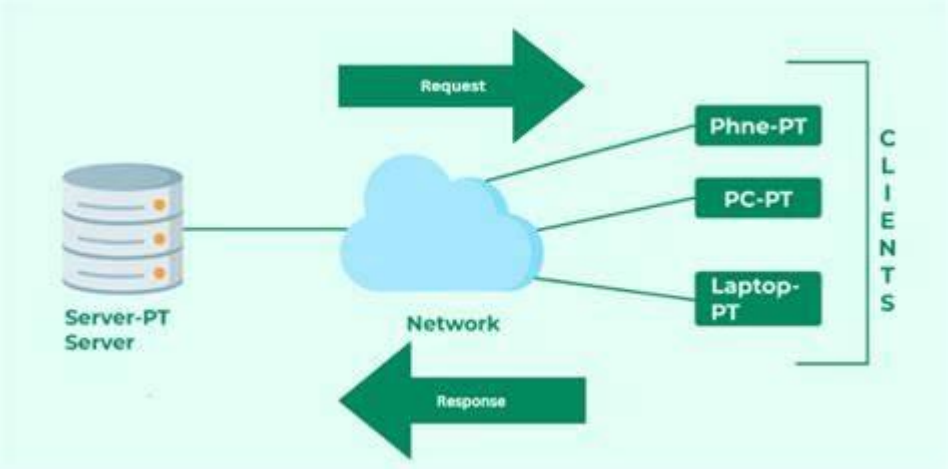
DAY1

CLIENT SERVER MODEL

The Client-server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters called clients.



OSI MODEL

>This is a conceptual thing

>7 layers

1. Physical layer

- connection is physical
- Transmission of raw bits over physical medium(radio waves,cable)
- Protocols- usb,sonet

2.Datalink layer

- node to node data transfer
- error correction
- ensure data accuracy
- frames
- Protocols- Ethernet,ppp

3.Network layer

- Routing
- Ip addressing
- Find best route for delivery. It also handles the routing of packets across networking
- Windowing
- Frames

- Protocols- IP,ICMP,IGMP

4.Transport layer

- Data delivery
- Error handling, error checking
- Choose right data delivery method
- End to end communication
- Ensure data sent in accurate order
- Segments/datagrams
- Protocol- TCP,UDP

5.Session layer

- Establish connection,manages the connection and terminate session
- Protocol- RPC

6.Presentation layer

- Encryption
- Data formatting
- Protocol- TSL/SSL

7.Application layer

- Create data
- Mail Services ,directory service
- Protocol- FTP,SMTP,DNS

ENCODING - The process of converting data into a specific format that can be easily understood by different systems. The primary goal of encoding is to ensure data usability and integrity. It does not provide any security measures, as the transformation is reversible and does not require a key.

ENCRYPTING - process of converting readable data (plaintext) into an unreadable format (ciphertext) using algorithms and keys. The main purpose of encryption is to provide confidentiality and prevent unauthorized access to sensitive information. Encryption is reversible only with the proper decryption key.

TCP/IP

- Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender's end and the same packets have to be recombined at the receiver's end to form the same data, and this thing happens to maintain the accuracy of the data.

- 4 layers

PROTOCOL

- IP – set of rules that govern the communication and exchange of data over the internet. They ensure that data packets are sent and received correctly between devices on a network. Operate on network layer
- TCP – ensures reliable and efficient data transmission over the internet,connection oriented. Operate on transport layer.
- UDP – A transport layer protocol which is unreliable,connectionless and fast
- ICMP – Internet Control Message Protocol is known as ICMP. The protocol is at the network layer. It is mostly utilized on network
- IGMP – **Internet Group Management Protocol**. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets
- ARP – **Address Resolution Protocol** which is in Data link layer .convert IP address to MAC address
- HTTP/HTTPS – HTTP is a protocol used for transferring hypertext over the web. It operates at the application layer.HTTPS is an extended version of HTTP that provides secure communication by encrypting the data using Transport Layer Security (TLS) or Secure Sockets Layer (SSL)
- FTP – standard communication protocol used to transfer files between a client and a server on a computer network.
- SMTP – It operates at the **application layer** of the TCP/IP protocol stack and is essential for email communication.

