Information Assurance Model in Cyber Security

Information Assurance concerns implementation of methods that focused on protecting and safeguarding critical information and relevant information systems by assuring confidentiality, integrity, availability, and non-repudiation. It is strategic approach focused which focuses more on deployment of policies rather than building infrastructures.

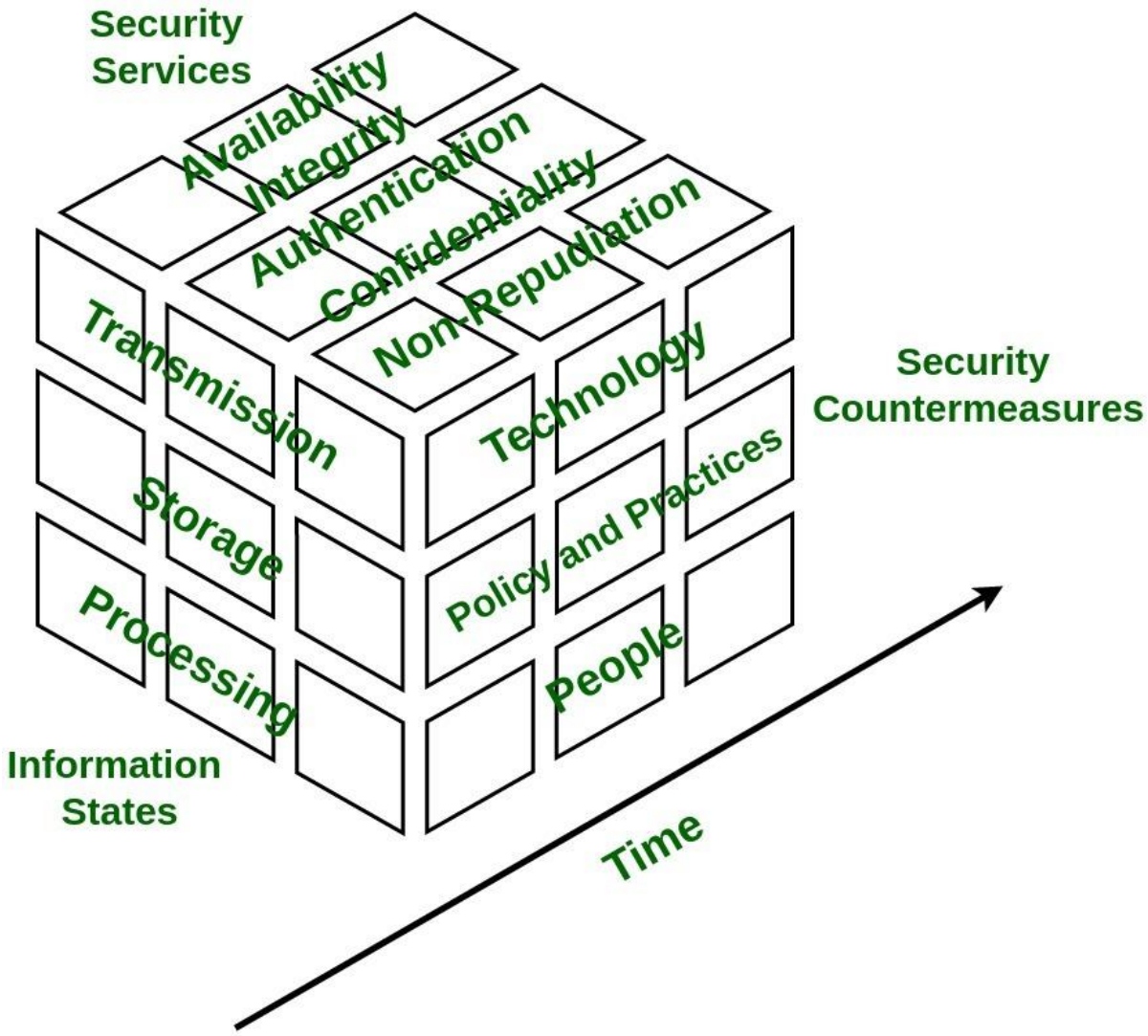
Information Assurance Model :
The security model is multidimensional model based on four dimensions :

1. **Information States –**
   Information is referred to as interpretation of data which can be found in three states stored, processed, or transmitted.

2. **Security Services –**
   It is fundamental pillar of the model which provides security to system and consists of five services namely availability, integrity, confidentiality, authentication, and non-repudiation.

3. **Security Countermeasures –**
   This dimension has functionalities to save system from immediate vulnerability by accounting for technology, policy & practice, and people.

4. **Time –**
   This dimension can be viewed in many ways. At any given time data may be available offline or online, information and system might be in flux thus, introducing risk of unauthorized access. Therefore, in every phase of System Development Cycle, every aspect of Information Assurance model must be well defined and well implemented in order to minimize risk of unauthorized access.



Information States :

1. **Transmission –**
   It defines time wherein data is between processing steps.

   Example :
   In transit over networks when user sends email to reader, including memory and storage encountered during delivery.

2. **Storage –**
   It defines time during which data is saved on medium such as hard drive.Example: Saving document on file server's disk by user.

3. **Processing –**
   It defines time during which data is in processing state.

Example :
Data is processed in random access memory (RAM) of workstation.

Security Services :

1. **Confidentiality –**
   It assures that information of system is not disclosed to unauthorized access and is read and interpreted only by persons authorized to do so. Protection of confidentiality prevents malicious access and accidental disclosure of information. Information that is considered to be confidential is called as **sensitive information**.

   To ensure confidentiality data is categorized into different categories according to damage severity and then accordingly strict measures are taken.

   Example :
   Protecting email content to read by only desired set of users. This can be insured by data encryption. Two-factor authentication, strong passwords, security tokens, and biometric verification are some popular norms for authentication users to access sensitive data.

2. **Integrity –**
   It ensures that sensitive data is accurate and trustworthy and can not be created, changed, or deleted without proper authorization. Maintaining integrity involves modification or destruction of information by unauthorized access.

