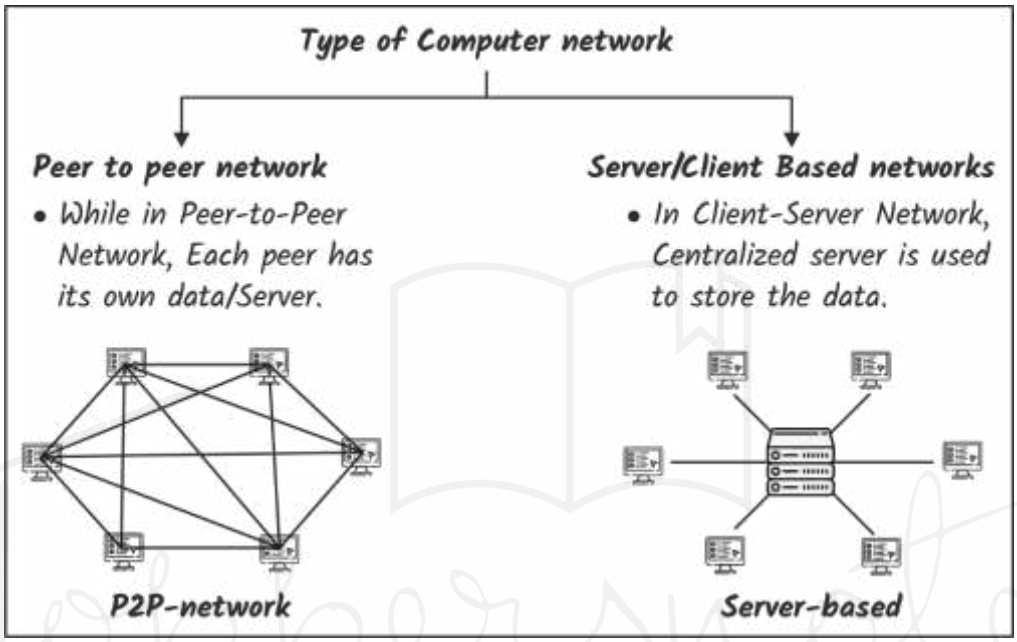
SIERRA INNOVATIONS

INDEX

1 CHAPTER ICT

Computer Network

Computer networks are formed when two or more computers are interconnected to exchange information and resources, enabling communication and collaboration across various distances and scales.



Types of Computer Networks based on the Area/Extent of Coverage

1) **LAN (Local Area Network):** Network used to interconnect computers from a certain and small geographical area (up to about 1 km). e.g. Ethernet.
2) **MAN (Metropolitan Area Network):** Network used to interconnect computers from a big geographical area (up to about 100 km) e.g. City
3) **WAN (Wide Area Network):** WAN connects computers together across longer physical distances such as country, continent and world e.g. Internet
4) WLAN (Wireless Local Area Network): WLAN is also known as LAWN (Local Area Wireless Network).
5) HAN (Home Area Network): Suitable network for connecting computers used in a home.

Network Topology

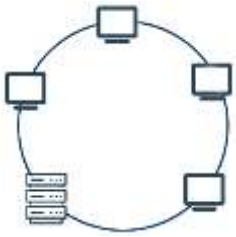
- The medium by which computers are connected to each other in a computer network is called network topology.

(a) Bus Topology-

In this type of topology, computers are connected to each other in a line through a central cable.

(b) Ring Topology-

- ✓ In this type of topology, computers are connected to each other in a circular manner through a cable.

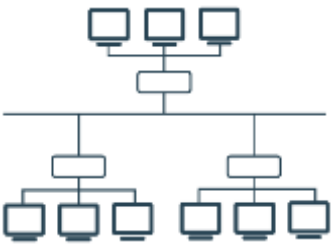


(c) Star Topology-

- ✓ In this type of topology, computers are connected through a central device called a hub.

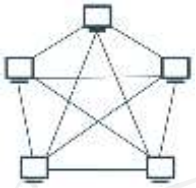
(d) Tree Topology-

- ✓ In this type of topology, computers are connected to each other at different levels.



(e) Mesh Topology-

- ✓ This type of topology is used in geometry.
- ✓ This topology works to transfer data at the fastest speed.



Networking Devices

- ➢ In a computer network, a hardware is used to connect two or more computers together, which is called a networking device.
- ➢ Different networking devices are used in the computer depending on the network. As -

(i) **Switch** – This device is used in a local area network (LAN) , which also provides security.

- ✓ Computers, servers and printers are shared through switches.

(ii) **Hub (HUB)** - It is also used in LAN , but it does not provide security like a switch , rather it provides the same data equally to all types of computers connected to the network.

(iii) **Bridge (Bridge)** - This device is used to connect two similar LANs.

(iv) **Gateway** - This device is used to connect two different LANs

(v) **Router** – This device is used to connect different computers over the Internet or WAN.

(vi) **Repeater (Repeater)** - This device is used to speed up the data process by dividing the weak signal coming through the network into many signals.