NIC

- Network interface card/Ethernet card
- It connects computers to network
- Using unique mac address

Submarine cable map

- Optical fibre cable
- They are fibre optic cables under oceans that ensure globally internet connectivity by carrying data with high speed.

SCALABILITY

1.Vertical scaling – scale up, scale down

2. Horizontal scaling- scale out, scale in

? To scale horizontally what should we ensure and do?

- Ensure that no data persist in any application.that is the data should be stateless.For that you have to store the data in database.

MODEM

* Convert signal for internal access

* Convert digital signal to analog and viceversa.

*Connect directly to ISP

*Receive public IP

*WAN

ROUTER

- A **router** in computer networks is a device that forwards data packets between different networks.
- It acts as a traffic manager, directing data from one network to another based on the destination IP address in the data packet.
- Routers are essential for connecting multiple networks together, such as linking a local area network (LAN) to the internet.

How Router works??

1. Data Packet Creation:

When you send data over a network (e.g., browsing a website, sending an email), the information is broken down into smaller units called **data packets**. Each packet contains:

- **Source address**: The origin of the data (your device's IP address).
- **Destination address**: The target address where the data should go (e.g., the website server's IP address).
- **Other routing information**: Information that helps routers determine the best path.

2. Routing the Data:

The router receives the data packet and reads the **destination address**. Using a routing table, which stores information about the best paths for data to travel, the router decides where to send the packet next.

3. Forwarding the Packet:

Once the router identifies the best path, it forwards the data packet to the next router or the destination network. This process continues as the packet travels through multiple routers on its way to its final destination.

Key Functions of a Router:

- **Directing traffic**: Ensuring data moves between devices and networks.
- **Security**: Providing a firewall, which helps block unauthorized access to your network.
- **Wi-Fi management**: Managing wireless connections for devices.
- **NAT**: Translating private local addresses to a public one and vice versa.

ROUTER AND GATEWAY

	ROUTER	GATEWAY
Primary function	Routes data packets between different networks	Translates and facilitates communication between different protocols or networks
Layer	Operates at Layer 3 (Network Layer)	Operate at multiple layers
Scope	Typically used within local networks to manage traffic between devices and the internet	Used to bridge different networks with varying protocols or architectures
Complexity	Simpler in comparison, mainly focusing on routing	More complex as it may involve translating
Example	Home or office routers connecting LAN to the internet	VoIP gateway, email gateway, HTTP gateway

ADVANTAGES

- Efficient Traffic Management
- Network Segmentation
- Security
- Scalability

DISADVANTAGES

- Routers introduce some delay (latency) due to the processing required for packet forwarding and routing. This can be a concern in real-time applications like VoIP or gaming.
- Single Point of Failure
- Bandwidth Limitation

TOPOLOGIES

1.Bus – all device connected to a single line, if that line break whole devices fails

2. Ring – Each device connected to 2 other device

3. Tree -Hierarchal arrangement, combination of bus and star, Secure and reliable.

4. Mesh -every node is connected to every other node, Direct communication, Complex

Peer to peer communication – Devices communicate directly without any central server

HTTP OVERVIEW

Methods

GET - Retrieve Data (There won't be any json)
POST - Create Data (json format)
PUT - Update Data (json format)
DELETE - Remove Data

DAY2

HTTP error/status codes //Stateless Protocol

- 200 – OK
- 404 -Not found
- 500 - internal server error

Cookies

Cookies are termed as certain messages when a **web server** transmits any messages to a web browser so that the web server can monitor the user's activity on a particular website. It is a small piece of information that a website stores on your computer, and uses it at the time of your iteration on that website. When you revisit the website your browser sends information back to the site.

VPN(virtual private network)

A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet. A Virtual Private Network is a way to extend a private network using a public network such as the Internet. The name only suggests that it is a "Virtual Private Network", i.e. user can be part of a local network sitting at a remote location. It makes use of tuneling protocols to establish a secure connection.

Types of VPN

- Remote Access VPN
  Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.

- Site to Site VPN
  A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use

Site-to-site VPN to connect the network of one office location to the network at another office location.

