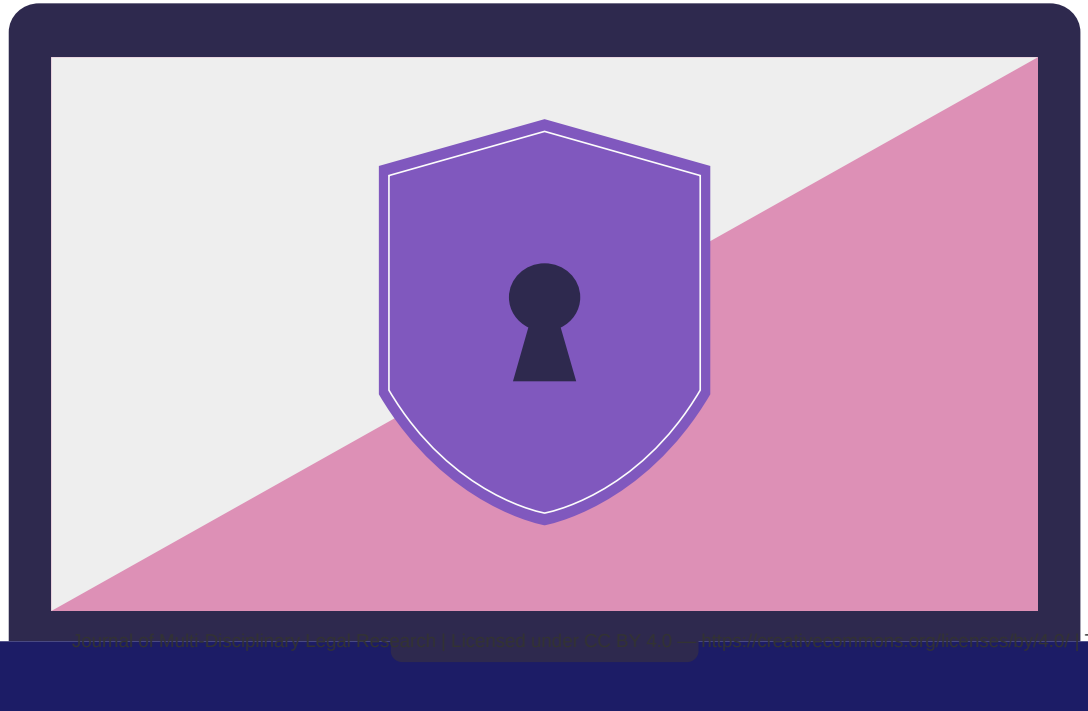
Vinay Joy - Cyber PPT



Topics

- Authentication
- Authorization
- CDN
- Operating system

Agenda

1) Authentication
    - What
    - Why
    - Types
    - Session Based Authentication
    - Cookies Based Authentication
    - Token Based Authentication
    - Certificate Based Authentication
    - SSO
    - SAML
2) Authorization
    - What
    - Why
    - Working of Authorization
    - Types
3) CDN
    - CDN Components
    - Working of CDN
    - Types
    - CDN Security
4) Operating System
    - What
    - Functions of OS
    - Types of OS

Authentication

What Authentication?

- **Authentication** is the process of verifying the identity of a user.
- IT is the process of verifying the identity of a user when that user logs in to a computer system.

  In simple terms **“Who are you”**

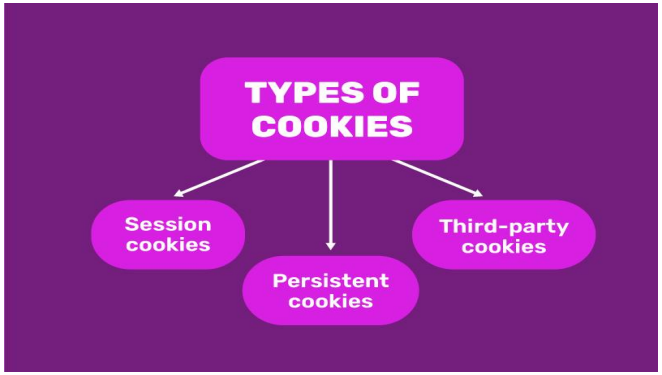
Why Authentication?

- To allow authorized users to access the computer
- To deny access to unauthorized users.
- To give the user appropriate permissions

What are cookies sessions and tokens?

Cookies

- Cookies are small files of information that a web server generates and sends to a web browser.
- This files are stored in the users computer
- The data's in the cookies contains user's identity such as (Usernames & Passwords).
- Specific cookies are also used to identify specific users and improve their web browsing experience.



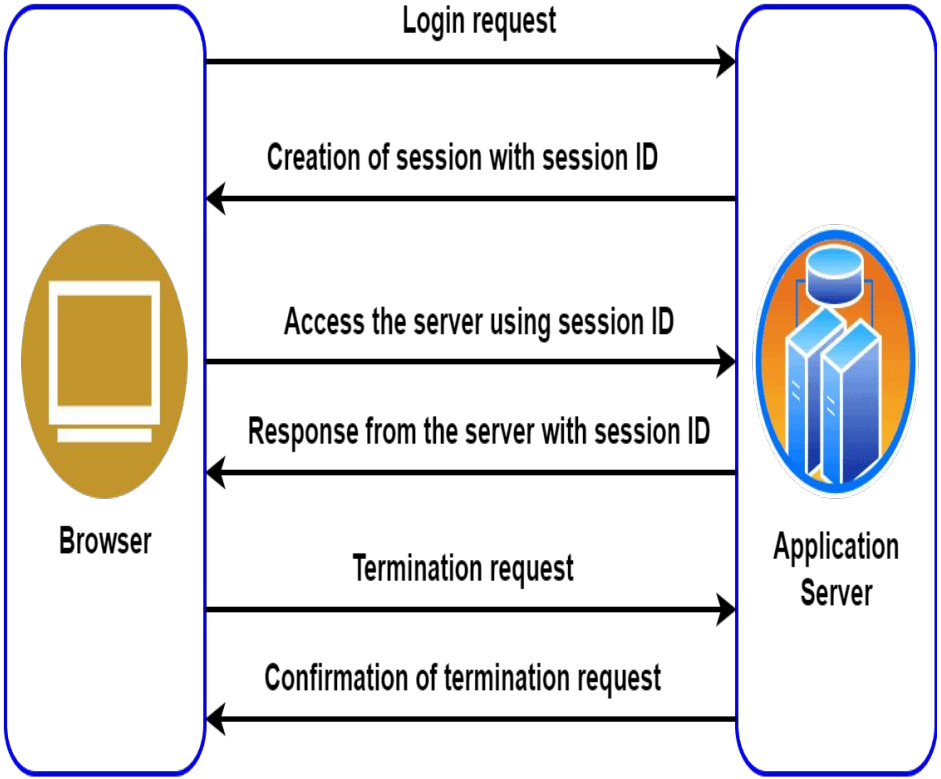
- Session Cookies : A session cookie is a file that a website server delivers to a browser with a session ID, this session cookies is **to identify a user that has logged into a website**,They are stored in random access memory, once session ends session cookies automatically gets deleted

- Persistent cookies: persistent cookies remain in a user's browser for a extended length of time,They get erased when the cookies expire or the users clear them from the browser. They are stored in users Hard drive. This cookies **stores to store information such as login credentials, language preferences, and browsing history.**

- Third-party Cookies: Third-party cookies are most often used for tracking **to identify visitors and see which websites they visited**. These are set by domains that the user does not visit directly.This occurs when publishers include third-party elements on their website.

Session

- A session refers to a way of **establishing and maintaining** state **information** about a user's interactions with a website or web application.
- When a user visits the website a session is created for the user.
- Sessions helps the server to **track the user informations**.
- This informations contains such as the user's login status, preferences, and any data entered into forms.
- Server generates the **session ID** also known as "session tokens"
- The session ID allows the server to associate the user's requests with their specific session
- Session ID also helps in **retrieve and update the session data** as needed.
- **Session ID are stored in user's browser cookies and session Data is stored in the server.**



Token

- A Token is a **computer-generated code** that acts as a digitally encoded signature of a user.
- They are used to authenticate the identity of a user to access any website or application network.
- A valid token allows a user to retain access to an online service or web application until the token expires.
- Token also helps the user can continue to access a resource without re-entering their login credentials every time
- The Tokens are stored in user web browsers, local storage, cache
- Tokens are encrypted and machine-generated.

Two types of tokens

Physical Token:

- A Physical token use a tangible device to store the information of a user.
- the secret key is a physical device that can be used to prove the user's identity.
- Further it is divided in two types of tokens
    - Hard tokens and soft tokens

- Hard token uses smart cards and USB to grant access.

- Soft token uses OTP via authorized app or SMS.

Web Token :

- The Web token is fully digital
- Here, the server and the client interface interact upon the user's request.
- Web tokens are also known as **JWT (JSON Web Tokens)**
- **JWT is used for securely transmitting data in JSON format.**