   To ensure integrity backups should be planned and implemented in order to restore any affected data in case of security breach. Besides this cryptographic checksum can also be used for verification of data.

   Example :
   Implementation of measures to verify that e-mail content was not modified in transit. This can be achieved by using cryptography which will ensure that intended user receives correct and accurate information.

3. **Availability –**
   It guarantees reliable and constant access to sensitive data only by authorized users. It involves measures to sustain access to data in spite of system failures and sources of interference.

   To ensure availability of corrupted data must be eliminated, recovery time must be speed up and physical infrastructure must be improved.

   Example :
   Accessing and throughput of e-mail service.

4. **Authentication –**
   It is security service that is designed to establish validity of transmission of message by verification of individual's identity to receive specific category of information.

   To ensure availability of various single factors and multi-factor authentication methods are used. A single factor authentication method uses single parameter to verify users' identity whereas two-factor authentication uses multiple factors to verify user's identity.

   Example :
   Entering username and password when we log in to website is example of authentication. Entering correct login information lets website verify our identity and ensures that only we access sensitive information.

5. **Non-Repudiation –**
   It is mechanism to ensure sender or receiver cannot deny fact that they are part of data transmission. When sender sends data to receiver, it receives delivery confirmation. When receiver receives message it has all information attached within message regarding sender.

   Example :
   A common example is sending SMS from one mobile phone to another. After message is received confirmation message is displayed that receiver has received message. In return, message received by receiver contains all information about sender.

Security Countermeasures :

1. **People –**
   People are heart of information system. Administrators and users of information systems must follow policies and practice for designing good system. They must be informed regularly regarding information system and ready to act appropriately to safeguard system.

2. **Policy & Practice –**
   Every organization has some set of rules defined in form of policies that must be followed by every individual working in organization. These policies must be practiced in order to properly handle sensitive information whenever system gets compromised.

3. **Technology –**
   Appropriate technology such as firewalls, routers, and intrusion detection must be used in order to defend system from vulnerabilities, threats. The technology used must facilitate quick response whenever information security gets compromised.

Following is a table of differences:

S. No.	Information Assurance	Information Security
1.	It is a practice of assuring and managing the risk and threats related to the company's information.	It is a practice of protecting information by mitigating the risks related to information.
2.	Information assurance is more concerned with the overall risks to be found in the company's data.	Information security helps prevent unauthorized access, use, disclosure, disruption, modification, or destruction of the data.
3.	The five main pillars of information assurance are to ensure the availability, integrity, authenticity, confidentiality, and non-repudiation of the company's data.	The main three motives of information security are to provide integrity, confidentiality, and availability of data.
4.	Information assurance often employs the application of organizational-wide standards to reduce the threats to data.	Information security pays more attention to developing tools, technologies, and other measures to secure the data.
5.	Information assurance is the main branch, that works with information security to provide protection to data.	Information security is a sub-unit of information assurance.
6.	Information assurance includes the tasks like restoration of information systems by incorporating protection, detection, and reaction capabilities.	Information security can be achieved through security solutions, encryption, and other technology, and processes.
7.	The work of Information assurance is more focused on organizational risk management and the overall quality of the data.	The work of Information security is to provide a safe method to reduce the risks like unwanted access, compromise, or stealing data,
8.	Information assurance includes the methods like Security audits, network architecture, compliance audits, database administration, implementation, and enforcement of organisational information management policies.	On the other hand, information security provides the functions like Vulnerability management, penetration testing, and technology solutions such as firewalls, anti-virus, data loss prevention, and encryption.

Advantages related to information security:

- **It provides security to all confidential information:** An information security provides security to all the information that needed to be protected, whether, it's an intangible asset, organizational secrets, or Personal information. it makes no difference, whether it is in physical or digital form.
- **Serves against cyber-attacks and threats:** the information security safeguards against cyber-attacks and hacking threats. it increases the resilience of the organization against cyber-attacks.
- **It reduces the unnecessary costs regarding security:** A risk assessment and analysis method of information security is a reliable and cost-effective method,

which, as a result, allows the organizations to save money instead of investing it in putting layers on layers of defensive technologies, which may not be proved as effective.

- **Ensuring the confidentiality, integrity, and availability of information:** Information security is a method that uses a set of policies, as well as technical and physical controls, to help safeguard an organization's confidential data, while ensuring its integrity and availability of it.

Advantages related to information assurance

- **Enhances the data protection:** the first and most important benefit that information assurance provides is the protection of the confidential data of an organization. It helps enhance the protection of the company data to keep it safe from all sorts of threats.
- **Reduces the overall risk of cyber attacking:** Information assurance is a method that is more concerned with the overall risk of the company's data being lost or stealthy. It typically involves implementing organizational-wide standards to mitigate vulnerabilities to information security.
- **Risk management:** The key aspect of information assurance is that it works closely with risk management techniques, which means that it can determine when and how to take action to reduce risk.
- **Ensures the Quality, Dependability, and Retrievability;** The purpose of information assurance is to ensure the quality, dependability, and retrievability of data so that it can be easily reachable and can be used when needed. while also protecting it. And for this, it employs a variety of approaches and procedures.

arameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.

arameters	CYBER SECURITY	INFORMATION SECURITY
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defence	Acts as first line of defence.	Comes into play when security is breached.
Threats	Primarily deals with digital threats, such as hacking, malware, and phishing	Addresses a wider range of threats, including physical theft, espionage, and human error
Goal	Protects against unauthorized access, use, disclosure, disruption, modification, or destruction of digital information	Protects the confidentiality, integrity, and availability of all types of information, regardless of the medium in which it is stored
Technologies	Relies on a variety of technologies, such as firewalls, antivirus software, and intrusion detection systems	Uses a range of technologies, including encryption, access controls, and data loss prevention tools
Skills required	Requires specialized knowledge of computer systems and networks, as well as programming and software development skills	Requires knowledge of risk management, compliance, legal and regulatory issues, as well as technical knowledge
Focus on data	Emphasizes protecting the data itself, regardless of where it is stored or how it is transmitted	Emphasizes the protection of information assets, which includes data but also other information such as intellectual property, trade secrets, and confidential customer information
Threat landscape	Deals with constantly evolving threats, such as new forms of malware and emerging cybercrime techniques	Deals with a wide range of threats, including physical security breaches, insider threats, and social engineering attacks