- Cloud VPN

  A Cloud VPN is a virtual private network that allows users to securely connect to a cloud-based infrastructure or service. It uses the internet as the primary transport medium to connect the remote users to the cloud-based resources. Cloud VPNs are typically offered as a service by cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. Cloud VPNs are often used by organizations to securely connect their on-premises resources to cloud-based resources, such as cloud-based storage or software-as-a-service (SaaS) applications.

- Mobile VPN

  Mobile VPN is a virtual private network that allows mobile users to securely connect to a private network, typically through a cellular network. It creates a secure and encrypted connection between the mobile device and the VPN server, protecting the data transmitted over the connection. Mobile VPNs can be used to access corporate resources, such as email or internal websites, while the user is away from the office. They can also be used to securely access public Wi-Fi networks.

- SSL VPN

  SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses the SSL protocol to secure the connection between the user and the VPN server. It allows remote users to securely access a private network by establishing an encrypted tunnel between the user's device and the VPN server. SSL VPNs are typically accessed through a web browser, rather than through a standalone client.

- Double VPN

  It is one where an internet connection is run through two VPN servers operated by the same VPN service, one after the other. This is called a cascade configuration, where one connection "falls" into another one.Give extra security.

CHECKSUM

Checksum is the error detection method used by upper-layer protocols . This method uses a **Checksum Generator** on the sender side and a **Checksum Checker** on the receiver side. It is a unique number generated from data to verify its integrity. When data is created, a checksum is calculated and sent or saved with it. Later, when accessing the data, the checksum is recalculated. If the two checksums match, the data is likely error free.

IP

ICMP

The protocol is at the network layer. It is mostly utilized on network equipment like routers and is utilized for error handling at the network layer. Since there are various kinds of network layer faults, ICMP can be utilized to report and troubleshoot these errors.

PING

Ping is a basic yet powerful network utility that helps you check the reachability of a server or IP address and measures the round-trip time for messages sent from your computer to the destination and back. It is primarily used to verify whether a device or server is **active** and responsive over a network.This uses ICMP echo request,without ICMP Ping will not work.

TRACEROUTE

Traceroute also called as **Tracert Command** is a more advanced network tool used to trace the path that packets take from your computer to a remote server or host. It provides a **detailed map** of the route the data packets follow across the network and shows how long it takes to travel from one hop (router or intermediary device) to the next.

ARP(Address Resolution Protocol)

- Convert Ip to MAC Address
- This is a Datalink Layer Protocol
- Ip - logical address
  0 - 255 is the range
- MAC - unique physical address
  0 - 255 not in this range

TCP/IP layers

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data link Layer

IP Addressing and Subnetting

A subnet is like a smaller group within a large network. It is a way to split a large network into smaller networks so that devices present in one network can transmits data more easily. For example, in a company, different departments can each have their own subnet, keeping their data traffic separate from others. Subnet makes the network faster and easier to manage and also improves the security of the network.

It provides security to one network from another network. Eg :In an Organisation, the code of the Developer department must not be accessed by another department.

VPC

Virtual Private Cloud is a service that allows its users to launch their virtual machines in a protected as well as isolated virtual environment defined by them.

AVAILABILITY ZONE

Availability Zone is the part or place to deploy the application in the same geographical location (Region). Each availability zone is made up of one or more data centers that have independent power, cooling, and networking.

REGION

The Region is a Specific geographical location to host your applications. Each region is designed to comply with specific laws and regulations and to provide low-latency network connectivity to specific geographic areas.

DATA CENTRE

Each availability zone is made up of one or more data centers that have independent power, cooling, and networking. This allows for the creation of highly available and fault-tolerant applications and services.

NAT(Network address translation)

It is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa to provide Internet access to the local hosts. It also does the translation of port numbers, i.e., masks the port number of the host with another port number in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Generally, the border router is configured for NAT i.e. the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

SSL

Provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

There are two primary types of encryption techniques:

1.symmetric key encryption

In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

2.asymmetric key encryption

Asymmetric key encryption is one of the most common cryptographic methods that involve using a single key and its pendent, where one key is used to encrypt data and the second one is used to decrypt an encrypted text. The second key is kept highly secret, while the first one which is called a public key can be freely distributed among the service's users.

MICROSERVICES

Microservice is a small, loosely coupled service that is designed to perform a specific business function and each microservice can be developed, deployed, and scaled independently.