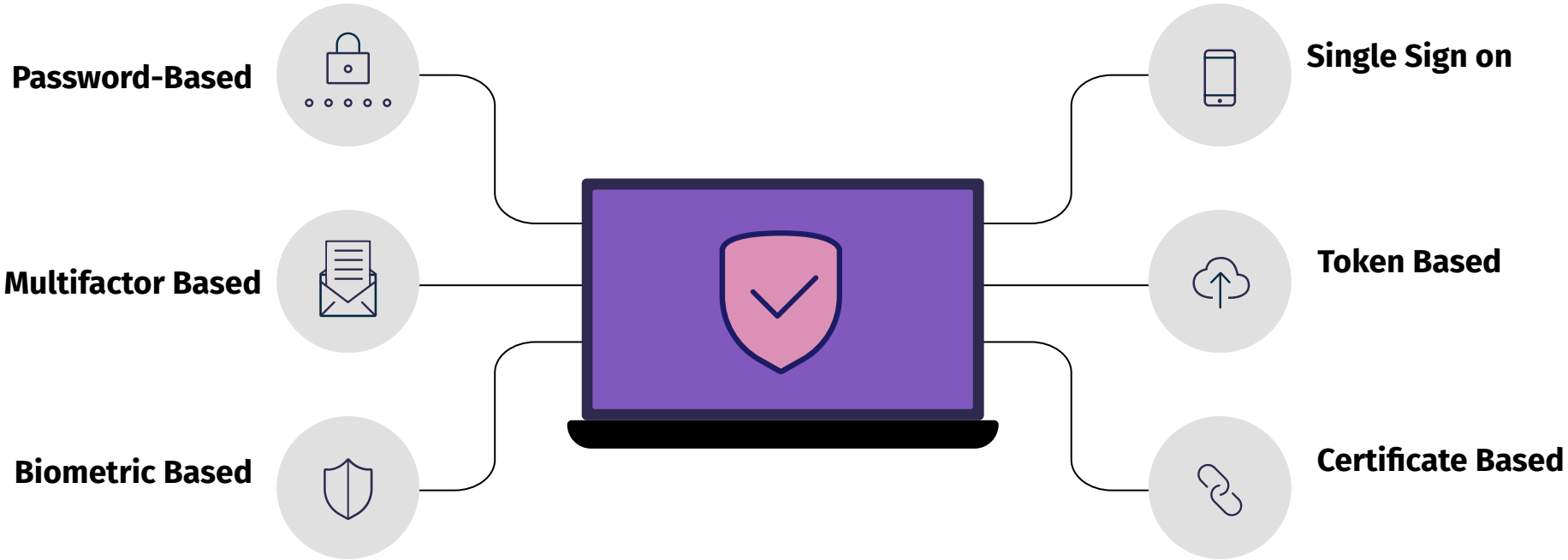
Stateful Authentication

- In stateful authentication, the server keeps track of the authentication state of each user session.
- When a user logs in, the server creates a session for that user and stores it, usually in the form of a session ID or a cookie.
- Stateful authentication refers to the context of session and cookies

Stateless Authentication

- In stateless authentication, the server does not store any session information for authenticated users.
- Stateless authentication refers to the tokens using JWT, OAuth,etc.
- Stateless authentication can be scalable for microservices architecture

Types of Authentication

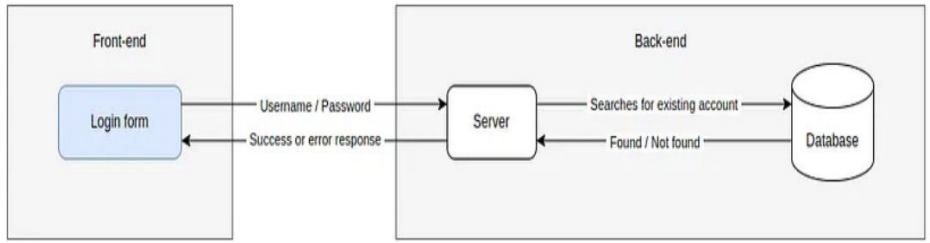


Password based Authentication

Password-based authentication is a method that requires the user to enter their credentials in order to confirm their identity.

“username and password”

Once entered the right credentials and they’re granted access to a page or service.



Simple password-based authentication mechanism using a database

Multi-factor Based Authentication

- Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password.
- A 2 pieces of evidence, such as their password and a temporary passcode, to prove their identity.

Example : To log into an email account, a user might need to enter both their account password and a single-use passcode(OTP) or verifying by validating a number which will be displayed in the users authorized mobile number, the email provider sends to the single or double digit number to be verified.

Biometric Based

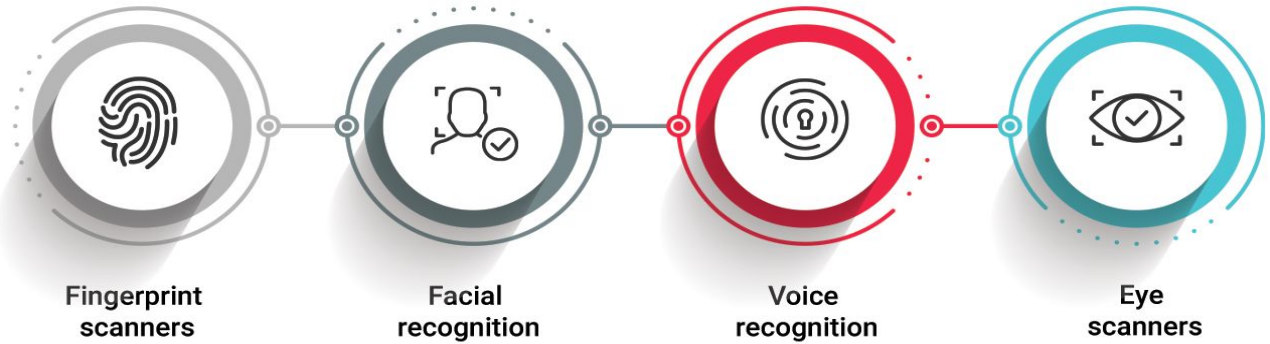
- Biometric authentication is a security measure that matches the biometric features of a user looking to access a device or a system.

- It is a systems compare physical or behavioral traits to stored, confirmed, authentic data in a database.

-

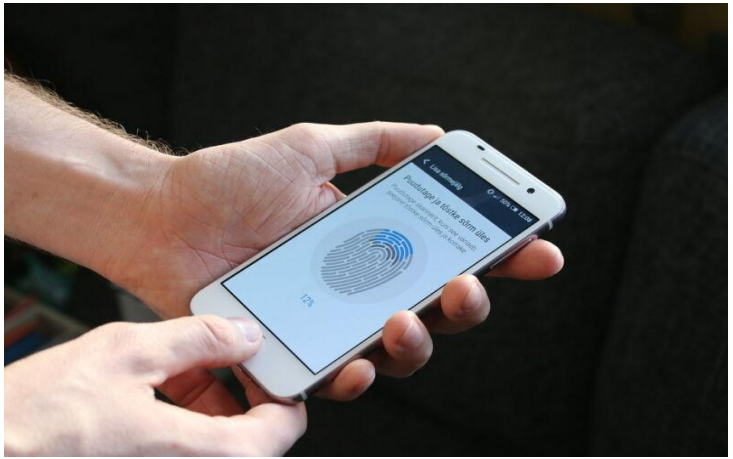
TOOLBOX™

TYPES OF BIOMETRIC AUTHENTICATION



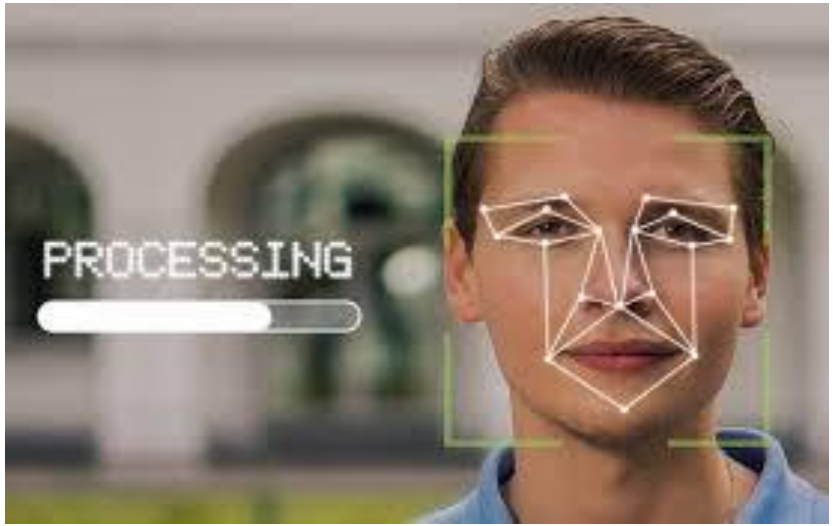
Types of Biometric Authentication

1) **Fingerprint Scanners:**
   - This fingerprint scanners works according to the **human fingers patters like ridges and lines** that represent a pattern wholly unique.
   - This patterns get **stored in the device in the first attempt**, so whenever users tries to input the fingerprint device checks the database and authenticated the user.



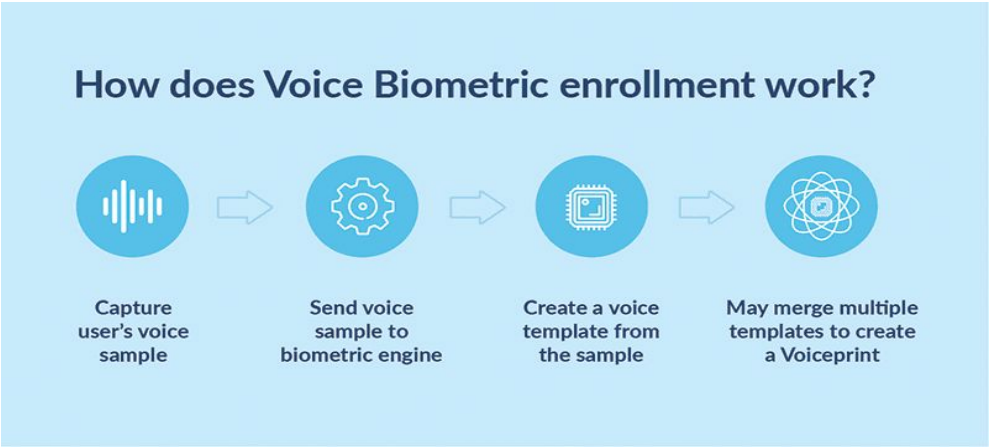
2) Facial Recognition:

- Here the device or the software scans videos and images to create a map of a person's facial features called a facial signature.
- This includes data like their **eyes' precise location, scars, or other facial differences** devices then compare the individual's facial signature to its database.



3) Voice Recognition:

- A voice is captured to a database, and several data points are recorded as parameters for a voiceprint.
- Vocal recognition technologies **focus more on mouth and throat shape formation and sound qualities**.
- The result is a **“voiceprint”** analogous also known as **“voice template.”**
- Voice recognition systems enroll a known person by creating an initial template, often merging several templates from samples of that person’s speech for higher accuracy.
- The initial template is called the enrollment template or enrollment voiceprint.