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

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

Features Of Cryptography are as follows:

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

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

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

Applications Of Cryptography:

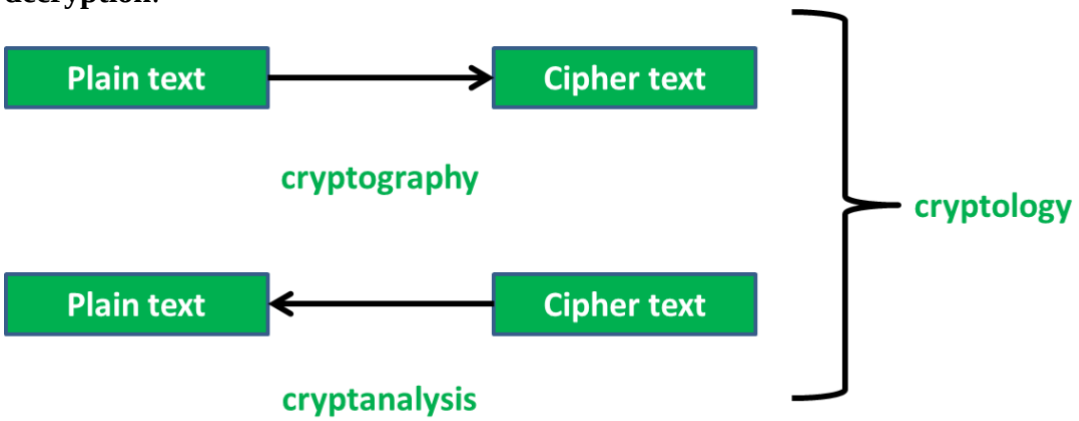
1. **Computer passwords:** Cryptography is widely utilized in computer security, particularly when creating and maintaining passwords. When a user logs in, their password is hashed and compared to the hash that was previously stored. Passwords are hashed and encrypted before being stored. In this technique, the passwords are encrypted so that even if a hacker gains access to the password database, they cannot read the passwords.
2. **Digital Currencies:** To safeguard transactions and prevent fraud, digital currencies like Bitcoin also use cryptography. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
3. **Secure web browsing:** Online browsing security is provided by the use of cryptography, which shields users from eavesdropping and man-in-the-middle assaults. Public key cryptography is used by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data sent between the web server and the client, establishing a secure channel for communication.
4. **Electronic signatures:** Electronic signatures serve as the digital equivalent of a handwritten signature and are used to sign documents. Digital signatures are created using cryptography

and can be validated using public key cryptography. In many nations, electronic signatures are enforceable by law, and their use is expanding quickly.

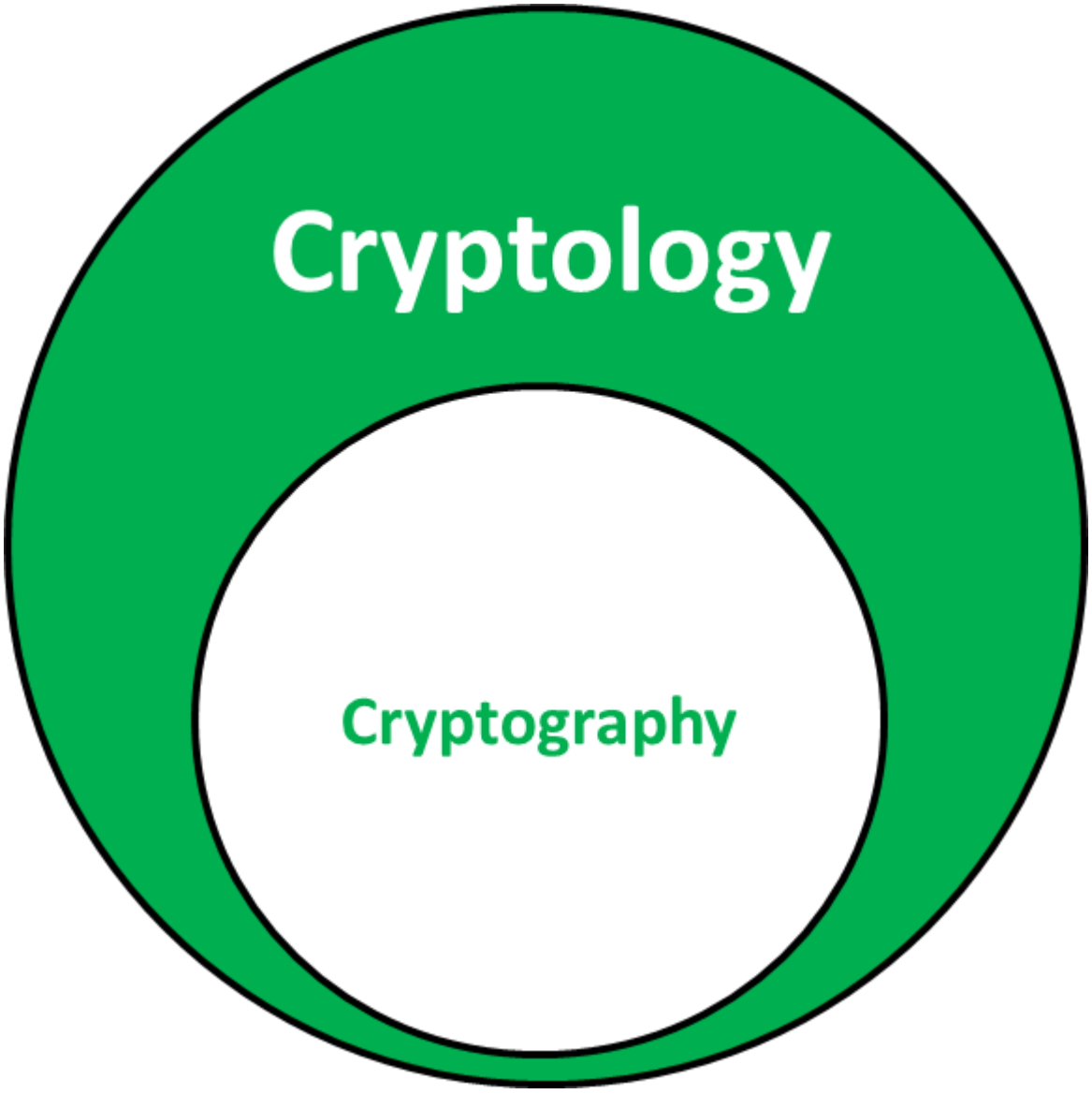
5. **Authentication:** Cryptography is used for authentication in many different situations, such as when accessing a bank account, logging into a computer, or using a secure network. Cryptographic methods are employed by authentication protocols to confirm the user's identity and confirm that they have the required access rights to the resource.
6. **Cryptocurrencies:** Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum to safeguard transactions, thwart fraud, and maintain the network's integrity. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.
7. **End-to-End Encryption:** End-to-end encryption is used to protect two-way communications like video conversations, instant messages, and email. Even if the message is encrypted, it assures that only the intended receivers can read the message. End-to-end encryption is widely used in communication apps like WhatsApp and Signal, and it provides a high level of security and privacy for users.