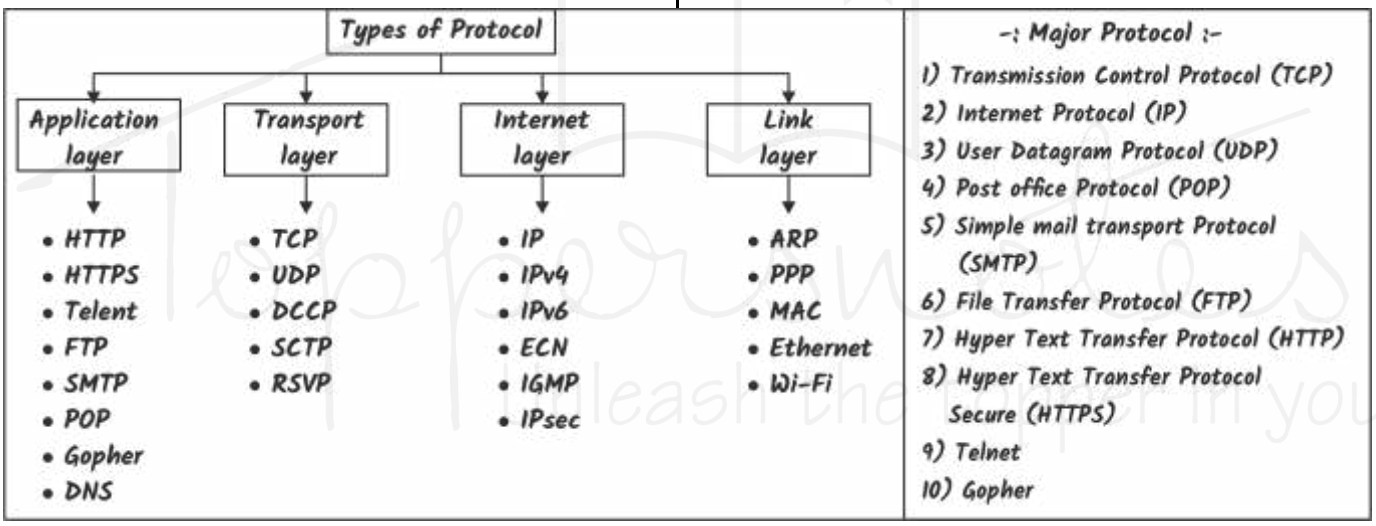
(vii) **MODEM** - It is a telecommunication device , which is used to convert digital data to analog and analog data to digital in the network.

Internet

- The Internet is a complex network of computers connected by high-speed communication technologies, with no single person or government owning it, making it a free and open resource.
- The Internet originated from ARPANET, a project funded by the U.S. Department of Defense in the late 1960s. It expanded through the 1980s and 1990s, becoming a global network of interconnected computers facilitating the exchange of information and communication worldwide.

Internet Protocol

- The Internet protocol is the set of communications protocols used in the Internet and similar computer networks. It is commonly known as TCP/IP {Transmission Control Protocol (TCP) and the Internet Protocol (IP)}.
- The Internet protocol provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received.
- Internet Protocol consists of four Communication Protocols Layers (Link Layer, Internet layer, Transport Layer, Application Layer).



Some Important Protocols

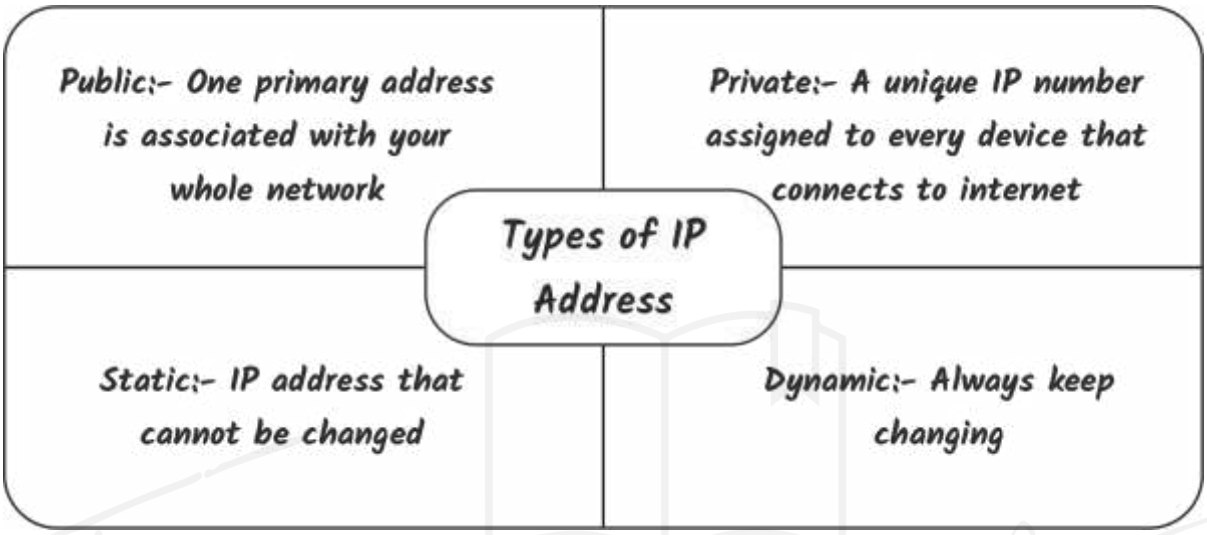
TCP

- TCP divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
- It performs its function together with the IP, which assigns a unique name (IP Address) to each computer. Therefore it is also called TCP / IP

Internet Protocol (IP)

- A unique address for device connected to the Internet. This special address is provided by the Internet Service Provider when connected to the Internet. Two computers can not have same IP address.