Load balancer

A **load balancer** is a networking device or software application that distributes incoming traffic among multiple servers to ensure high availability, efficient utilization of resources, and high performance. It acts as a "traffic cop" sitting in front of your servers, routing client requests across all servers to prevent any single server from being overloaded.

Two types

- Path based routing
- Service level routing

Authentication

Authentication is the method of verifying the identity of a consumer or system to ensure they're who they claim to be. It involves checking credentials which include usernames, passwords, or biometric information like fingerprints or facial recognition.

Authorisation

Authorization is the method of figuring out and granting permissions to a demonstrated user or system, specifying what assets they can access and what actions they're allowed to carry out. It comes after authentication and guarantees that the authenticated entity has the proper rights to use certain data, applications, or services.

Two types of communication :

Synchronous : An application or instance makes a call and wait for the response. This is inefficient

Asynchronous : Here there is no wait for response.That is not hooked on the communication.

Two types:

Public subscribe model/ Notification model

The subscriber no need to check, they will notified when there is something. Eg; SMS

Queue model

The subscriber or instance have to go and check whether there is a notification or not. Eg; SQS(Simple Queue Service)

DAY 3

FIREWALL

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 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

Ingress refers to **incoming traffic** that enters a network from an external source, such as the internet or another network.

Egress refers to **outgoing traffic** that leaves a network and goes to an external destination, like a website on the internet.

Stateful firewall

This firewall is situated at Layers 3 and 4 of the OSI Model. As the name suggests, a stateful firewall always keeps track of the state of network connections.

Stateless firewall

It is also known as an Access Control List (ACL), does not store information on the connection state.

*Stateless firewalls do not take as much into account as stateful firewalls, they're generally considered to be less rigorous. That is why they are fast.

*They are generally cheaper than stateful firewalls.

IPSec

IP Security (IPSec) refers to a collection of communication rules or protocols used to establish secure network connections. Internet Protocol (IP) is the common standard that controls how data is transmitted across the internet. IPSec enhances the protocol security by introducing **encryption** and **authentication**. IPSec encrypts data at the source and then decrypts it at the destination. It also verifies the source of the data.

IPSec	**Firewall**
• IPsec is a suite of protocols used to secure communications over an IP network. It ensures the confidentiality, integrity, and authenticity of data transmitted between two devices (typically	• A firewall is a network security device that monitors and controls incoming and outgoing traffic based on security rules and policies. It is used to prevent unauthorized access to or from a private network.

routers, gateways, or hosts) over an untrusted network, like the internet. • Operates at the network layer • Provides encryption and authentication • Secure communication	• Operate primarily at the network layer and transport layer • Does not provide encryption and authentication • Traffic control

GATEWAY

A gateway is a network connectivity device that connects two different configuration networks. It works as the entry-exit point for a network because all traffic that passes across the networks must pass through the gateway. A gateway monitors and controls all the incoming and outgoing network traffic.

How it works?

- The gateway receives data from devices within the network.
- After receiving data the gateway intercept and analyse data packets, which include analysing packet header, payload etc.
- Based on the analysis of the data packets, the gateway calculate an appropriate destination address of data packet. It then routes the data packets to their destination address.
- In some cases, the gateway might also want to transform the format of the obtained data to ensure compatibility at the receiver.
- Once the data packets have been analysed, routed, and converted, then the gateway sends the last packets to their respective destinations address.

BRIDGE

Bridge is a local internetworking device that is used to connect two or more network segments together. A bridge operates at the Data Link Layer (Layer 2) of the OSI model and uses the MAC addresses of devices to make forwarding decisions.

SWITCH

The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices. It operates in the Data Link Layer and have full duplex communication.

HUB

A hub is a hardware device used at the physical layer to connect multiple devices in the network. Hubs are widely used to connect LANs. A hub has multiple ports. Unlike a switch, a hub cannot filter the data, i.e. it cannot identify the destination of the packet, So it broadcasts or sends the message to each port. A hub is a multiport device, which has multiple ports in a device and shares the data to multiple ports altogether. A hub acts as a dumb switch that does not know, which data needs to be forwarded where so it broadcasts or sends the data to each port.

PAT

In Port Address Translation (PAT), Private IP address are translated into the public IP address through port numbers. PAT also uses IPv4 address but with port number. PAT is a dynamic NAT.