4) Eye Scanners:

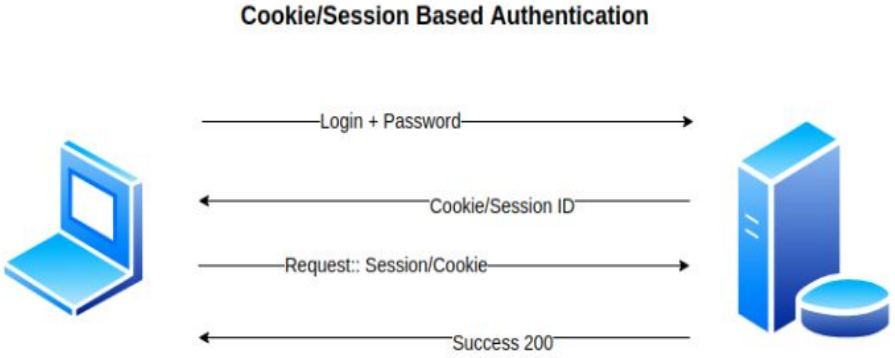
- Eye scanning also known as **Iris scan or iris recognition** .
- The technology used **for the scan directs infrared light into the eye at wavelengths smaller than visible light.** These wavelengths allow the scanner to see more delicate patterns in the i**ris consisting of approximately 240 different features** that, together, comprise a unique digital representation of the user.
- This information is usually **stored in an identity database for authenticating** the users through iris scanning.

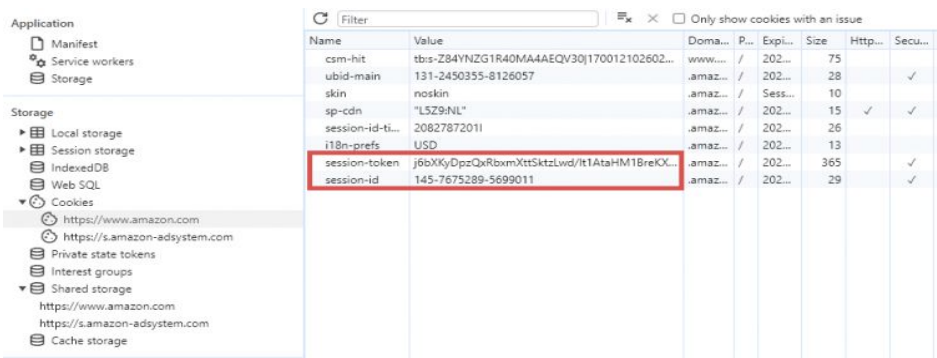
Session Based Authentication

- This is **stateful** authentication
- Use to store the information about the user
- Method of identifying users once logged in.
- This is to secure the authentication .

Working:

- User submits the login request (Username & Password) for authentication.
- Request is sent to the server.
- Server validates the credentials verifying through databases and other servers.
- If the credentials are valid, the server initiates a session and stores the session information in the file system or in the database server.
- Server generates unique identifier (session ID)
- Server sends this unique session identifier to the client.
- Session ID is stored in the cookies
- And for each request the session ID is sent to the server



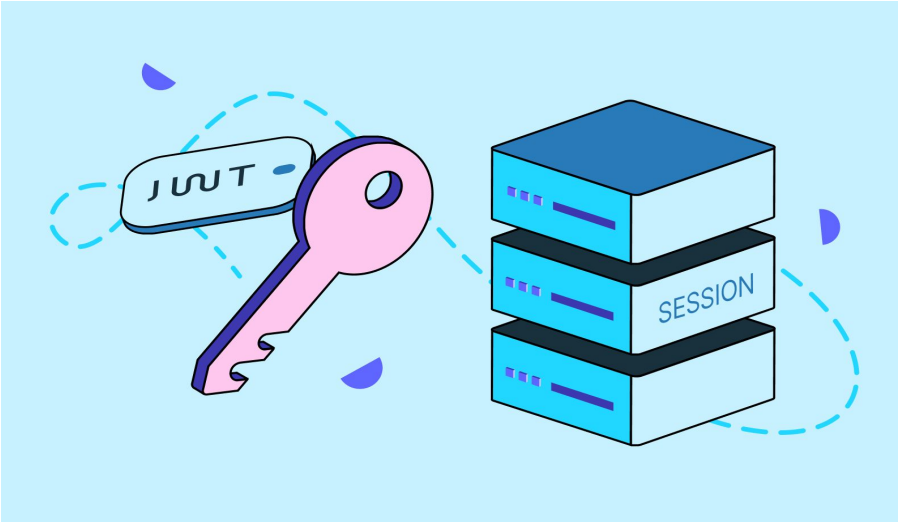


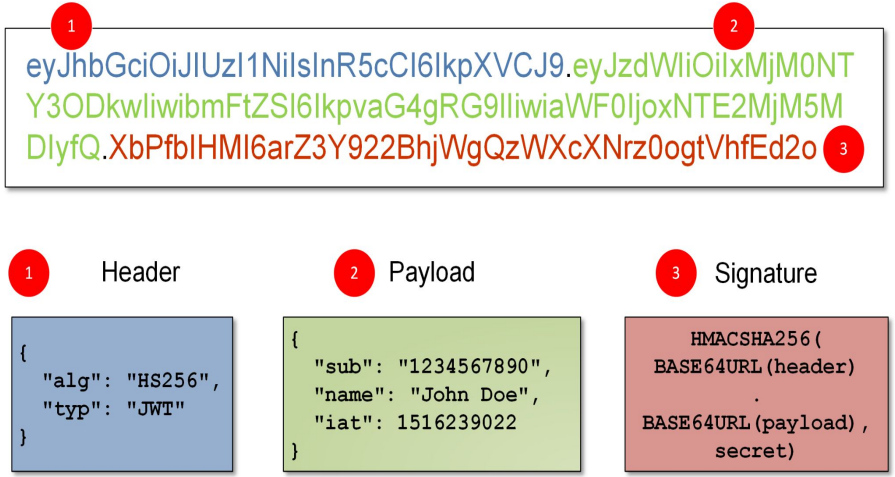
Benefits of Session Based Authentication

- Easy to use
- Storage Size
- Security
- Automatic Expiration
- Scalable

Token Based Authentication

- Verifying the identity by checking a token.
- It's a two-step authentication strategy.
- Token-based authentication is stateless.
- users can directly access the website or application without login requirement.





Types of Token Based Authentication

Connected tokens

Connected tokens are hardware devices that must be **physically inserted** into a computer or device sensor to enable user access to an application or network of resources.

Disconnected tokens

The most popular type, disconnected tokens, are **computer generated**. These tokens facilitate authentication by communicating with servers across distances and through the internet.

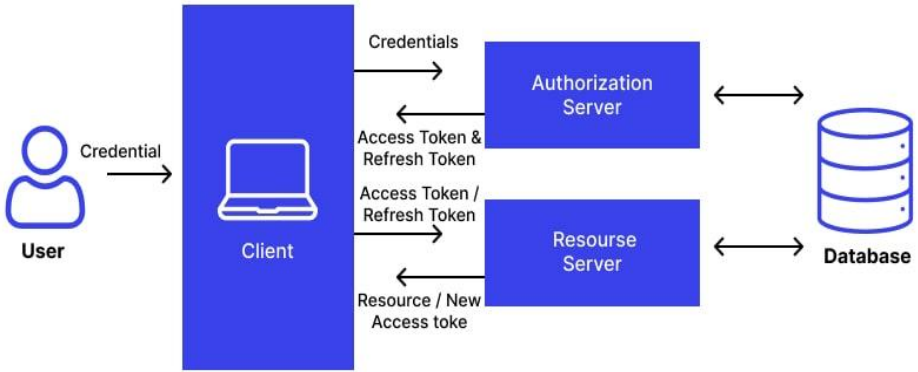
Contactless tokens

Contactless tokens are similar to connected tokens. They're generated by a **hardware device**, but the device doesn't need to be inserted physically.

Instead, the token gets communicated wirelessly when the hardware device is within range of the server or resource the user needs to access. **Bluetooth tokens** are examples of this technology.

Token based authentication works in 4 methods, which are as follows:

1) **Request:** User adds the credentials which involve a username & password.
2) **Verification:** The login info is sent to the authentication server for verification
3) **Token Creation:** Once the user is verified, the server generates a **secret key** which creates a token for the user.
4) **Token validation:** The user receives the token code.
   a) This token may store in the local storage.
   b) Token is the form of JWT.
5) Here, client sends the token to the server not the cookie.
   a) Users sends the token to the resource server with a new request.
   b) Resource servers validates the token for granting access.
   c) Once the token is validated it stores in Database.



Benefits of Token Based Authentication

- Offers robust security
- Flexible
- Very efficient
- Less vulnerable

Certificate Based Authentication

Digital Certificate:

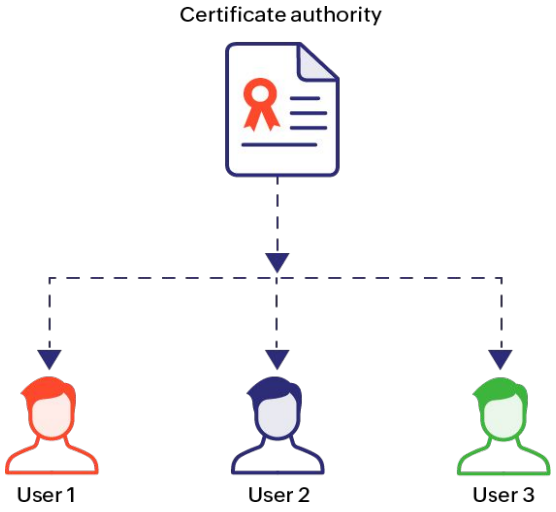
- A digital certificate is a file or electronic passport that proves the authenticity of a device, users.
- It is used to prove your identity by confirming your ownership of a private key.
- Confirms the authenticity of a website to a web browser, known as SSL certificate.
- Contains information, such as a user's name, company, or department and a device's Internet Protocol (IP) address or serial number.

Types of Digital Certificate:

- TLS/SSL certificate
- Domain validated
- Code signing certificate
- Client certificate
- Organization validated
- Domain validated

Certificate Authorities(CA)

- Certificate Authorities, or Certificate Authorities / CAs, issue Digital Certificates.
- CAs issue millions of Digital Certificates each year, which are used to protect information, encrypt billions of transactions, and enable secure communication.
- They issues certificates for websites.
- CAs validate a website domain and, depending on the type of certificate and then issue TLS/SSL certificates.
- Every time you visit a website with HTTPS or see the little padlock in the URL bar, you are using a site that has been verified by a CA. Additionally.
- Anytime you visit a site that says “not secure,” you know that a site has not been validated by a CA or their validation has expired.