IPv4	IPv6
➢ IPv4 is the most used Internet Protocol developed in 1970. ➢ Each group is separated by a dot (.). ➢ Splitting the IP address in a 32-bit Format (4 bytes). ➢ Each three-number group can be given a number between 0-255.	➢ Developed in 1998. ➢ It splits the IP address in 128-bit Format (16 bytes). ➢ Each group is separated by a colon (:).



FTP – File Transfer Protocol

- This protocol is used to transfer files from one system to another, for which a particular software (called client) is used.
- Through this, simple text files from multimedia can be uploaded and downloaded easily and fast

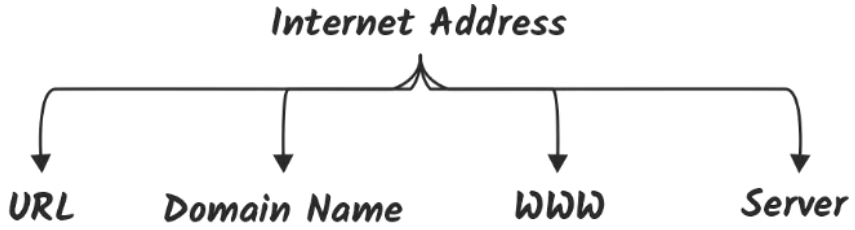
Simple mail transfer Protocol (SMTP)

- SMTP is a popular email protocol that is used to send email. This protocol prescribes rules for sending email from one computer to another.

HTTP – Hyper Text Transfer Protocol

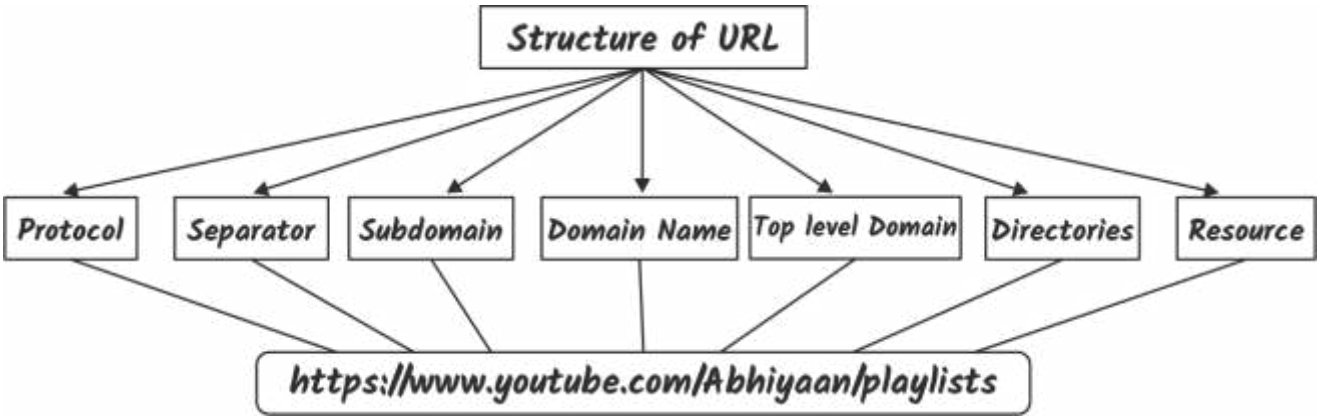
- HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting hypertext documents, such as web pages, over the Internet. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands.

Internet Address



URL

- Every web page that is displayed on the Internet has a specific address associated with it. This address is known as the URL. It tells us the location of the web page being displayed and other related information.



- **Protocol**:

  It is used to transfer data over the web. HTTPS is the most popular web protocol. Before HTTPS the HTTP - hypertext transfer protocol was used. Apart from HTTPS, ftp, mailto, telnet, news etc. is also standard protocol.

Separator:

- These are special signs that act to separate the parts of the URL from each other.

Domain Names

- Domain name is the name of a website. This is the nickname of IP Address. The domain name system converts the IP address to a domain name made up of words. Domain name can contain a maximum of 64 characters.

- Domain Name Service: A database that contains the names (Domain Names) and address of various hosts on internet.

www/ World Wide Web

- The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://example.com/), which may be interlinked by hypertext, and are accessible over the Internet.

Server

- A server is a type of data storage device by which information or data is provided to a client i.e. a computer and other devices connected to the Internet.

Our computer is a host computer because it can collect information from all servers.

Types of Servers and Their Applications

1. **Application Server:** Hosts web apps, allowing network users to run and use them without installation.

2. **Catalog Server:** Maintains indexes of distributed network information for easy retrieval.
3. **Communication Server:** Facilitates communication between endpoints within a network.
4. **Computing Server:** Shares extensive computing resources like CPU and RAM over a network.
5. **Database Server:** Maintains and shares databases, serving programs that require well-organized data.
6. **Fax Server:** Shares fax machines over a network for easy access by fax senders and recipients.
7. **File Server:** Shares files, folders, and storage space over a network to networked computers.
8. **Game Server:** Enables multiplayer gaming for PCs and gaming consoles.
9. **Mail Server:** Facilitates email communication, serving senders and recipients of emails.
10. **Print Server:** Shares printers over a network for convenient access by networked computers.
11. **Proxy Server:** Acts as an intermediary, controlling content, improving traffic performance, and securing network access.
12. **Web Server:** Hosts web pages, making the World Wide Web accessible to web browsers.

Major Types of Internet connections

There can be 4 major types of Internet connections.

1). Dial Up connections

2). Broadband connections.

3). Wireless connections.