Advantages

1. **Access Control:** Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource thanks to encryption.
2. **Secure Communication:** For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the internet.
3. **Protection against attacks:** Cryptography aids in the defence against various types of assaults, including replay and man-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
4. **Compliance with legal requirements:** Cryptography can assist firms in meeting a variety of legal requirements, including data protection and privacy legislation.
5. **Cryptography** is the study of conversion of plain text(readable format) to ciphertext(non-readable format) i.e. encryption. It is also called the **study of encryption**. **Cryptology**, on the other hand, is the study of the conversion of plain text to ciphertext and vice versa. It is also called the **study of encryption and decryption**.



One major difference is that Cryptology is the parent of Cryptography.



Let’s see the other differences.

Sl no.	Cryptography	Cryptology
1.	Cryptography is the process of conversion of plain text to cipher text.	Cryptology Is the process of conversion of plain text to cipher text and vice versa.
2.	It is also called the study of encryption	It is also called the study of encryption and decryption.
3.	It takes place on the sender side	It takes place on the sender and receiver side
4.	In Cryptography, sender sends the message to receiver.	In Cryptology, both sender and receiver send messages to each other.
5.	Cryptography can be seen as the child of Cryptology.	Cryptology can be seen as the parent of Cryptography
6.	Cryptography deals with the techniques of secure communication.	Cryptology deals with the study of secure communication.
7.	Cryptography focuses on the practice of hiding information	Cryptology focuses on the theoretical and mathematical aspects of information security

Sl no.	Cryptography	Cryptology
8.	Cryptography involves encryption, decryption, and authentication techniques	Cryptology involves the study of codes, ciphers, and cryptanalysis
9.	Cryptography is concerned with developing algorithms and protocols	Cryptology is concerned with analyzing and breaking existing encryption methods
10.	Cryptography utilized in various fields such as finance, e-commerce, and national security	Cryptology utilized in academia and research to understand and improve encryption
11.	Cryptography includes applications such as secure messaging, secure file transfer, and digital signatures.	Cryptology includes applications such as cryptanalysis, code breaking, and mathematical analysis of encryption methods.

Symmetric Key Encryption: Encryption is a process to change the form of any message in order to protect it from reading by anyone. 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.

Asymmetric Key Encryption: Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different key to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.

Symmetric Key Encryption	Asymmetric Key Encryption
The Mathematical Representation is as follows- P = D (K, E(K, P)) where K –> encryption and decryption key P –> plain text D –> Decryption E(K, P) –> Encryption of plain text using K Examples: 3DES, AES, DES and RC4	The Mathematical Representation is as follows- P = D(Kd, E (Ke,P)) where Ke –> encryption key Kd –> decryption key D –> Decryption E(Ke, P) –> Encryption of plain text using encryption key Ke. P –> plain text Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

Public Key Encryption

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as **ciphertext**.

Encryption:
The process of changing the plaintext into the ciphertext is referred to as **encryption.**
The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext.

The security of conventional encryption depends on the major two factors:

1. The Encryption algorithm
2. Secrecy of the key

Once the ciphertext is produced, it may be transmitted. The Encryption algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.
Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

Decryption:
The process of changing the ciphertext to the plaintext that process is known as **decryption**.

Public Key Encryption : Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as **Public Key Encryption.**

Difference between Encryption and Public-key Encryption:

basis	Encryption	Public-Key Encryption
Required for Work:	• Same algorithm with the same key is used for encryption and decryption. • The sender and receiver must share the algorithm and key.	• One algorithm is used for encryption and a related algorithm decryption with pair of keys, one for encryption and other for decryption. • Receiver and Sender must each have one of the matched pair of keys (not identical) .
Required for Security:	• Key must be kept secret. • If the key is secret, it is very impossible to decipher message. • Knowledge of the algorithm plus samples of ciphertext must be impractical to determine the key.	• One of the two keys must be kept secret. • If one of the key is kept secret, it is very impossible to decipher message. • Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be impractical to determine the other key.

Characteristics of Public Encryption key:

- Public key Encryption is important because it is infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and encryption key.
- Either of the two keys (Public and Private key) can be used for encryption with other key used for decryption.
- Due to Public key cryptosystem, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem is RSA (Rivest–Shamir–Adleman). The difficulty of finding the prime factors of a composite number is the backbone of RSA.

Example:
Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encrypt the message using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No other recipient other than C can decrypt the message because only C know C’s private key.

Domain Name System (DNS) in Application Layer

Domain Name System (DNS) is a hostname for **IP address** translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers. It is required for the functioning of the Internet.

What is the Need of DNS?