SERVER FARM

A server farm is a large number of servers (up to thousands) that are grouped to improve functionality and accessibility. A **server farm**, also known as a **server cluster**, is a large group of computers placed together in one place. These computers are all connected and work together to handle big computing tasks. Businesses and organizations use server farms to manage lots of data, handle many internet actions at once, and run complex programs. A server farm includes many different servers that may perform tasks like processing data, storing information, or running applications.

PROXY AND REVERSE PROXY

PROXY

A forward proxy, also referred to as a "proxy server," or simply a "proxy," is a server that sits in front of one or more client computers and serves as a conduit between the clients and the internet. The forward proxy receives the request before sending it on from the client machine to the internet resource. On behalf of the client machine, the forward proxy then sends the request to the internet and returns the response.

REVERSE PROXY

A server that sits in front of one or more web servers and serves as a go-between for the web servers and the Internet is known as a reverse proxy. The reverse proxy receives the request before sending it on to the internet resource for the client. After sending the request to one of the web servers, the reverse proxy receives the response from that server. The response is then sent back to the client by the reverse proxy.

THREAT, VULNAREBILITY AND RISK

THREAT

- A threat is anything that has the potential to cause harm to a network, system, or data. It is a potential danger that could exploit a vulnerability and negatively affect the network's security.
- Threats can be either intentional (like hacking or malware) or unintentional (like a natural disaster or human error).

VULNERABILITY

- A vulnerability is a weakness or flaw in a network, system, or application that can be exploited by a threat to cause harm. Vulnerabilities are often technical flaws or security gaps that allow unauthorized access or actions.
- Vulnerabilities could exist in hardware, software, configurations, or even human practices.

RISK

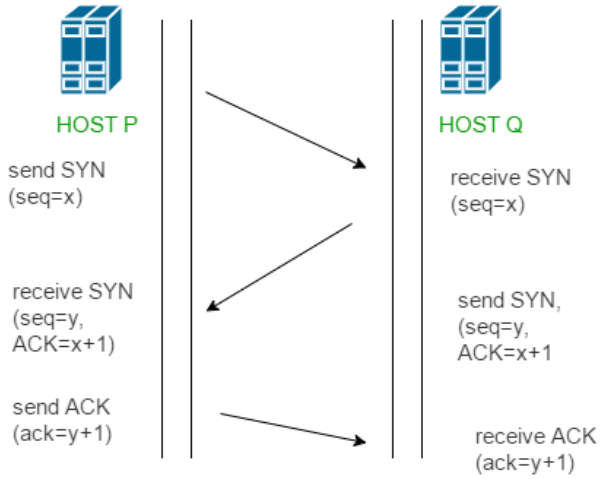
- Risk refers to the probability of a threat exploiting a vulnerability and causing harm, paired with the impact of that harm if it were to occur. It is a measure of the potential loss or damage from a threat exploiting a vulnerability.
- Risk is typically calculated as: **Risk=Threat × Vulnerability**

IPV4 AND IPV6

IPV4	**IPV6**
• **32-bit** address length. • written in **dotted decimal format** • Limited address space • Routing is less efficient due to the larger number of routing tables required to manage IPv4 addresses and subnets. • require **manual configuration** or the use of **DHCP**	• **128-bit** address length. • written in **hexadecimal format** • Virtually unlimited address space • Pv6 has more efficient routing. The address structure is designed to reduce the size of routing tables and simplify packet processing • supports **automatic configuration** and **DHCPv6** is also available

3 WAY HANDSHAKE

The TCP 3-Way Handshake is a fundamental process that establishes a reliable connection between two devices over a TCP/IP network. It involves three steps: SYN (Synchronize), SYN-ACK (Synchronize-Acknowledge), and ACK (Acknowledge). During the handshake, the client and server exchange initial sequence numbers and confirm the connection establishment.



***Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with

***Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

***Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.

WIFI

Wi-Fi is wireless networking technology enabling various devices like computers, smartphones, and other equipment to connect to the Internet and communicate with each other without a cable. It creates a network where these devices can exchange information. These established connections through a wireless router act as an intermediary between the WiFi-compatible devices and the Internet. Follows IEEE 802.11 standards.