4). Integrated Services Digital Netwrork

Dial Up connections- Dial-up connections are a connection between two devices using standard telephone service.

Broadband Connection- The full form of Boradband is broad bandwidth. It is a high-speed Internet connection using wide band frequencies. Coaxial cable, optical fiber, twisted pair are used to use broadband connections.

- Digital Subscriber Line: It is a popular broadband connection, using copper wires. It works like a dial service but at a much faster speed, requiring a DSL modem.
- Cabel Modem: Under this, cable operators can provide internet etc. facilities through coaxial. Its transmission speed can be 1.5Mbps or even more.
- Fiber Optics: In which the information is sent from one place to another through optical fiber in the form of light points.

Wireless Connection- Wireless connection is a type of broadband in which internet facilities are provided with the help of radio frequencies without wires.

Modes of wireless connection can be Wi-Fi, LiFi, Satellite internet connection.

WiFi (Wireless Fidelity)

- It is **a wireless-based transmission of Internet signals** in the form of a radio wave.
- It works at **spot frequency of 2.4 or 5 GHz** at a **high speed of 11 million bits per second** within a **range of 100 meters.**
- This is **used in home networks, mobile phones, video games** and other electronic devices.
- **Working : Operates** via **3 essential elements**
  - ✓ Radio waves,
  - ✓ Antenna,
  - ✓ Router.
- **The Radio Waves** - key **to make Wi-Fi networking possible.**

Elements of Wi-Fi :

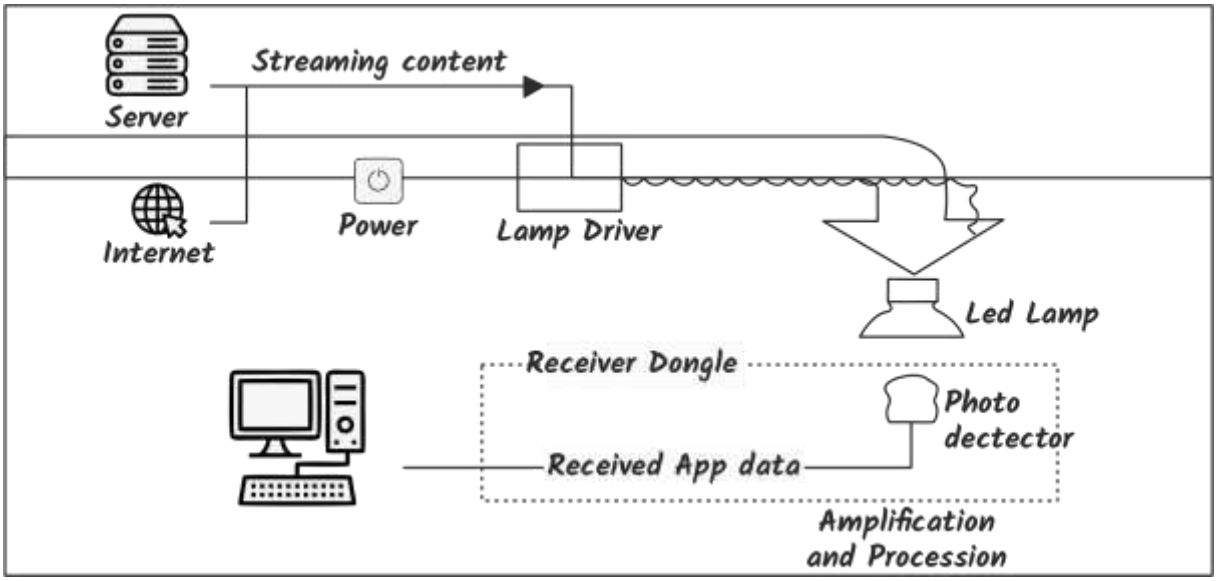
- **Wireless Access Point :**
  - ✓ Used **to allow wireless devices for connecting** to the wireless network.
- **WiFi Cards :**
  - ✓ **Allows the wireless signal & information** of the relay(can be internal or external).
  - ✓ Wifi cards are **also known as adapters.**
- **Safeguards :**
  - ✓ **A Firewalls - protect networks** like antivirus software's **from uninvited users** and keeps the information secure.

Wi-fi generations

Generation/IEEE Standard	Maximum Linkrate	Adopted	Frequency
Wi-Fi 6 (802.11ax)	600-9608 Mbit/s	2019	2.4/5 GHz 1-6 GHz ISM
Wi-Fi 5 (802.11ac)	433-6922 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72-600 Mbit/s	2009	2.4/5 GHz
Wi-Fi 3 (802.11g)	3-54 Mbit/s	2003	2.4 GHz
Wi-Fi 2 (802.11a)	1.5 to 54 Mbit/s	1999	5 GHz
Wi-Fi 1 (802.11b)	1 to 11 Mbit/s	1999	2.4 GHz

Li-Fi (Light Fidelity)

- A technology which **utilizes light to transmit data and position between devices.**
- It is **capable of transmitting data at high speeds** over the **visible light, ultraviolet, and infrared spectrums.**



Working

- An **ordinary LED bulb is connected to a device**, which in turn is connected to the Internet.
- The **Internet data flows in** from the **device to the bulb** and is **carried by light waves.**
- **Light waves** carrying the Internet data **fall on a receiver or a dongle** that is connected to the computer.