Every host is identified by the IP address but remembering numbers is very difficult for people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Types of Domain

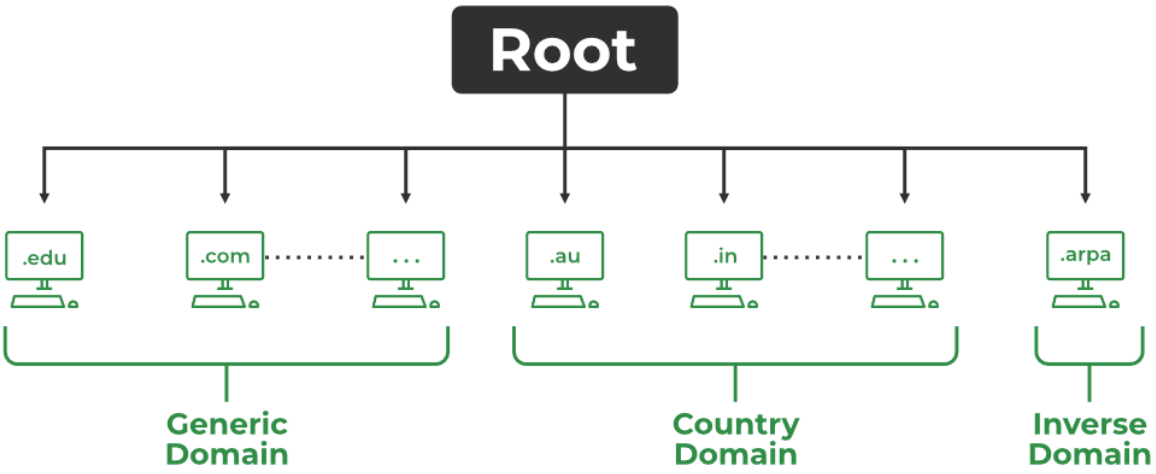
There are various kinds of domain:

1. **Generic domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.

2. **Country domain:** .in (India) .us .uk

3. **Inverse domain:** if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type

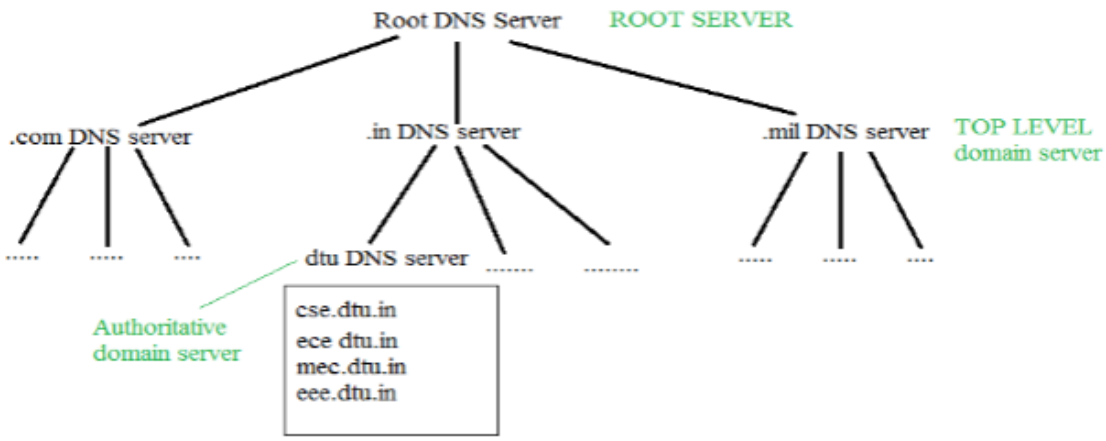
nslookup www.geeksforgeeks.org



Types of DNS

Organization of Domain

It is very difficult to find out the IP address associated with a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delays for that to happen organization of the database is very important.



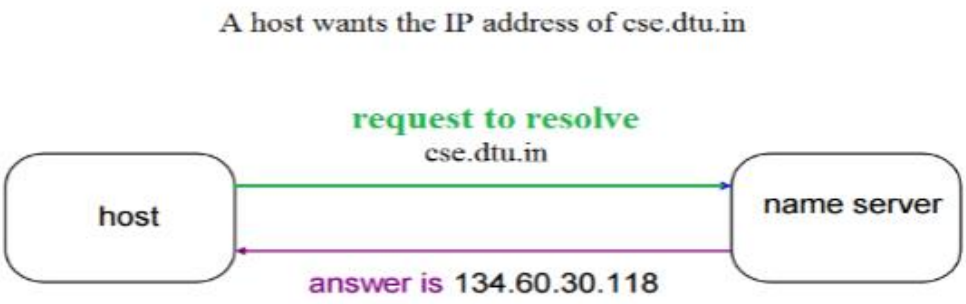
Root DNS Server

- **DNS record:** Domain name, IP address what is the validity? what is the time to live? and all the information related to that domain name. These records are stored in a tree-like structure.
- **Namespace:** Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.
- **Name server:** It is an implementation of the resolution mechanism.

```
DNS = Name service in Internet – A zone is an administrative unit, and a
domain is a subtree.
```

Name-to-Address Resolution

The host requests the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.