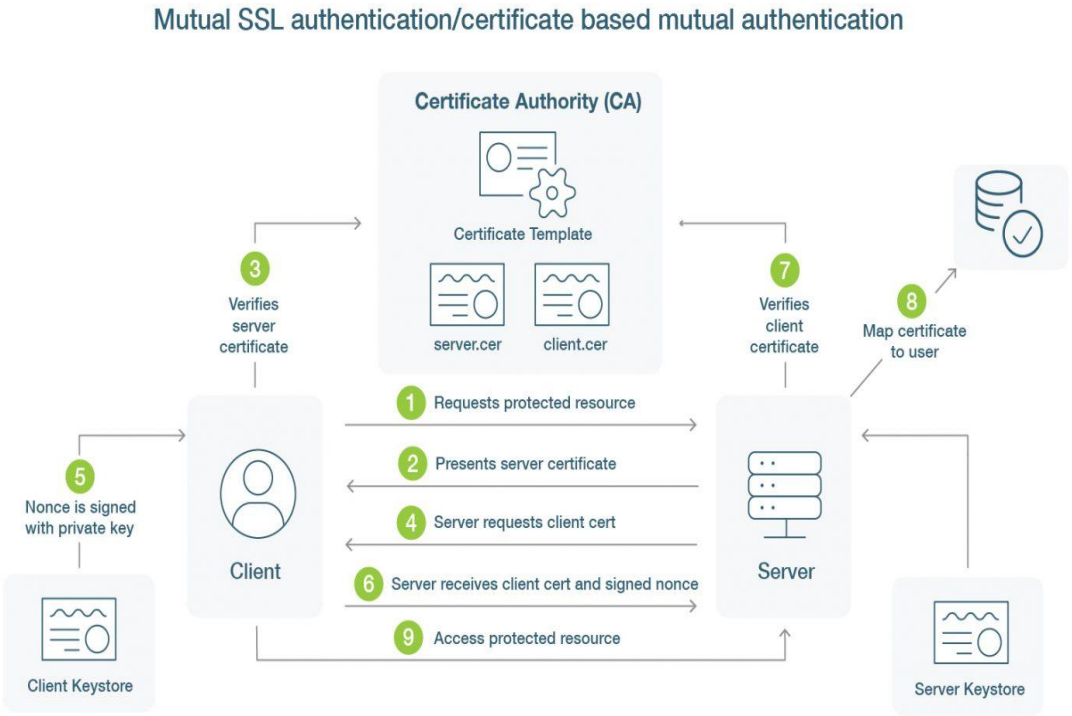


Certificate Based Authentication

- Certificate-based authentication involves the use of digital certificates, which are electronic papers, to confirm your identity.
- this digital certificate verifies your identification by proving you are the owner
- uses a digital certificate created by cryptography to confirm the identity of a person,
- More secure than username & password combinations

Working of certificate based authentication

-

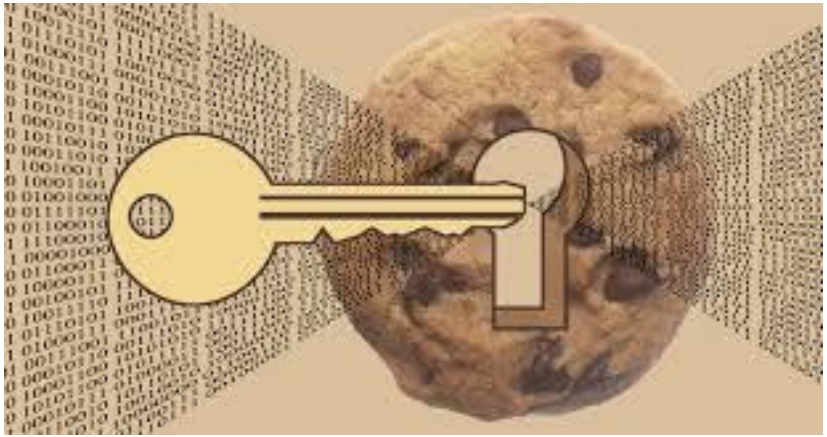


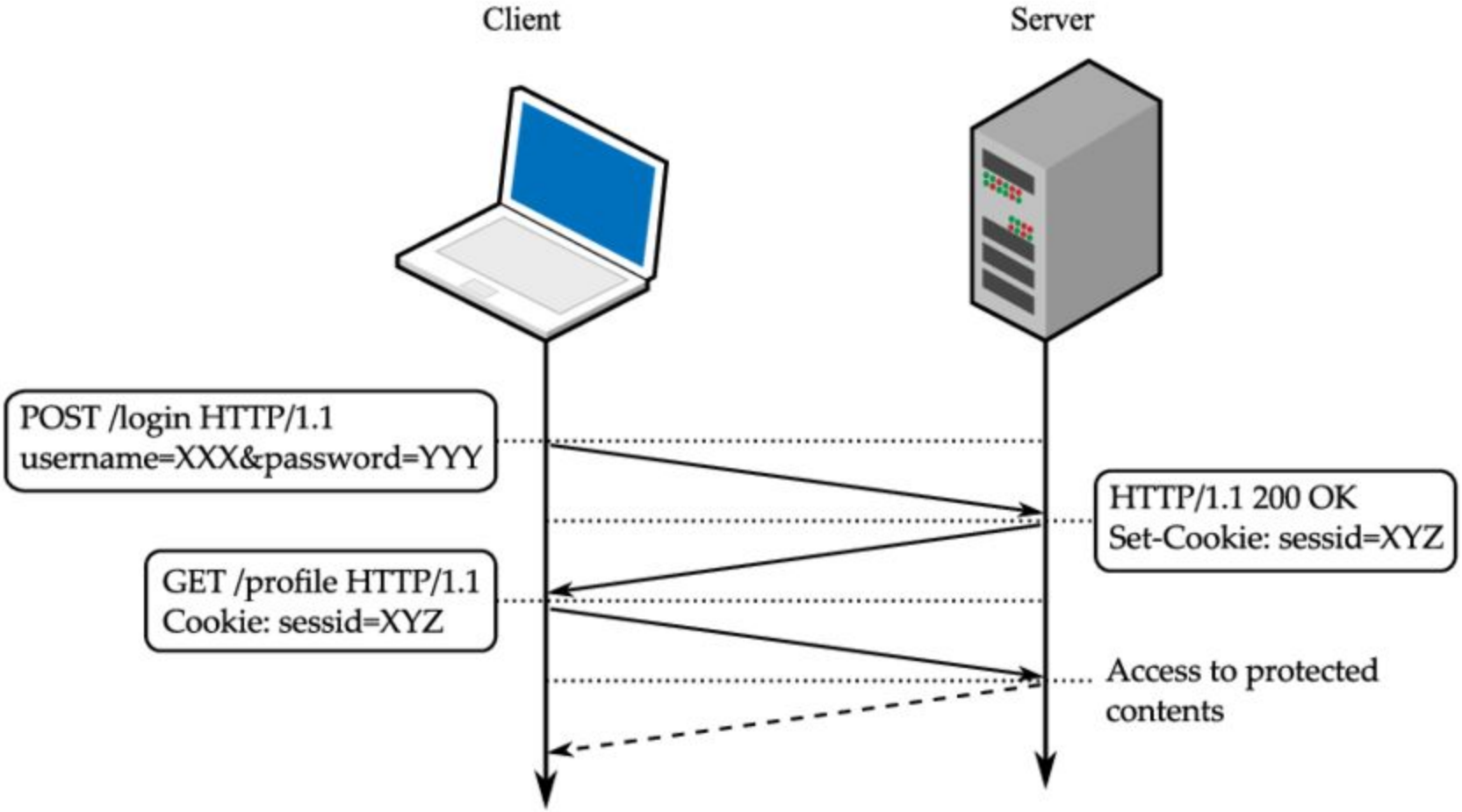
Benefits of CBA

- Cost effective management
- Phishing Resistant
- Single Sign On (SSO) enabled Authentication
- Efficiency in cloud is enabled
- Scalable
- Reduces insecure password practices
- better access controls

Cookie based authentication

- Cookies are **Stateful** authentication
- Cookies are pieces of data used to identify the user and their preferences.
- The browser returns the cookie to the server every time the page is requested.
- Specific cookies like HTTP cookies are used to perform cookie-based authentication to maintain the session for each user.
- The client and the server store the authentication data contained in a cookie
-




Client
Server
POST /login HTTP/1.1
username=XXX&password=YYY
HTTP/1.1 200 OK
Set-Cookie: sessid=XYZ
GET /profile HTTP/1.1
Cookie: sessid=XYZ
Access to protected
contents

Benefits of Cookie Based Authentication

- Convenience
- Scalability
- Personalization
- Less source code
- Small storage
- Safe for XSS attacks

Single Sign On Authentication (SSO)

- Single sign-on (SSO) is a technology which **combines several different application login screens into one.**
- Using SSO a user only has to enter their login credentials (username, password, etc.) one time on a single page to access all of their SaaS applications.
- Single-Sign On (SSO) describes an identity solution that allows multiple applications to use the same authentication session, so avoiding repetitive credential entry.

Example: -

when you try to access Gmail without being authenticated, Google redirects you to a central service(the mainserver) that is hosted at accounts.google.com. There, you will see a sign-in form where you will have to input your user credentials. If the authentication process is successful, then Google redirects you to Gmail, where you gain access to your email account. Then, after authenticating through this central service, if you head to another service (like Youtube, for example), you will see that you are automatically signed in.

SAML

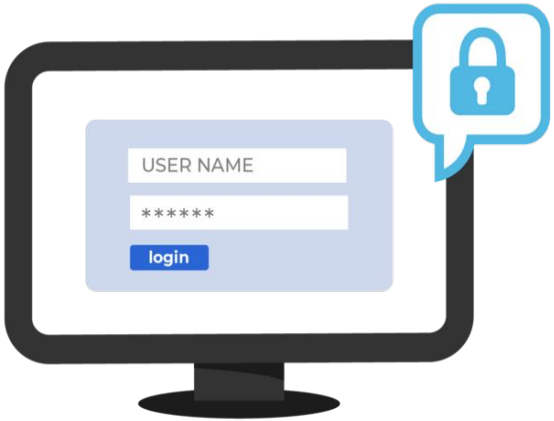
- Security Assertion Markup Language
- **SAML is an XML-based computer language** that facilitates single sign-on.
- (SAML) is a protocol that enables an identity provider (IdP) to send a user's credentials to a service provider (SP) **to authenticate and authorize that user to access a service.**
- It is used for **transferring identity data between two parties**: an identity provider (IdP) and a service provider (SP).
- **Identity Provider** — Performs authentication and passes the user's identity and authorization level to the service provider.
- **Service Provider** — Trusts the identity provider and authorizes the given user to access the requested resource.
-

Authentication Protocols

1) Kerberos : Strongly authenticate the users during the reporting of the application.
2) Lightweight Directory Access Protocol (LDAP) : we can determine the organization, individual, or any other devices during the networking over the internet.
3) OAuth2: It provides permission to the users which are coming through the HTTP servers
4) SAML: It provides authorization between the service provider and the identity provider.
5) RADIUS : provides accounting, centralized authentication, and authorization.