Internet Terminology

- **Web Browser** - A web browser is a software application that enables users to access, navigate, and interact with websites by retrieving, presenting, and transferring information over the Internet. Key features include displaying web pages, managing bookmarks, and supporting extensions; notable browsers are Chrome, Firefox, Safari, Edge, and Opera.
- **Web Server-** A web server is a software or hardware system that hosts websites, delivering web pages and content to users' browsers over the Internet. It handles HTTP requests, serves static and dynamic content, and supports features like security, load balancing, and logging; prominent web servers include Apache, Nginx, Microsoft IIS, and Lite Speed.
- **Search Engine**- A search engine is a software system designed to search for information on the Internet, indexing web pages, and delivering relevant results based on user queries. It features web crawling, indexing, and ranking algorithms; major search engines include Google, Bing, Yahoo, and DuckDuckGo.
- **E-mail-** Email is a digital communication method that allows users to send and receive messages over the Internet, featuring functionalities like attachments, address books, and folders for organization. Key email services include Gmail, Outlook, Yahoo Mail, and Proton Mail.

Social Networking Sites

- It is a form of electronic communication through which users share information, ideas, personal messages, videos and pictures and other content through it instantly. Example :- Facebook twitter etc.
- A social network can be represented as Graph and Tree.

Types of social networking sites

- Social Networks – Services that allow you to connect with other people of similar interests and background. Such as Facebook and LinkedIn.
- Bookmarking Sites – Services that allow you to save, organize and manage links to various websites and resources around the internet. Such as Delicious and Stumble Upon.
- Social News :- Services that allow people to post various news items or links to outside articles and then allows its users to "vote" on the items Such as Digg & Reddit.
- Media Sharing :- Services that allow you to upload and share various media such as pictures & videos such as YouTube, Instagram and Flickr.
- Microblogging :- Services that focus on short updates that are pushed out to anyone subscribed to receive the updates. The most popular is Twitter.

Positive Impacts of social media

- **Global Connectivity**: Social media connects people globally, transforming communication and fostering relationships across borders.
- **Voice for the Marginalized**: It amplifies the voices of marginalized groups, enabling them to express their views and reach a wider audience.
- **Business Growth**: Social Media Optimisation (SMO) helps businesses grow by optimizing their presence, increasing visibility, and targeting the right audience through online publicity.
- **Job Creation**: Social media has created new job opportunities in digital marketing, content creation, and social media management.
- **Information and Awareness**: It spreads important information and raises awareness on various social issues, empowering global communities.

Negative Impacts of Social Media

- **Mental Health Issues**: Excessive use of social media can negatively affect mental health, leading to depression and emotional distress.
- **Cyberbullying:** Social media platforms can encourage harmful behaviors like cyberbullying, affecting individuals' well-being.
- **Spread of Fake News and Hate Speech:** Social media plays a key role in the rapid spread of misinformation and hate speech, influencing public opinion.
- **Privacy Concerns:** Social media platforms often lack adequate privacy measures, putting user data at risk.

- **Increase in Cyber Crimes:** The risk of cybercrimes, such as hacking and phishing, is heightened due to vulnerabilities in social media platforms.
- **Legal and Regulatory Challenges:** Social media faces challenges related to regulations on fake news, privacy, and content removal, with varying laws in place across countries.

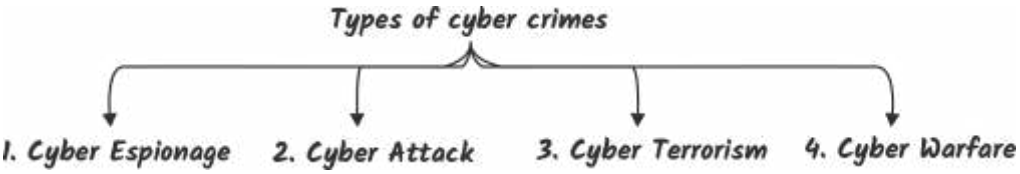
Cyber Security

- **Cyber Space:** Cyberspace refers to the virtual environment of computer networks, including the internet, where communication, data exchange, and information processing take place. It encompasses all the interconnected digital systems and networks that allow users to interact globally. E.g. Internet.
- **Cybercrime:** Cybercrime refers to criminal activities that involve computers, networks, or the internet. These activities can include hacking, identity theft, online fraud, cyberbullying, and data breaches.
- **Cyber security**: Cybersecurity refers to the practices, technologies, and processes designed to protect computers, networks, and data from unauthorized access, attacks, or damage. It aims to safeguard systems from cyber threats like viruses, hackers, and other malicious activities.

Features of Cyber security:

- **Compliance:** Ensures adherence to legal, regulatory, and industry standards like GDPR and HIPAA to protect data privacy.
- **Defense Against Internal Threats:** Protects systems from internal threats, including insider attacks, by controlling user access and monitoring activities.
- **Threat Prevention:** Proactively detects and prevents cyber threats using firewalls, encryption, antivirus software, and system updates.
- **Data Integrity:** Ensures data is accurate, reliable, and unaltered, even during transmission.
- **Incident Response**: Involves a structured approach to respond to and recover from cyberattacks, minimizing damage and downtime.
- **Risk Management:** Identifies, assesses, and mitigates cybersecurity risks to maintain the integrity of networks and systems.
- **Continuous Monitoring:** Ongoing surveillance of systems to detect potential security breaches or vulnerabilities in real-time.