Name-to-Address Resolution

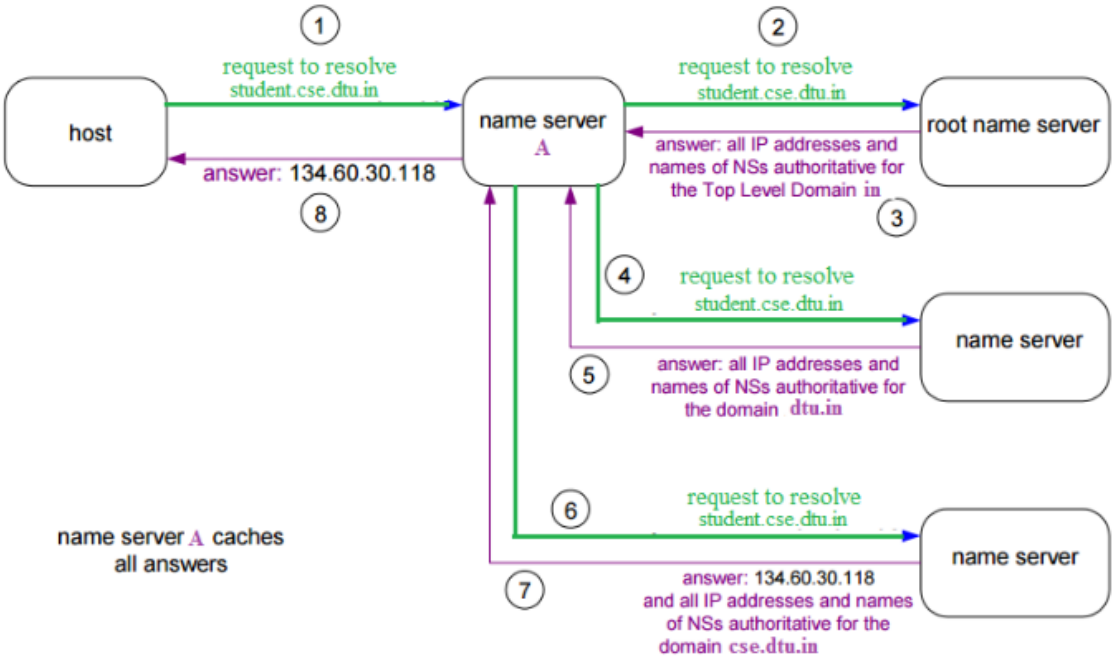
- **Hierarchy of Name Servers Root name servers:** It is contacted by name servers that can not resolve the name. It contacts the authoritative name server if name mapping is not known. It then gets the mapping and returns the IP address to the host.

- **Top-level domain (TLD) server:** It is responsible for com, org, edu, etc, and all top-level country domains like uk, fr, ca, in, etc. They have info about authoritative domain servers and know the names and IP addresses of each authoritative name server for the second-level domains.

- **Authoritative name servers** are the organization's DNS servers, providing authoritative hostnames to IP mapping for organization servers. It can be maintained by an organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top-level domain server and then to the authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative IP address.

Domain Name Server

The client machine sends a request to the local name server, which, if the root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to a top-level domain (TLD) or authoritative name server. The root name server can also contain some hostName to IP address mappings. The Top-level domain (TLD) server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

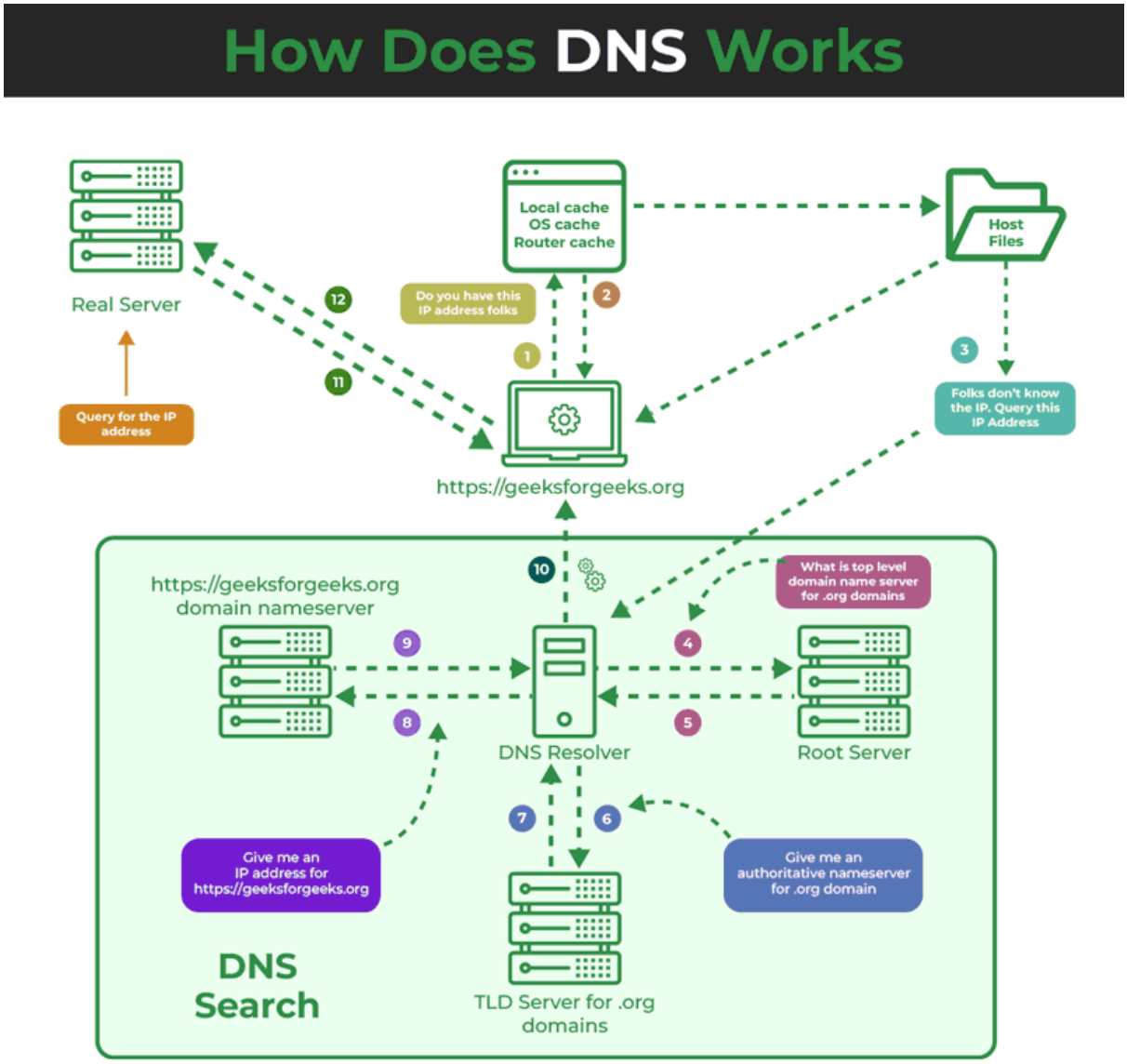


Domain Name Server

How Does DNS Work?