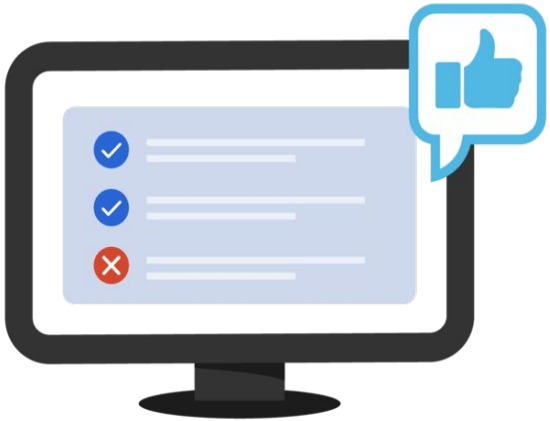
Authorization

Authentication



Confirms users
are who they say they are.

Authorization



Gives users permission
to access a resource.

okta

Authorization

What Authorization?

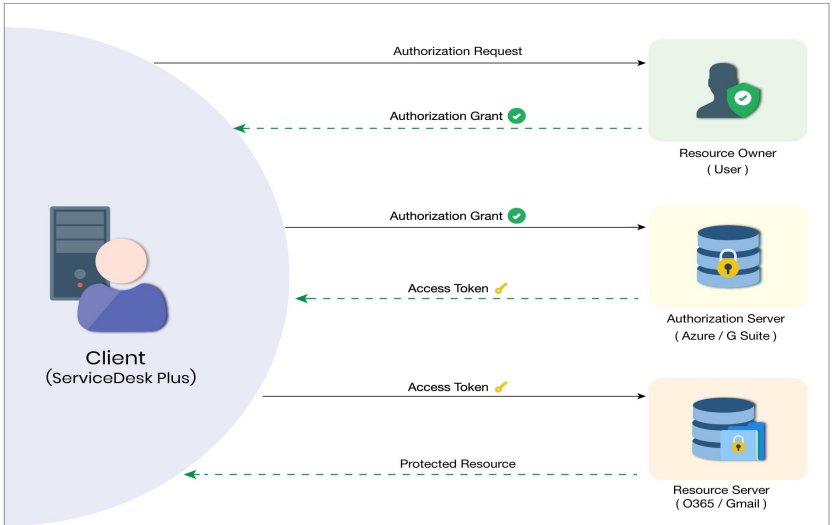
- Authorization is the process of giving someone the ability to access a resource.
- determines the level and type of access to resources
- Authorization decides which user has which level of access.
- In simple terms **“Who can do what”**

Why Authorization?

- To protect the Confidentiality
- To ensure the Availability of the data
- The best practice to secure the data

Working of Authorization

- **Initial authentication:** First, users will authenticate by adding credentials.
- **Authorization request:** Once the user is authenticated, they can request access to a particular resource.
    a. This request includes user details like username, and relevant access to the roles.
- **Access control evaluation:** The access control system receives the authorization request and verifies the access request for the resources, by checking the policies or rules.
- **Authorization decision:** Based on the access control policies, the system makes a decision, either granting or denying the user's request.
- **Activity logging:** Following the authorization decision, the system records all relevant information, such as the time of access, the user's identity, and activity.
    a. This information can be used for auditing and compliance purposes.
- **Revoking permissions:** Access permissions can be withdrawn at any time, either automatically or manually .
    a. When access is revoked, the user can no longer access the resource. Their activities are then logged for auditing and investigation.



Types of Authorization

RBAC
Role-Based Access Control (RBAC)

ABAC
Attribute-Based Access Control (ABAC)

DAC
Discretionary Access Control (DAC)

MAC
Mandatory Access Control

ReBAC
Relationship-Based Access Control

PBAC
Permission-Base d Access Control

Types of Authorization

- **Role-Based Access Control (RBAC):** where permissions are granted based on organizational **job roles or functions.** Users are assigned roles, and these roles determine their access rights.

- **Attribute-Based Access Control (ABAC):** This considers various attributes such as **user attributes, resource attributes,** and environmental conditions when granting access

- **Discretionary Access Control (DAC):** DAC allows resource **owners to determine who can access them**. It's commonly used in file systems, where the owner decides who can read, write, or execute their files

- **Mandatory Access Control (MAC):** MAC enforces strict access policies based on **security labels or classifications.** It's prevalent in government and military settings where data confidentiality and integrity are critical.

- **Relationship-Based Access Control (ReBAC):** ReBAC is a policy model focused exclusively on the relationships or **how resources and identities are connected to each other and between themselves.** These connections are used to implement Authorization

- **Permission-Based Access Control (PBAC):** PBAC grants access based on explicitly defined permissions. Each resource has a list of authorized users or groups; **access is granted to those on the list.**

Benefits & Examples of Authorization

- Building strong digital security
- Protecting CIA trade
- Organization's data will be safe
- Protection Against Insider Threats
- Improve user experience

Examples

- Offboarding former employees
- Working with vendors and contractors
- Admin Roles
- Company Specific roles

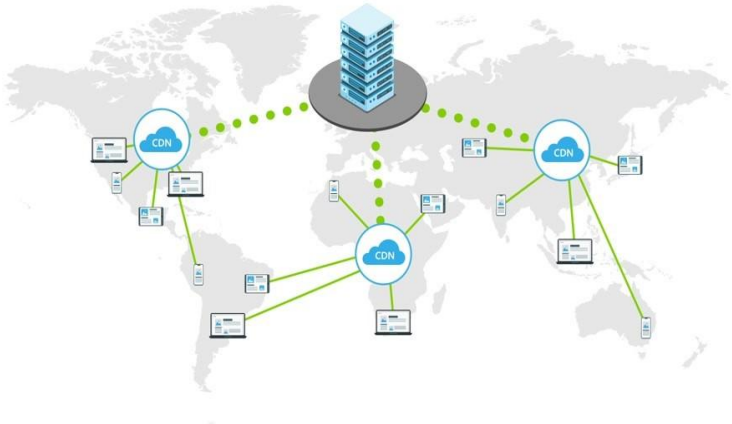
CDN

- A content delivery network (CDN) is a geographically distributed group of servers that caches content close to end users.

- Fast transformation of the data within a geographical distributed servers.

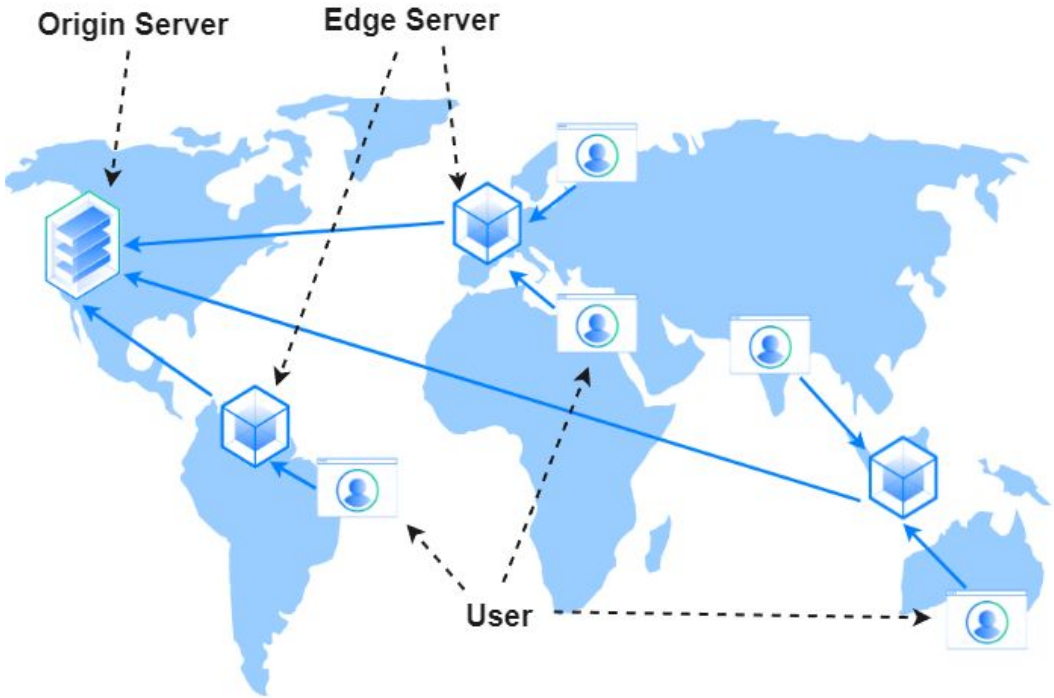
- The primary goal of a CDN is to **improve web performance** by reducing the time needed to send content and rich media to users

- The main motive of this network is to help the servers and applications in **reducing the bandwidth, reducing the downtime and increases the speed of the data.**