Types of Cyber crimes



- **Cyber Espionage:** Cyber espionage involves the use of digital tools and techniques to gain unauthorized access to confidential data or intelligence for political, military, or economic advantage.
- **Cyber Attack**: A cyber attack is any offensive action aimed at compromising the functionality, integrity, or confidentiality of a computer system or network. It can include hacking, denial of service (DoS) attacks, or data breaches.
- **Cyber Terrorism**: Cyber terrorism refers to the use of digital platforms and tools to carry out attacks that cause widespread fear, disrupt critical infrastructure, or harm society in a manner similar to traditional terrorism.
- **Cyber Warfare**: Cyber warfare involves state-sponsored or large-scale cyber attacks targeting a nation's critical infrastructure, military systems, or other key assets to cause damage, disrupt operations, or gain strategic advantages during conflicts.

Tools of Cyber Crime

- **Hacking:** Hacking refers to the act of gaining unauthorized access to computer systems, networks, or digital devices to manipulate, steal, or alter data, often exploiting security vulnerabilities. While hacking can be used for malicious purposes (black hat hacking), it can also be employed ethically (white hat hacking) to improve system security.

Types of Hackers

- **Black Hat:** Hackers who exploit security vulnerabilities for malicious purposes, such as stealing data, creating malware, or causing damage to systems.
- **White Hat (Ethical Hacker)**: Hackers who use their skills to identify and fix security vulnerabilities in systems to improve security, typically working with organizations to safeguard their networks.
- **Grey Hat**: Hackers who fall between black and white hats; they may break into systems without malicious intent, but often without permission, and may report vulnerabilities or use them for personal gain.
- **Script Kiddie:** Inexperienced hackers who use pre-written scripts or tools created by others to carry out attacks, typically lacking the skills to write their own code.
- **Hacktivist:** Hackers who use hacking techniques to promote political or social causes, often targeting government websites or corporations to make a statement.
- **Red Hat:** Hackers who target black hats by disrupting their operations, often with aggressive tactics, including denial-of-service attacks or hacking back.

- **Blue Hat:** Hackers who are hired by organizations to test systems for vulnerabilities, but unlike white hats, they might not have formal security training.
- **Phreaker:** Hackers who specialize in manipulating telecommunication systems, especially to bypass charges or gain unauthorized access to phone networks.

Hacking Glossary

- **Adware** – Adware is software that is designed to force pre-chosen ads to be displayed on the screen.
- **Attack** – This is an action performed on a system to gain access to it and extract sensitive data.
- **Backdoor** – This back door or trap door is a hidden entry into a computing device or software that helps bypass all security measures such as logins and password protections.
- **Bot** – A Bot is a program that helps to automate an action by performing it repeatedly at a higher rate and without error than is possible for a human operator, that too for a much longer period of time. For example sending HTTP, FTP or Telnet at a higher rate and calling scripts through which it creates objects at a higher rate.
- **Botnet**– Botnet is also called Zombie army. It is a group of computers which is used without the knowledge of the owner. Botnets are used to send spam or to carry out denial of service attacks.
- **Brute force attack** – A brute force attack is automated and is the simplest method to gain access to a system or website. It repeatedly tries different combinations of usernames and passwords until it finds the right combination.
- **Buffer Overflow** – Buffer Overflow is a type of flow that occurs when more data is written into a block of memory or buffer. In this, the buffer is instructed to hold more than the allocated space.
- **Clone Phishing** – Clone Phishing is a type of modification of an existing, legitimate email with a false link to trick the recipient into giving away all their personal information.
- **Denial of Service Attack (DoS)** – A Denial of Service (DoS) attack is when a malicious attempt makes a server or a network resource available for a period of time that was previously unavailable to users. Usually, this involves temporarily interrupting or suspending the services that are connected to the host.
- **DDoS** – This is a Distributed denial of service attack.
- **Firewall** – A Firewall is a type of filter designed to keep unwanted intruders out of your computer system or network, thus providing safe communication between systems and users within a firewall.

- **Keystroke logging** – Keystroke logging is the process of tracking the keys that are pressed in a computer. It is simply a map of the computer/human interface. It is used by grey and black hat hackers to record login IDs and passwords. Keyloggers are often secretly installed on a device, using a Trojan to phish e-mail.
- **Logic bomb** – This is a virus that is secretly inserted into the system and is triggered when certain conditions are met. This is the most common version of the time bomb.
- **Malware** – Malware is an umbrella term used to refer to many types of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware and other malicious programs.
- **Master Program** – A master program is a program used by black hat hackers to remotely transmit commands to activate infected zombie drones. It is also used to carry out denial of service attacks or spam attacks.
- **Phishing** – Phishing is a type of e-mail fraud method in which the sender sends e-mails that look exactly like legitimate-looking e-mails with the main goal of gathering personal and financial information from recipients.
- **Phreaker** – Phreakers are often considered the original computer hackers, as they illegally break into telephone networks and use them to make free long-distance phone calls or to tap people's calls.
- **Rootkit** – Rootkit is a type of stealthy type of software which is typically malicious and is designed in such a way that it is not detected by common security software and can carry out its work.
- **Shrink Wrap Code** – A Shrink Wrap Code Attack is an act used to exploit holes in unpatched and poorly configured software.
- **Social engineering** – Social engineering means deliberately misleading people so that they give you all their details. Such as personal information like credit card details, user names and passwords etc.
- **Spam** – Spam is simply unsolicited e-mail, also known as junk email, which is sent to many recipients against their will.
- **Spoofing** – Spoofing is a technique used to gain unauthorized access to other people's computers. Here, the intruder sends messages to the computer that contain an IP address, making it appear as if the message has come from a trusted host.
- **Spyware** – Spyware is a software which is mainly used to gather information of a person or company, but in this the target has no clue about this and he/she provides all the information even if he/she doesn't want to.
- **SQL Injection** – SQL injection is a type of SQL code injection technique designed to attack data-driven applications. Here malicious SQL statements are inserted into the entry field for execution (for example dumping the contents of a database to the attackers).