The working of DNS starts with converting a hostname into an IP Address. A domain name serves as a distinctive identification for a website. It is used in place of an IP address to make it simpler for consumers to visit websites. Domain Name System works by executing the database whose work is to store the name of hosts which are available on the Internet. The top-level domain server stores address information for top-level domains such as .com and .net, .org, and so on. If the Client sends the request, then the DNS resolver sends a request to DNS Server to fetch the IP Address. In case, when it does not contain that particular IP Address with a hostname, it forwards the request to another DNS Server. When IP Address has arrived at the resolver, it completes the request over Internet Protocol.

For more, you can refer to Working of DNS Server.



How Does DNS Work?

Authoritative DNS Server Vs Recursive DNS Resolver

Parameters	Authoritative DNS Server	Recursive DNS Resolver
Function	Holds the official DNS records for a domain	Resolves DNS queries on behalf of clients
Role	Provides answers to specific DNS queries	Actively looks up information for clients
Query Handling	Responds with authoritative DNS data	Queries other DNS servers for DNS data
Client Interaction	Doesn't directly interact with end-users	Serves end-users or client applications

Parameters	Authoritative DNS Server	Recursive DNS Resolver
Data Source	Stores the DNS records for specific domains	Looks up data from other DNS servers
Caching	Generally, doesn't perform caching	Caches DNS responses for faster lookups
Hierarchical Resolution	Does not participate in the recursive resolution	Actively performs recursive name resolution
IP Address	Has a fixed, known IP address	IP address may vary depending on ISP
Zone Authority	Manages a specific DNS zone (domain)	Does not manage any specific DNS zone

What is DNS Lookup?

DNS Lookup or DNS Resolution can be simply termed as the process that helps in allowing devices and applications that translate readable domain names to the corresponding IP Addresses used by the computers for communicating over the web.

DNS Servers Involved in Loading a Webpage

Upon loading the webpage, several DNS Servers are responsible for translating the domain name into the corresponding IP Address of the web server hosting the website. Here is the list of main DNS servers involved in loading a Webpage.

- Local DNS Resolver
- Root DNS Servers
- Top-Level Domain (TLD) DNS Servers
- Authoritative DNS Servers
- Web Server

This hierarchical system of DNS servers ensures that when you type a domain name into your web browser, it can be translated into the correct IP address, allowing you to access the desired webpage on the internet.

For more information you can refer DNS Look-Up article.

What is DNS Resolver?

DNS Resolver is simply called a DNS Client and has the functionality for initiating the process of DNS Lookup which is also called DNS Resolution. By using the DNS Resolver, applications can easily access different websites and services present on the Internet by using domain names

that are very much friendly to the user and that also resolves the problem of remembering IP Address.

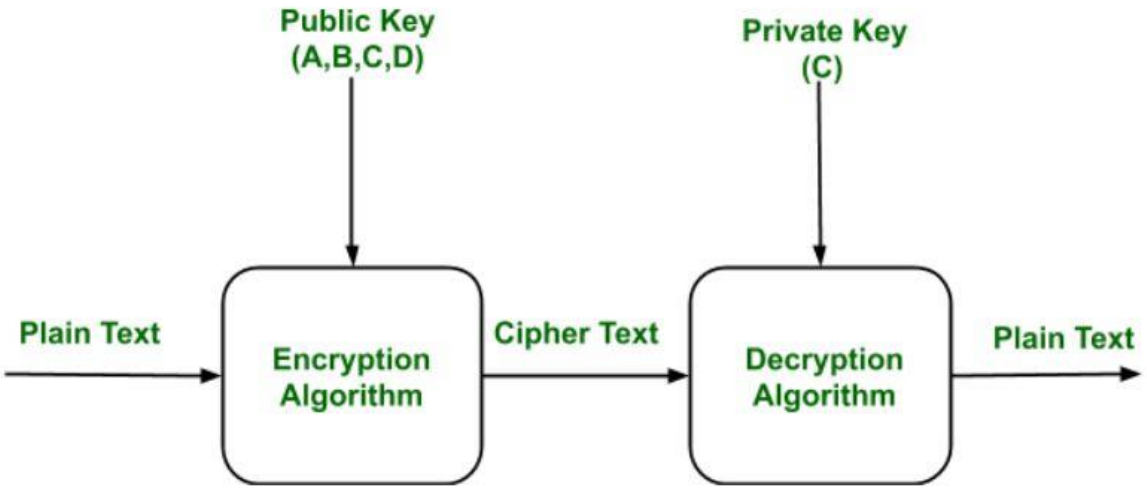
What Are the Types of DNS Queries?

There are basically three types of DNS Queries that occur in DNS Lookup. These are stated below.

- **Recursive Query:** In this query, if the resolver is unable to find the record, in that case, DNS client wants the DNS Server will respond to the client in any way like with the requested source record or an error message.

- **Iterative Query:** Iterative Query is the query in which DNS Client wants the best answer possible from the DNS Server.

- **Non-Recursive Query:** Non-Recursive Query is the query that occurs when a DNS Resolver queries a DNS Server for some record that has access to it because of the record that exists in its cache.



Components of Public Key Encryption:

- **Plain Text:**
  This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **Cipher Text:**
  The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **Encryption Algorithm:**
  The encryption algorithm is used to convert plain text into cipher text.
- **Decryption Algorithm:**
  It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text

- **Public and Private Key:**
  One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption

Weakness of the Public Key Encryption:

- Public key Encryption is vulnerable to Brute-force attack.
- This algorithm also fails when the user lost his private key, then the Public key Encryption becomes the most vulnerable algorithm.
- Public Key Encryption also is weak towards man in the middle attack. In this attack a third party can disrupt the public key communication and then modify the public keys.
- If user private key used for certificate creation higher in the PKI(Public Key Infrastructure) server hierarchy is compromised, or accidentally disclosed, then a "man-in-the-middle attack" is also possible, making any subordinate certificate wholly insecure. This is also the weakness of public key Encryption.