DHCP

Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network. Instead of manually configuring each device with an IP address, DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway, and DNS server addresses, automatically from a DHCP server.

PORT FORWARDING

Port forwarding (also known as **port mapping**) is a networking technique used to allow external devices (or the internet) to access services on a private internal network, such as a home or office network. It works by forwarding incoming network traffic on specific ports from a router or firewall to a designated device or server within the local network.

VLAN

A **VLAN** (Virtual Local Area Network) is a **logical subgroup** within a physical network that groups together devices even if they are not physically connected to the same network switch. VLANs are used to segment and organize networks, improving security, performance, and management flexibility.
A **VLAN** is a powerful tool for segmenting a network into smaller, manageable sections. It helps improve security, reduce broadcast traffic, and make network management more efficient. By using VLANs, you can create a more organized and scalable network infrastructure, especially in large or complex environments.

DAY 4

DATA CENTER

In a dedicated space with strong security levels, where enterprises or organizations store and share large amounts of data, is known as a data center.

Key components

- **Servers** (compute power)
  Servers are the backbone of any data center, responsible for running applications, managing data, and providing services to clients or users. These can include web servers, database servers, application servers, and storage servers.
- **Storage systems** (data management)

Data storage systems hold and manage large volumes of data within a data center. This can include both primary data (active data) and backup or archival data.

- **Networking equipment** (communication)
  Networking equipment connects all the components of a data center, ensuring communication between servers, storage systems, and external networks.(Router, Switch, Firewall)
- **Power supply and backup systems** (reliable operation)
  Ensures that the data center operates continuously without interruption due to power failures.
- **Cooling systems** (temperature regulation)
  Servers and other IT equipment generate a lot of heat, so cooling systems are necessary to maintain an optimal operating temperature.
- **Security systems** (physical and cybersecurity)
  Protects the physical and logical infrastructure of the data center from unauthorized access, theft, and cyber threats.

Types of Data centers

On premise Data Center

- The organization owns the data center and is responsible for managing, maintaining, and upgrading the infrastructure.
- The company has complete control over how it is configured and customized to meet specific requirements.
- The data center is located within the organization's own premises.
- High initial investment.

Colocation Data Center

- A third-party data center where businesses can rent space, power, cooling, and network connectivity for their IT infrastructure.
- Lower investment
- Shared infrasructure

Cloud Data Center

- Data centers operated by cloud service providers (e.g., AWS, Google Cloud, Microsoft Azure) that host and manage virtualized resources and services.
- Pay-as-you-go model.
- High scalability

Storage Types

- **Direct Attached Storage (DAS)**:

* DAS refers to storage devices that are directly attached to a single computer or server, without being connected to a network. It is typically used for personal or small-scale applications.

* How it works: DAS storage is directly connected via interfaces such as USB, SATA, SAS, or Thunderbolt.

* Local storage directly attached to servers.
*Lack of scalability
*Potential to lost data
*Device specific
* Examples: External hard drives, internal hard drives, SSDs (Solid-State Drives).

- **Network Attached Storage (NAS)**:

*NAS is a storage device connected to a network, allowing multiple users and devices to access data over the network. It's often used for centralized file storage and sharing.

*How it works: NAS devices typically use Ethernet or Wi-Fi to connect to a local area network (LAN), and they present storage over protocols like SMB/CIFS (Windows), NFS (Linux/Unix), or AFP (Apple).
*File-based storage accessible over a network.
*Moderate scalability and perfomance
*Examples: Synology NAS, QNAP NAS, WD My Cloud.

- **Storage Area Networks (SAN)**:

*SAN is a high-speed network that connects storage devices (such as disk arrays) with servers, enabling block-level data access. Unlike NAS, which provides file-level access, SAN provides block-level access to data, typically used for large-scale enterprise applications.
*How it works: SANs often use Fibre Channel, iSCSI, or FCoE (Fibre Channel over Ethernet) to connect storage devices and servers. Data is accessed as blocks rather than files.
*High-speed network of storage devices, often used for large-scale enterprise data storage.
*Examples: EMC VMAX, NetApp FAS, Dell PowerMax

TYPES OF STORAGES

PRIMARY STORAGE

Primary storage refers to the storage that is directly accessible by the CPU and is used to store data and instructions that are actively being processed.