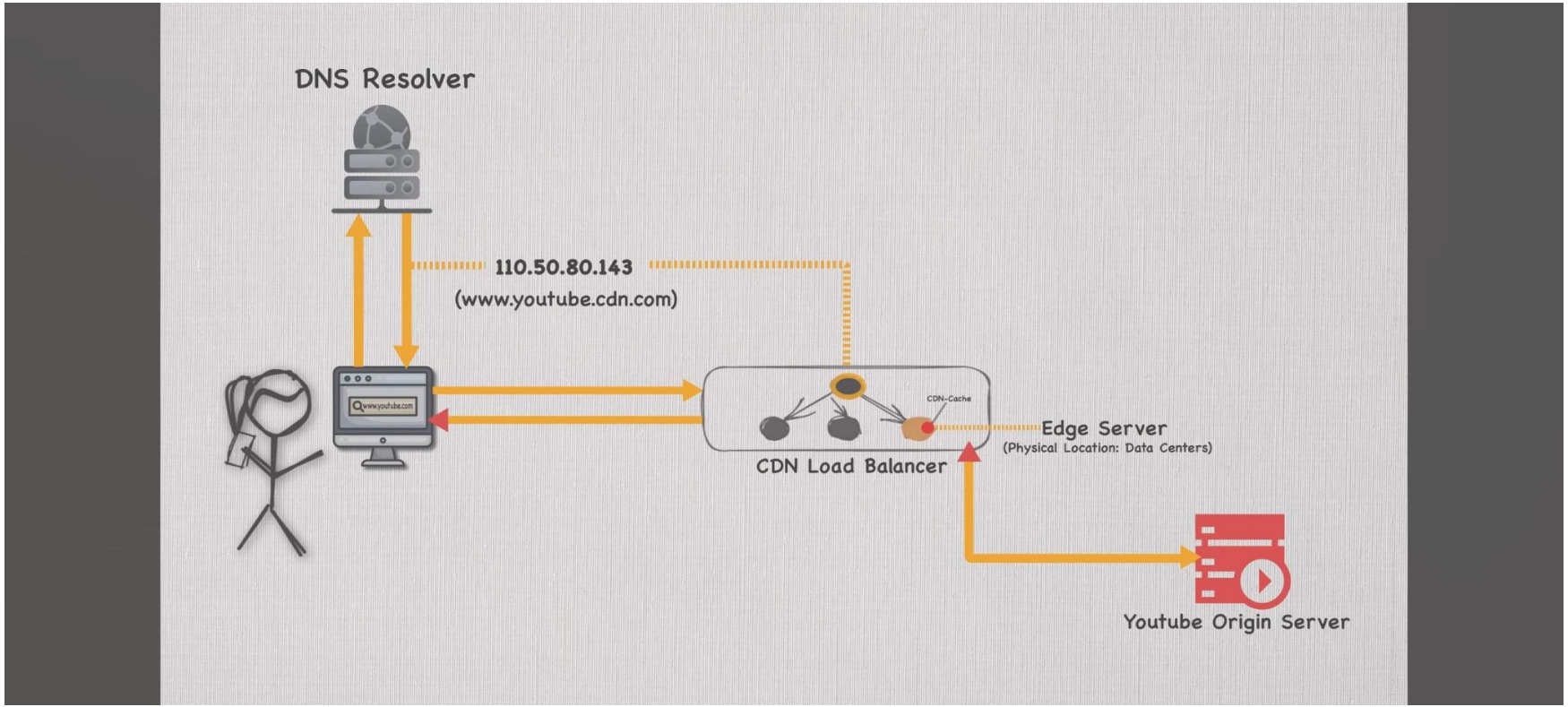
CDN Components

1) Origin Server
2) Edge Server
3) Content Distribution Nodes
4) Cache
5) DNS Resolver
6) Load balancer Algorithm



Content Delivery Network (CDN)

Working of CDN



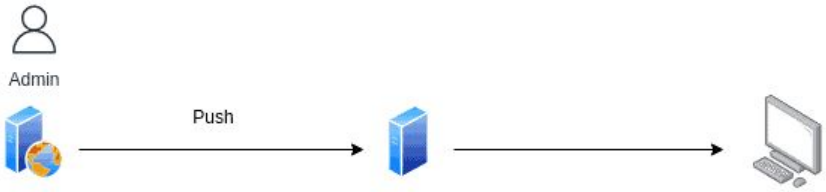
CDN Types

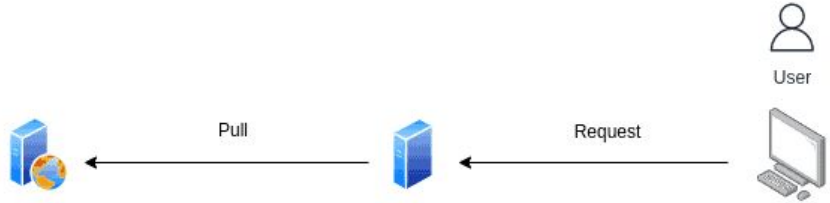
Push CDN:

- content is uploaded or “pushed” to the CDN’s servers in advance of when it is needed.
- This type improves the performance by ensuring the content is available for the users
- Use for caching large files/contents

Pull CDN:

- Content is pulled from the origin server, if the content is not available in the cache of the CDN server.
- The CDN server will fetch the newly updated content from the origin server and gets stored in the cache.
- Less maintenance





CDN Security

1) DoS Attack
2) WAF
3) Enhances SSL/TLS
4) Handles a lot of online traffics

CDN Services Providers

- Cloudflare
- Amazon Cloudfront
- Bootstrap CDN
- Microsoft
- Google
- HP

Operating System

OS - Operating System

- Interface between software and hardware parts of the computer

- Communication channel between software and hardware systems.

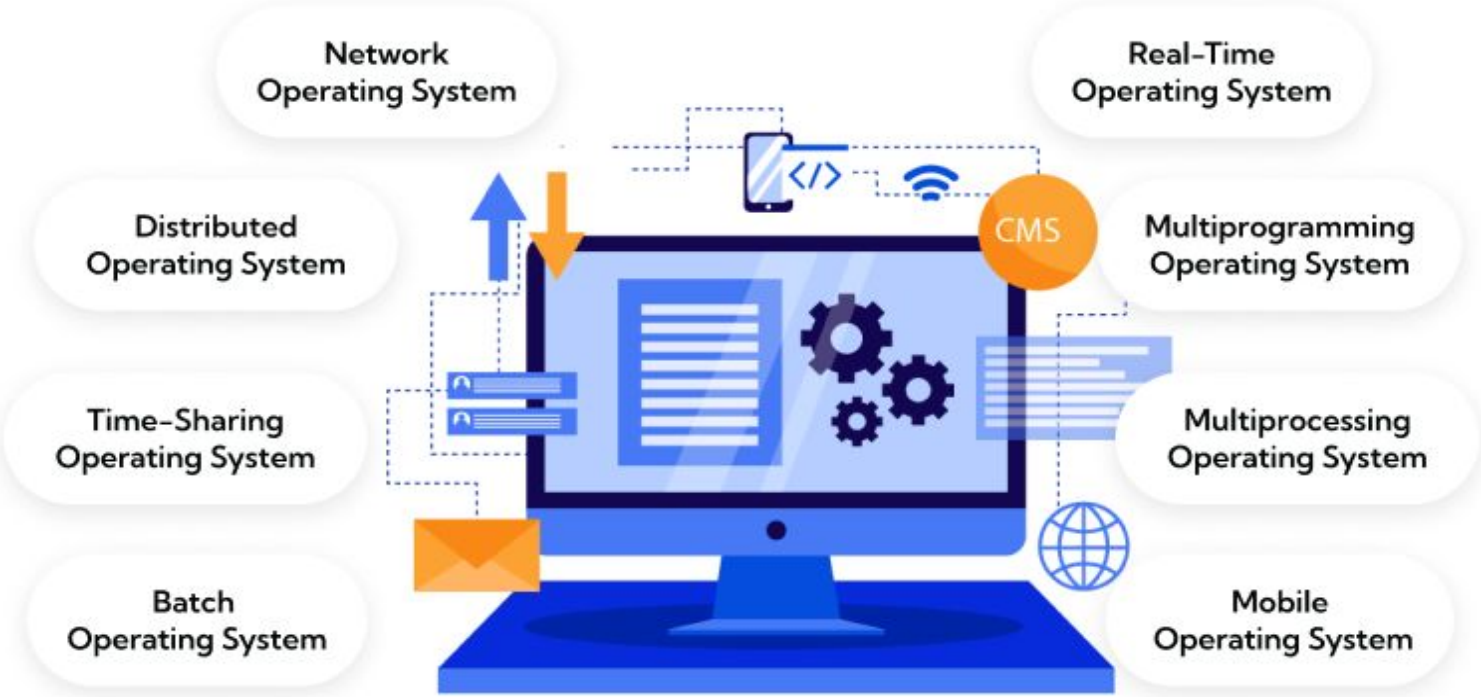
- It is designed in such a way that can manage all the resources and operations of the computers

- It also controls and monitors the execution of all the programs of a computer

Functions of Operating Systems

- Resource Management
- Process Management
- Memory Management
- Security
- Job Accounting
- File Management
- Device Management
- Networking
- Backup and Recovery
- Virtualization
- Performance Monitoring
- System Calls

Types of Operating Systems



Batch Operating System

JOB: Job refers to the commands or the instruction that the user & the program should perform

Job is a mixture of {Program + Input Data + Control Instructions}, this complete data is called job.

Batch: The OS keeps the this number of similar kind of jobs in a memory are called as Batches.

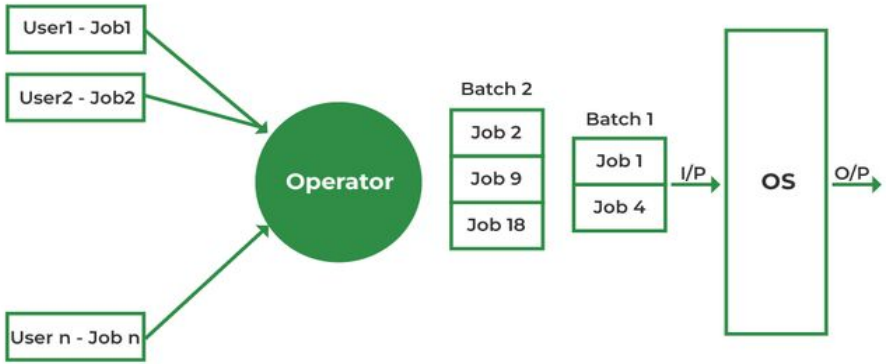
Punch Card: Punch card is a piece of cardstock that stores digital data using punched holes. It is common in data processing and the control of automated machines.

Operator: Operator collects the jobs from different users and sort the jobs into batches with similar needs. Then, operator submits the batches to the processor one by one.

- In batch OS the **user cannot interact with the Operating system** directly to perform task.
- There is an operator who takes similar jobs having the same requirements and groups them into batches.
- The purpose of this operating system was mainly to transfer control from one job to another as soon as the job was completed.
- In this OS when user wants to perform task then the user use to create a job in a punch card.