- **Threat** – Threat is a possible danger that can exploit a bug or vulnerability that can compromise any computer and network system.
- **Trojan** – A Trojan or Trojan Horse is a type of malicious program that appears like a valid program but is disguised so that it is not easy to distinguish it from a program but is specifically designed to destroy files, alter information, steal passwords, etc.
- **Vulnerability** – Vulnerability is a type of weakness that allows hackers to compromise the security of a computer or network system. **Worm** – Worm is a type of self-replicating virus that can alter files, but it is present within the active memory and keeps duplicating itself.
- **Cross Site Scripting** – Cross Site Scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into a web page that is then viewed by the user.
- **Zombie Drone** – Zombie Drones are hi-jacked computers that can be anonymously used by a soldier or 'drone' for malicious activity. For example, distributing unwanted spam e-mails.

Computer Virus

- The full form of VIRUS is Vital Information Resources Under Siege. Viruses are small programs in the computer. These are auto execute programs which enter the computer and affect the working system of the computer, they are called viruses.
- Virus is a malicious program which damages the computer's data.
- It works to erase or damage computer data. Virus is a program written intentionally.
- It attaches itself to the boot of the computer and the more the computer boots, the more the virus spreads.
- The virus slows down the speed of the hard disk by entering the boot sector of the hard disk. It can also prevent programs from running.
- Many viruses can damage data and programs even after a long time. The virus attached to any program does not become active until the program is run.
- When the virus becomes active, it attaches itself to the computer memory and starts spreading.
- Computer virus is a type of electronic code which is used to destroy the information contained in the computer.
- The word virus was first used by Fred Cohen, a student at the University of California, in his research paper.
- It is maliciously transmitted through a telephone line into a computer program.
- This code can provide wrong information, destroy collected information and if a computer is connected to a network, then due to being electronically connected, this virus can affect the entire network.
- These can remain in the computer for months or years without being detected and can cause damage to it.

- Some major computer viruses are - Michelangelo, Dark Avenger, Kilo, Philip, McMug, Scores, Cascade, Jerusalem, Data Crime, Columbus Crime, Internet Virus PatchCOM, Patch EXE, COM-EXE, Marijuana, Melissa, Anna Kournikova, My Doom, Poison Ivy, Sea Brain, Bloody, Chez Mungu and Desi.
- Some famous viruses that have infected computers on a large scale in the recent past are -

(i) michelangelo (Michelangelo) ,

- ✓ The most infamous virus till date is the Michelangelo virus. It got this name because March 6 is Michelangelo's birth date, on this day it destroys data. That is why it is also called the "March 6 virus"

(ii) Disc Washer ,

- ✓ The Disk Washer virus got its name due to the message "Disk Washer with Love" contained inside it. It was detected in India in the last months of 1993.
- ✓ This virus was so dangerous that it destroyed all the data available in the hard disk.

(iii) C-Brain (C-Brain) ,

- ✓ This virus was developed by two Pakistani brothers, Amjad and Basit, in January 1986.
- ✓ Its purpose was to discourage people from purchasing software illegally. It is considered to be possibly the world's first virus.

(iv) **McMag (Macmag)**

- ✓ This virus would end by giving a peace message on your monitor.
- ✓ It only infected Apple Macintosh computers.
- ✓ Richard Brando is considered to be the originator of this virus.
- ✓ Richard McMag was the publisher of the magazine and the virus was named after the magazine.

(v) **Jerusalem (Jerusalem) ,**

- ✓ The virus was first discovered at Havreyu University, Jerusalem around 1987, hence the name Jerusalem.
- ✓ One special thing about it was that it was active only on Fridays.

(vi) columbus (Columbus)

- ✓ Columbus virus is also known as Datacrime and 13 October. It was named after 13 October because it was activated on infected computers all over the world on 13 October 1989.
- ✓ Like Jerusalem, it also infects executable files and destroys data on the hard disk.
- ✓ The first computer virus discovered in India was C-Brain, which appeared in Madras (Chennai) in 1988.

(vii) Ransomware

- ✓ Ransomware is a computer program that enters your computer without your permission.
- ✓ This came to light in May 2017.
- ✓ He locks all the information present in the computer and tells you that if you deposit a ransom amount of 300 to 600 dollars in Bitcoin then he will give you the key to the lock.