(i) **RAM (Random access memory)**

Description: RAM is the most common type of primary storage and is used to store data and instructions that the CPU needs to access quickly while performing tasks.

Characteristics:

- Fast read and write access.
- Volatile memory (data is lost when power is turned off).
- Temporarily stores data being processed by running applications.

(ii) **ROM(Read only memory)**

Definition: ROM is a type of non-volatile memory used in computers and other electronic devices to store permanent data or instructions that are not meant to be altered or modified during normal operation.

Characteristics:

- Non volatile
- Read only
- Slower access

SECONDARY STORAGE

i. **HDD (Hard Disk Drives)**

Description: HDDs are mechanical storage devices that use spinning disks to read/write data. They are widely used for long-term storage.

Characteristics:

a. Larger capacity compared to primary storage.
b. Slower read/write speeds due to mechanical components.
c. Non-volatile (data persists even without power).

ii. **SSD (Solid-State Drives)**

Description: SSDs are storage devices that use flash memory to store data, providing faster read/write speeds compared to HDDs.

Characteristics:

a. Faster than HDDs but generally more expensive.
b. Larger capacity compared to primary storage.
c. Non-volatile, retains data without power.

OPTICAL DISC

- An **optical disc** is a storage medium that uses laser light to read and write data on a reflective surface.
- Optical discs are widely used for storing data such as software, music, videos, and backups.
- Example : CD, DVD, Floppy Disc

RAID LEVELS

RAID 0 (Striping)

- **Configuration**: Data is split into blocks and distributed across multiple disks (at least 2).
- **Redundancy**: No redundancy—if one drive fails, all data is lost.
- **Performance**: High performance, as data is read and written in parallel to multiple drives.
- **Capacity**: Total capacity is the sum of the capacities of all disks.
- **Use Case**: Suitable for applications requiring high performance and where data loss is not critical (e.g., temporary data, non-essential files).

RAID 1 (Mirroring)

- **Configuration**: Data is duplicated (mirrored) across two or more disks.
- **Redundancy**: High redundancy—if one drive fails, the data is still available from the other drive(s).
- **Performance**: Good read performance (because the system can read from multiple disks), but write performance is similar to a single disk.
- **Capacity**: Total capacity is the size of one drive (since data is duplicated).
- **Use Case**: Suitable for situations where data integrity is critical and write performance is not as important (e.g., personal computers, critical data storage).

RAID 5 (Striping with Parity)

- **Configuration**: Data is striped across multiple disks (at least 3), with parity information distributed across all disks.
- **Redundancy**: Moderate redundancy—if one disk fails, the data can be rebuilt using the parity data from the remaining disks.
- **Performance**: Good read performance, but write performance is slower compared to RAID 0 and RAID 1 due to the overhead of parity calculations.

- **Capacity**: Total capacity is the sum of all disks minus one (because one disk is used for parity).
- **Use Case**: Suitable for applications that require a balance of redundancy, performance, and storage capacity (e.g., file servers, databases).

RAID 6 (Striping with Double Parity)

- **Configuration**: Similar to RAID 5 but with **two sets of parity data**, which are stored across different disks (requires at least 4 disks).
- **Redundancy**: High redundancy—can tolerate the failure of **two disks** simultaneously without data loss.
- **Performance**: Read performance is good, but write performance is slower than RAID 5 because of double parity calculations.
- **Capacity**: Total capacity is the sum of all disks minus two (because two disks are used for parity).
- **Use Case**: Suitable for environments where data protection is more important than write performance (e.g., critical business data storage).

RAID 10 (RAID 1+0)

- **Configuration**: Combines the features of RAID 1 and RAID 0. Data is mirrored (RAID 1) and then striped (RAID 0).
- **Redundancy**: High redundancy—can tolerate the failure of one disk per mirrored pair.
- **Performance**: High performance for both read and write operations, as data is striped (RAID 0) and mirrored (RAID 1).
- **Capacity**: Total capacity is the sum of half of the disks (since data is mirrored).
- **Use Case**: Suitable for applications that require both high performance and redundancy (e.g., databases, high-performance servers).

BACKUP AND RECOVERY

A **backup** is the process of creating a duplicate copy of data that can be restored in case the original data is lost, corrupted, or inaccessible.