Working of Batch Operating System:

a) Each Users submit their jobs to the Operator
b) Operators sorts the jobs according to their needs.
c) Similar kind of jobs were handled by a single Batch, another kinds of jobs were handled in another batch
d) Operator checks the batch and sends to the OS.
e) One batch at a time is sent to the OS for the processing,if One batch is done with the processing then the operator sends the another batch for the processing.



Benefits of Batch Operating System

- Reduced Errors
- Cost Effective
- Scalability
- Efficient use of resources
- Can manage Large jobs again and again

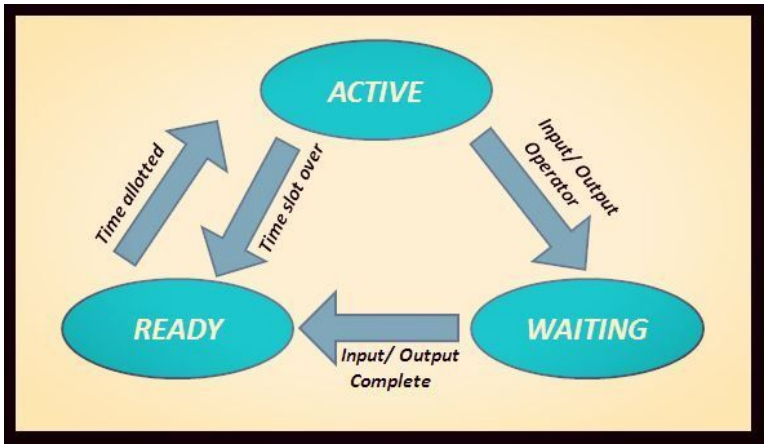
Examples of BOS

- IBM OS/360

- UNIVAC EXEC 8

Time Sharing Operating System

- This OS can execute **multiple processes at the same time.**
- CPU provides a allotted time period to each an every process to complete its task.
- It uses **CPU scheduling and multiprogramming** for every user,
- Each task is given a certain amount of time to complete so that everything runs properly.
- It is also known as **Multitasking OS.**
-



Time Sharing Operating System

Processes: User who performs task to be executed.

CPU Scheduling: CPU scheduling is a process which allows one process to use the CPU while the execution of another process is on hold

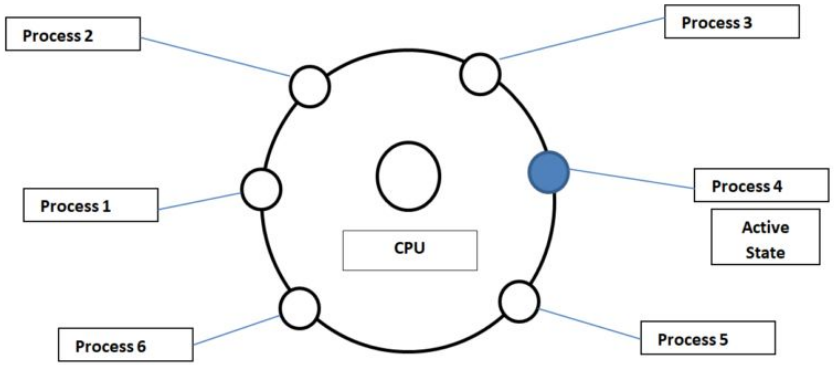
Quantum: A particular duration of time assigned to each task to be executed in the CPU.

Active State: This is the state of the process which is currently processing on the CPU. Only, one process is in the active state at a time.

Ready State: In this state, the process is ready for execution but, it is waiting for its turn to use the CPU. More than one process can be in the ready state at a time..

Working of Time Sharing OS:

a) Suppose, 6 Processes are running in the system
b) The Quantum time allocated is 10 sec
c) Now each process starts executing
d) Process P1, will execute first for 10 sec, It doesn't matter how long or short the process could be.
e) Once the execution of the process P1 completed, P2 will be executed for 10 sec.
f) One process runs at a time
g) This process continues till all the processes gets complete.
h) P4 is in the active state and p5 is in the ready state.



Benefits of Time sharing Operating system

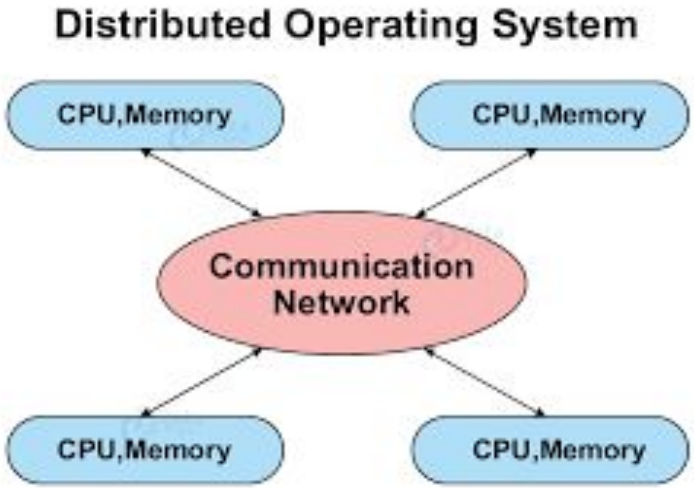
1. Each task gets an equal opportunity.
2. Fewer chances of duplication of software.
3. CPU idle time can be reduced.
4. Multiple users can work on same computer
5. Waiting period is less

Examples:

- Multics
- UNIX
- Linux
- Windows NT server
- Windows 2000 server

Distributed Operating System

- It connects **multiple computers via a single communication channel.**
- Each of these systems has its own processor and memory.
- This operating system consists of numerous computers, nodes, and sites joined together via **LAN/WAN** lines.
- Here, each system has its own cpu and processor only software can communicates with each other



Types of Distributed Operating System

1. **Client-Server Systems**

   clients request services from servers over a network.

   Clients initiate communication, send requests, and handle user interfaces, while servers listen for requests, perform tasks, and manage resources.

2. **Peer-to-peer System**

   The task is evenly distributed among the nodes.

   Additionally, these nodes can share data and resources as needed. Once again, they require a network to connect.

Benefits of Distributed Operating system

- Better Performance
- Cost Effectivity
- Efficiency
- Geographic Distribution
- Reduced Cost
- Flexibility

Examples of Distributed Operating System

Solaris

Micros

DYNIX

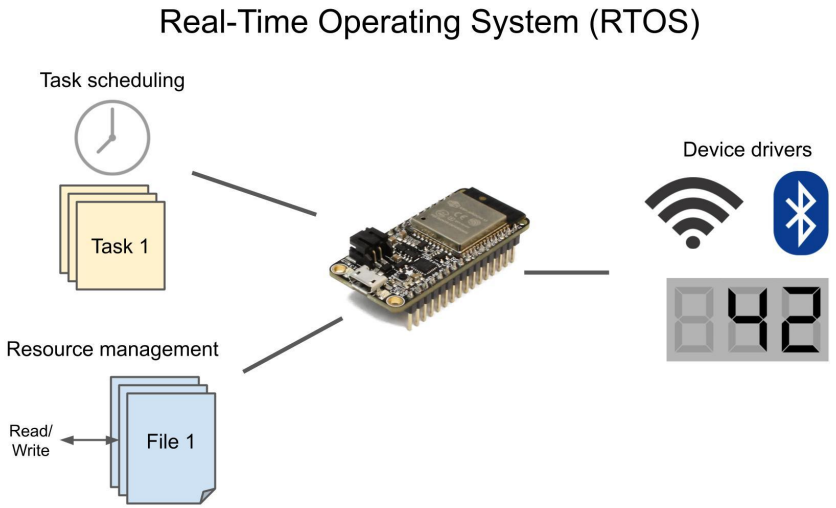
Mach

Ubuntu

Linux

Real Time Operating System

- A real-time operating system (RTOS) is a specialized operating system designed to **handle time-critical tasks within certain deadlines.**
- Jobs are performed quickly as possible.
- CPU provides maximum efforts
- OS has strict time constraints to perform jobs
- Communicated through sensors
- This system is time-bound and has a **fixed deadline.**



Types of Real time Operating System

Soft RTOS:

- A soft real-time RTOS **tolerates operating system delays.**
- Allows deadlines to certain jobs but can tolerate small-time delays.
- if the deadline is missed multiple times, that can lead to system failure.
- Example - Video games rely on user input and have limited time to process;

Hard RTOS:

- A hard real-time RTOS are very strict.
- Deadlines should be executed in allotted time.
- Does **Not accept any delays**
- Example - Air bag

RTOS

- **Priority Based Scheduling :** It's an algorithm that schedules processes according to the priority assigned to each of the processes.
- Higher priority processes are executed before lower priority processes.

- **Interrupt**: Interrupt is a signal that indicates to the CPU that an event needs immediate attention. (Like a system call, error in the software etc.)

- **Interrupt Handler:** Refers to the process by which an operating system manages interrupts when they occur. CPU stops the execution and transfers the control to the specific interrupt handler.

Working of RTOS

- Real-time has specified Deadlines assigned.
- The task are performed according to the priority Based Scheduling.
- Higher priority task should been implemented before lower priority task
- RTOS are efficient in interrupt handling, they must be able to respond to interrupts promptly to meet the system's timing requirements.
- RTOS includes various mechanism context switching, minimizing interrupt disabling time, and providing task synchronization

Benefits of Real time Operating System

- Reduced downtime
- Availability
- Dependability
- Task Administration
- Error-free.