- ✓ *If you pay the ransom then they give you access and you can access the data. If you do not pay the ransom then that data goes out of your hands forever.*

Steps to avoid Cyber crime

- ***Keep Software Updated:*** *Ensure that Microsoft Windows and all third-party software are regularly updated to prevent vulnerabilities.*
- ***Avoid Opening Unsolicited Email Attachments:*** *Do not open attachments from unsolicited emails to prevent malware infections.*
- ***Do Not Click on Suspicious Links:*** *Never click on URLs included in unsolicited emails, even if they appear to come from known contacts.*
- ***Maintain Antivirus Software:*** *Keep antivirus software updated on all systems to protect against new threats.*
- ***Secure Web Browsers:*** *Ensure web browsers are secure with accurate control settings to prevent exploitation.*
- ***Avoid Paying Ransoms:*** *Never pay ransoms to cybercriminals, as there is no guarantee that files will be released.*
- ***Report Cyber Fraud:*** *Report incidents of cyber fraud to CERT-In and law enforcement agencies for proper action.*
- ***Handshaking:*** *The sequence of information exchanges used to establish and control communication between two or more computers in a network, ensuring secure and reliable data transfer.*
- ***SmartScan:*** *A type of software used to detect and remove computer viruses.*
- ***Palladium:*** *A system developed by Microsoft to streamline computer security, addressing data security and intellectual property concerns.*
- ***Encryption:*** *is the process of converting readable data into an unreadable format using algorithms, ensuring that only authorized parties can decrypt and access the original information. It plays a vital role in cybersecurity by protecting sensitive data during transmission or storage, making it inaccessible to unauthorized users. **Blowfish**, RSA etc are the major encryption algorithms.*
- ***Firewall:*** *A network security device, either software or hardware, that monitors and filters incoming and outgoing network traffic based on established security policies, acting as a barrier to protect the computer from unauthorized access and threats.*
- ***Antivirus:*** *Software designed to detect, prevent, and remove malware, including viruses, worms, and trojans. It scans the computer's files and compares them against a database of known malware signatures, ensuring that any malicious software is identified and dealt with. Examples include Norton, McAfee, and Avast.*

- **Virtual Keyboard:** A software-based keyboard that allows users to input characters without using a physical keyboard. It is particularly useful for entering sensitive information such as passwords and banking details, as it reduces the risk of keylogging attacks, where malicious software records keystrokes to steal information.

Artificial Intelligence

- Artificial Intelligence (AI) is a branch of computer science focused on developing machines that can simulate human-like intellectual abilities such as thinking, understanding, learning, and decision-making.

Background

- 1950: The Turing Test, proposed by Alan Turing in 1950, evaluates a machine's ability to exhibit intelligent behavior indistinguishable from that of a human. If a human evaluator cannot reliably distinguish between responses from a machine and a human, the machine is considered to have passed the test.
- 1956: The scientist John McCarthy defined the term Artificial Intelligence. That is why John McCarthy is called the father of artificial intelligence.
- 1981: Japan was the first to take this initiative and in 1981 launched a scheme called Fifth Generation.
  - ✓ Britain launched the "Elvi" project, while European Union countries initiated the "Esprit" program to advance artificial intelligence research and development.
- 1983: Some private organizations jointly established a consortium 'Micro-Electronics and Computer Technology' to develop advanced technologies applicable to Artificial Intelligence, such as Very Large-Scale Integrated Circuits.
- 2011: SIRI, AI based virtual Vaice Assistant
- 2014: Amazon launched AI based virtual voice Assistance 'Alexa'
- 2014: Microsoft launched its virtual assistant 'Cortana'
- 2016: Google launched AI based virtual assistant 'Google Assistant'
- 2016: The (human-like) intelligent robot known as Sophia was developed by David Henson of Henson Robotics Company in Hong Kong in 2016.
- 2017: Samsung's AI based virtual voice Assistance 'Bixby'.
- 2022: ChatGPT was launched by OpenAI in November 2022. It is a conversational AI model based on the GPT-3 architecture, designed to interact in a conversational manner, answering questions, providing information, and engaging in discussions on a wide range of topics.

Types of AI

- **Reactive Machines:** AI systems that can only react to current situations without using past experiences or memories. They perform specific tasks based on predefined rules and do not learn or adapt from previous interactions.

- **Limited Memory**: AI systems that can use historical data to make decisions and improve over time. They can learn from past experiences and adjust their actions based on new information.
- **Theory of Mind**: A future AI concept where machines will understand human emotions, beliefs, and intentions. This enables better interactions by predicting and responding to human behaviors.
- **Self-Awareness**: The most advanced AI stage where machines possess consciousness and self-awareness. They have their own perceptions, emotions, and understanding of their existence and environment.

Subfields of AI

AI can be divided into several subfields, including machine learning, deep learning, natural language processing, and computer vision

Basic AI Concepts to Know

Artificial Intelligence (AI)

- **Definition**: AI is a field in computer science focused on creating machines that mimic human intelligence, such as learning, reasoning, problem-solving, decision-making, and creativity.
- **Function**: AI systems learn from large datasets, identify patterns, and improve over time to automate tasks and solve problems efficiently.

Machine Learning (ML)

- **Definition**: A subset of AI that enables machines to learn from data without explicit programming.
- **Function**: ML uses algorithms to identify patterns in data and make predictions or decisions. It refines its abilities with more data.
- **Types**:
  - ✓ **Supervised Learning**: Uses labeled data to predict outcomes.
  - ✓ **Unsupervised Learning**: Analyzes unlabeled data to find hidden patterns.
  - ✓ **Semi-Supervised Learning**: Combines a small amount of labeled data with a large amount of unlabeled data.
  - ✓ **Reinforcement Learning**: Learns by trial and error, rewarding desired behaviors.

Deep Learning

- **Definition**: A subfield of ML that uses neural networks with many layers to process unstructured data like text, images, and audio.
- **Function**: Deep learning models automatically identify important features in data, improving accuracy with more data.
- **Example**: Image recognition systems that identify objects like cars by learning relevant characteristics.