TYPES OF BACKUP

Full Backup

- **Definition**: A full backup is a complete copy of all selected data. It copies everything, including all files, folders, and system data (depending on the configuration).
- **How It Works**: Every time a full backup is performed, all data is backed up in its entirety, regardless of whether it has changed since the last backup.

Incremental Backup

- **Definition**: An incremental backup only backs up the data that has changed since the **last backup** (whether it was a full backup or the most recent incremental backup).
- **How It Works**: After an initial full backup, subsequent incremental backups only capture changes made to files since the last backup. This can be multiple times over a period.

Differential Backup

- **Definition**: A differential backup captures all the changes made since the last **full backup**. Unlike incremental backups, differential backups do not rely on previous differential backups, but only on the full backup.

Mirror Backup

- **Definition**: A mirror backup creates an exact copy (or "mirror") of the selected data. It is similar to a full backup but continuously synchronizes data between the source and the backup location.

3-2-1 BACKUP STRATEGY

The **3-2-1 backup strategy** is a widely recommended method for ensuring robust data protection and recovery. It helps mitigate the risks of data loss from various types of disasters (e.g., hardware failure, cyberattacks, accidental deletions). This strategy involves creating multiple copies of data and storing them in different locations to increase redundancy and resilience.2 Copies stores in two different media types and one in offsite.

BASIC SERVER COMPONENTS

- **MOTHER BOARD:** A **motherboard** is the central printed circuit board (PCB) in a computer that connects and allows communication between various hardware components. It serves as the backbone of the computer, providing essential connections for components like the CPU, RAM
- **CPU**
- **RAM**
- **NIC**
- **STORAGE DRIVE**

LOAD BALANCING

- **ROUND ROBIN: Round Robin** is one of the simplest and most commonly used load balancing algorithms. It is a method used to distribute client requests (or traffic) across a group of servers or resources in a circular order.
- **LEAST CONNECTION: Least Connections** is a dynamic load balancing algorithm that directs incoming traffic to the server with the **fewest active connections** at the time of the request. This method is designed to distribute load based on the number of active connections each server is currently handling, aiming to prevent overloading any single server.
- **LEAST RESPONSE TIME: Least Response Time** is a dynamic load balancing algorithm that routes incoming client requests to the server with the **quickest response time** at the moment of the request. The goal of this algorithm is to optimize user experience by sending traffic to the server that is not only least loaded but also currently capable of processing requests the fastest.
- **SOURCE IP HASHING: Source IP Hashing** is a load balancing algorithm that uses the **client's IP address** to determine which server in the pool should handle a particular request. The key idea behind this approach is to ensure that requests from the same client IP address are always directed to the same backend server, creating session persistence (also called sticky sessions).
- **WEIGHTED ROUND ROBIN: Weighted Round Robin (WRR)** is an enhancement of the traditional **Round Robin** load balancing algorithm. In **Weighted Round Robin**, each server

in the pool is assigned a **weight** that reflects its capacity or performance. The load balancer distributes incoming requests across the servers, but it gives more requests to servers with higher weights, effectively allowing more powerful servers to handle more traffic.

TYPES OF LOAD BALANCER

HARDWARE LOAD BALANCER

Hardware load balancer is a physical appliance designed specifically for load balancing tasks. It is a dedicated device with specialized hardware and software to handle traffic distribution efficiently.

SOFTWARE LOAD BALANCER

A software load balancer is a software application that runs on general-purpose hardware (such as a server or virtual machine) to perform load balancing tasks. It uses algorithms and protocols to distribute traffic among multiple servers.

CONFIDENTIALITY

Confidentiality is one of the core principles of **information security**, ensuring that sensitive information is only accessible to those authorized to view it. It involves preventing unauthorized individuals, organizations, or systems from accessing data, ensuring that private and personal information is protected from exposure or misuse.

INTEGRITY

Integrity refers to the concept of maintaining and assuring the accuracy, consistency, and trustworthiness of data throughout its lifecycle. It ensures that data is not altered, tampered with, or corrupted—either accidentally or maliciously—while it is being stored, transmitted, or processed.

AVAILABILITY

Availability refers to the concept of ensuring that information, systems, and services are accessible and usable by authorized individuals when needed.