Example of RTOS

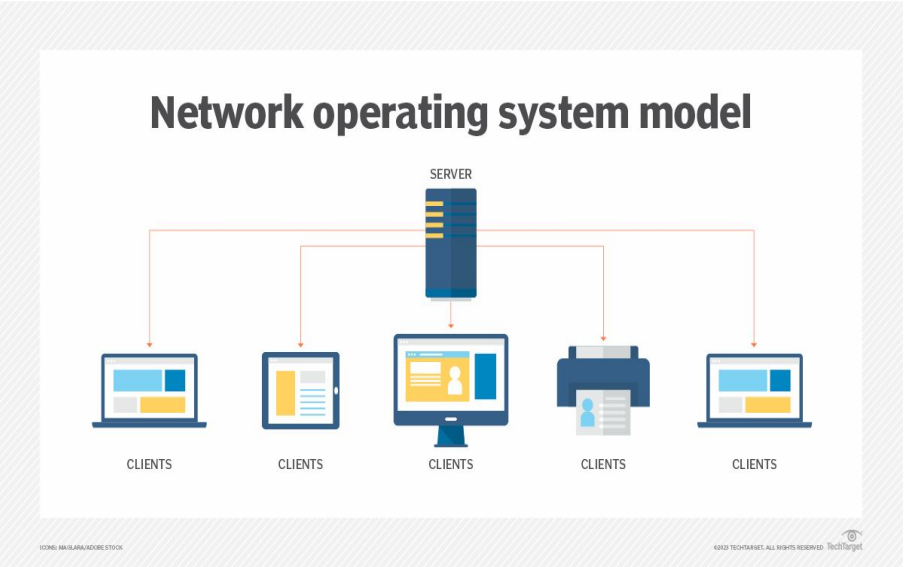
- airline traffic control systems
- Command Control Systems
- airline reservation systems
- Heart pacemakers
- Network Multimedia Systems
- Robots

Network Operating System

- An Operating system, which includes software and associated protocols to communicate with other computers is called Network Operating System.
- Its primary function is to enable file sharing and provide access to printers, disks, devices, etc on a private network,

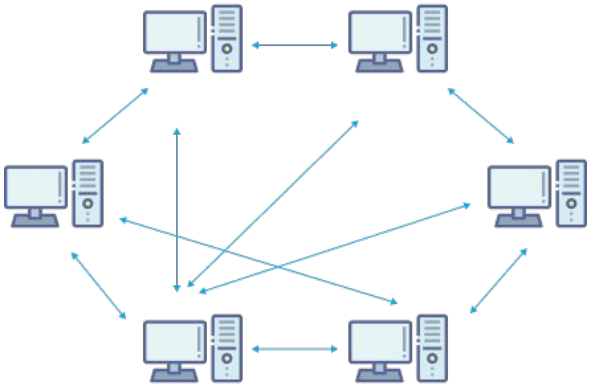
Functions of Network Operating Systems

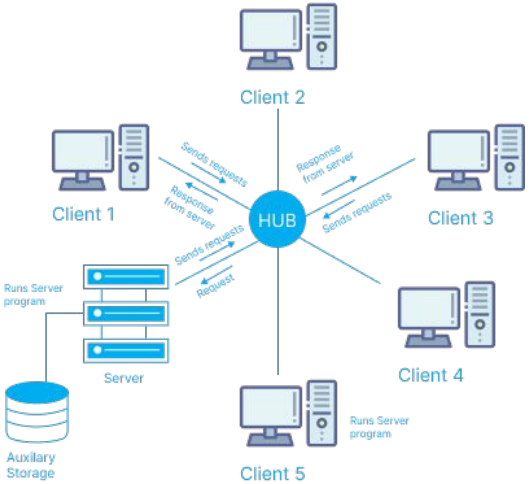
- Creating and managing user accounts on the network.
- Controlling access to resources on the network.
- Provide communication services between the devices on the network.
- Monitor and troubleshoot the network.
- Configuring and Managing the resources on the network.



Types of Network OS

- **Peer to Peer:**
  - Peer-to-peer NOS allow the sharing of resources and files with **small-sized networks.**
  - have fewer resources
  - They work on LAN
- **Client/server:**
  - Client-server NOS provide users access to resources through the **central server.**
  - Expensive to implement and maintain.
  - Good for the big networks which provide many services.





Benefits of Network Operating System

- high level of stability from central computers.
- Authentication and access control for security
- The network is readily upgradeable.
- Provide remote access to servers from different locations.

Examples:

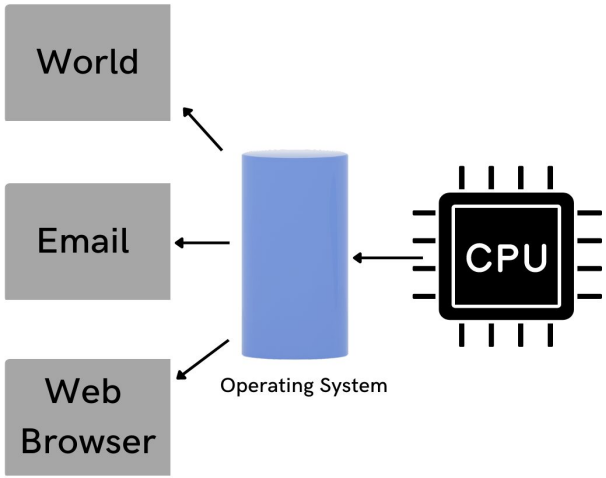
- UNIX,
- Linux,
- Microsoft Windows Server 2008,
- Microsoft Windows Server 2003,
- Mac OS X,
- BSD.

Multiprogramming OS

- A multiprogramming operating system is a type of operating system that allows **multiple programs to run simultaneously on a single CPU.**
- The primary goal of multiprogramming is to manage the entire system's resources.
- The key components of a multiprogramming system are the file system, command processor, transient area, and I/O control system.

- There two types of Multiprogramming OS
  - Multitasking OS
  - Multiprocessor OS

-



Multiprogramming Operating System

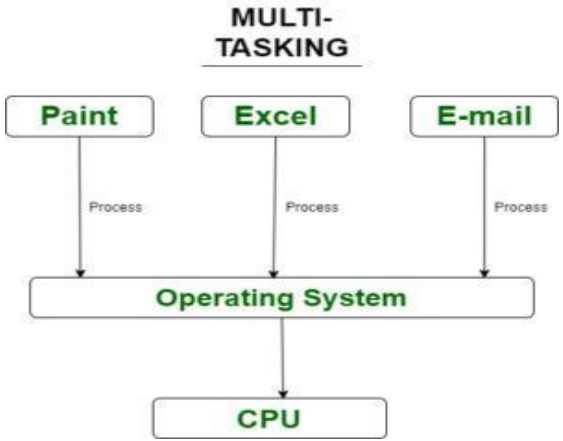
Types of Multiprogramming OS

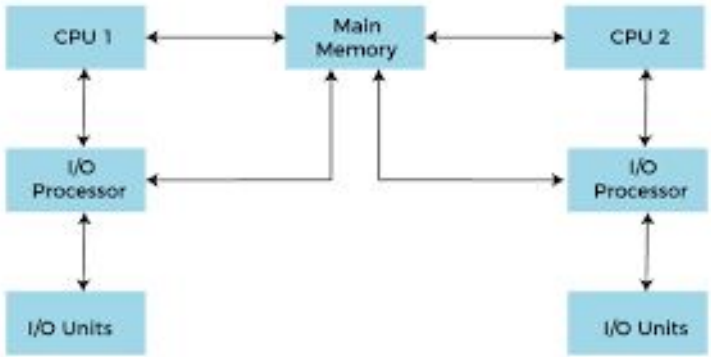
Multitasking OS

- A multitasking operating system enables the execution of **two or more programs at the same time.**
- users can run multiple programs and tasks simultaneously.
- The operating system keeps track of each job and allows you to switch between jobs without allowing the data to be lost.

Multiprocessor OS:

- To improve the performance **more than one CPU is been used** within one system.
- Multiple CPUs are interconnected so that a job can be divided among them for faster execution.
- Multiple CPUs can also be used to run multiple jobs simultaneously.





Working of Multiprocessor System

The main benefits of Multiprogramming OS are:

- It provides less response time.
- Helps to run various jobs in a single application simultaneously.
- Optimizes the total job of the computer.
- Various users may use the multiprogramming system at once.
- It helps in improving CPU utilization and never gets idle.
- The resources are utilized smartly.

Examples:

- Download software
- transfer data,
- Google Chrome,
- MS-Excel,
- Firefox browser,

References

- https://www.cloudflare.com/learning/privacy/what-are-cookies/
- https://www.kaspersky.com/resource-center/definitions/cookies
- **https://www.tutorialspoint.com/internet-cookies-and-their-types**
- **https://www.baeldung.com/cs/web-sessions#:~:text=The%20session%20ID%20allows%20the,and%20preferences%20throughout%20the%20site.**
- **https://www.geeksforgeeks.org/how-does-the-token-based-authentication-work/**
- **https://www.strongdm.com/blog/token-based-authentication#:~:text=What%20is%20a%20token?,JWT**
- **https://www.geeksforgeeks.org/how-does-the-token-based-authentication-work/**
- **https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-biometric-authentication-definition-benefits-tools/**
- **https://www.1kosmos.com/biometric-authentication/fingerprint-authentication/**
- **https://us.norton.com/blog/iot/how-facial-recognition-software-works**
- **https://www.idrnd.ai/voice-biometrics/**
- **https://www.1kosmos.com/biometric-authentication/iris-biometrics/**
- **https://www.cloudflare.com/learning/access-management/token-based-authentication/**
- **https://www.fortinet.com/resources/cyberglossary/single-sign-on**
- **https://www.geeksforgeeks.org/how-does-the-token-based-aut hentication-work/**
- **https://auth0.com/intro-to-iam/what-is-single-sign-on-sso**
- https://www.cloudflare.com/learning/cdn/what-is-a-cdn/
- https://docs.google.com/presentation/d/1mh4IOzXkSQaf2pYJYHImyvkOeoMpNsyxHZ1xfNbVETs/edit#slide=id.g2d9f8b8ad61_0_3

- https://rocketcdn.me/cdn-security/
- https://www.geeksforgeeks.org/what-is-an-operating-system/
- https://www.shiksha.com/online-courses/articles/learning-about-time-sharing-operating-system/
- https://www.spiceworks.com/tech/hardware/articles/what-is-rtos/
- https://www.geeksforgeeks.org/what-is-a-network-operating-system/
- https://www.geeksforgeeks.org/advantages-and-disadvantages-of-distributed-systems/
- https://www.shiksha.com/online-courses/articles/real-time-operating-system/
- https://www.geeksforgeeks.org/how-does-the-token-based-authentication-work/
- https://www.fortinet.com/resources/cyberglossary/digital-certificates
- https://www.geeksforgeeks.org/how-does-certificate-based-authentication-work/
- https://www.yubico.com/resources/glossary/what-is-certificate-based-authentication/
- https://dev.to/emmykolic/cookies-based-authentication-vs-session-based-authentication-1f6
- https://www.descope.com/learn/post/authorization
- https://amazic.com/6-types-of-authorizations-and-how-to-choose-the-best-one-for-your-company/
- https://www.netsuite.com/portal/resource/articles/erp/authorization.shtml


Thank you