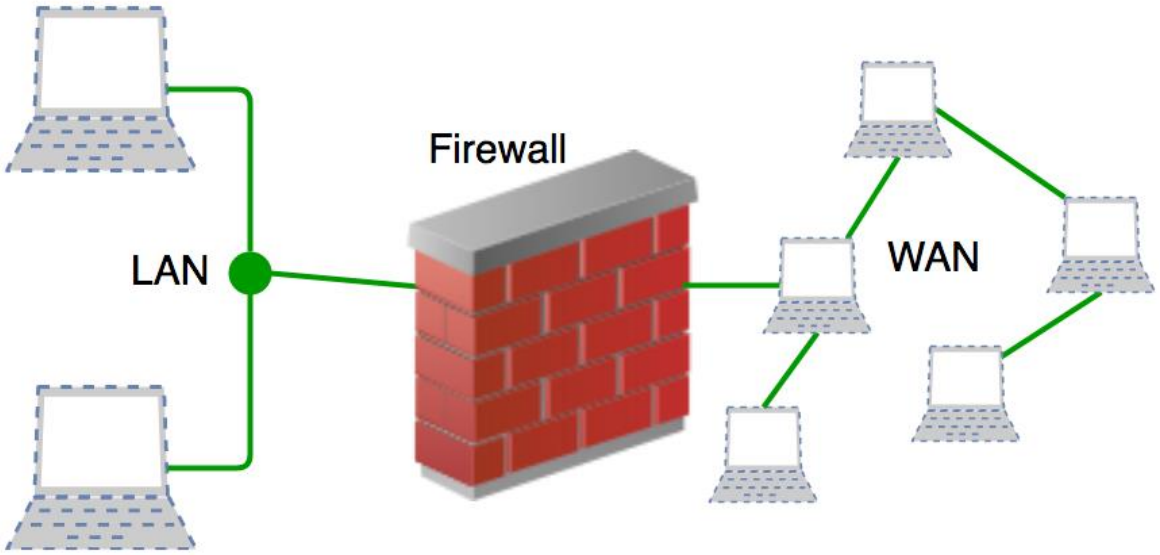
Applications of the Public Key Encryption:

- **Encryption/Decryption:**
  Confidentiality can be achieved using Public Key Encryption. In this the Plain text is encrypted using receiver public key. This will ensure that no one other than receiver private key can decrypt the cipher text.
- **Digital signature:**
  Digital signature is for senders authentication purpose. In this sender encrypt the plain text using his own private key. This step will make sure the authentication of the sender because receiver can decrypt the cipher text using senders public key only.
- **Key exchange:**
  This algorithm can use in both Key-management and securely transmission of data.

Introduction of Firewall in Computer Network

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

as the Internet.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced. Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How does Firewall work?

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet. **Default policy:** It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Generation of Firewall

Firewalls can be categorized based on their generation.

1. **First Generation- Packet Filtering Firewall:** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be filtered according to the following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for the internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

2. Second Generation- Stateful Inspection Firewall: Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

3. Third Generation- Application Layer Firewall : Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules. *Note: Application layer firewalls can also be used as Network Address Translator(NAT).*

4.Next Generation Firewalls (NGFW): Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

What is Magic Firewall?

"Magic Firewall" is a term used to describe a security feature provided by the web hosting and security company Cloudflare. It is a cloud-based firewall that provides protection against a wide range of security threats, including DDoS attacks, SQL injections, cross-site scripting (XSS), and other types of attacks that target web applications.

The Magic Firewall works by analyzing traffic to a website and using a set of predefined rules to identify and block malicious traffic. The rules are based on threat intelligence from a variety of sources, including the company's own threat intelligence network, and can be customized by website owners to meet their specific security needs.

The Magic Firewall is considered "magic" because it is designed to work seamlessly and invisibly to website visitors, without any noticeable impact on website performance. It is also easy to set up and manage, and can be accessed through Cloudflare's web-based control panel.

Overall, the Magic Firewall is a powerful security tool that provides website owners with an additional layer of protection against a variety of security threats.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Advantages of using Firewall

1. **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.

2. **Prevention of malware and other threats:** Malware and other threat prevention: Firewalls can be set up to block traffic linked to known malware or other security concerns, assisting in the defense against these kinds of attacks.

3. **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.

4. **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity. This information is essential for identifying and looking into security problems and other kinds of shady behavior.

5. **Regulation compliance:** Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.

6. **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Disadvantages of using Firewall

1. **Complexity:** Setting up and keeping up a firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of users and devices.

2. **Limited Visibility:** Firewalls may not be able to identify or stop security risks that operate at other levels, such as the application or endpoint level, because they can only observe and manage traffic at the network level.

3. **False sense of security:** Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.

4. **Limited adaptability:** Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.

5. **Performance impact:** Network performance can be significantly impacted by firewalls, particularly if they are set up to analyze or manage a lot of traffic.

6. **Limited scalability:** Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.

7. **Limited VPN support:** Some firewalls might not allow complex VPN features like split tunneling, which could restrict the experience of a remote worker.

8. **Cost:** Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

Real-Time Applications of Firewall

1. **Corporate networks:** Many businesses employ firewalls to guard against unwanted access and other security risks on their corporate networks. These firewalls can be set up to only permit authorized users to access particular resources or services and to prevent traffic from particular IP addresses or networks.

2. **Government organizations:** Government organizations frequently employ firewalls to safeguard sensitive data and to adhere to rules like HIPAA or PCI-DSS. They might make use of cutting-edge firewalls like Next-generation firewalls (NGFW), which can detect and stop intrusions as well as manage access to particular data and apps.

3. **Service providers:** Firewalls are used by service providers to safeguard their networks and the data of their clients, including ISPs, cloud service providers, and hosting firms. They might make use of firewalls that accommodate enormous volumes of traffic and support advanced features such as VPN and load balancing.

4. **Small enterprises:** Small firms may use firewalls to separate their internal networks, restrict access to specific resources or applications, and defend their networks from external threats.

5. **Networks at home:** To guard against unwanted access and other security risks, many home users employ firewalls. A firewall that many routers have built in can be set up to block incoming traffic and restrict access to the network.

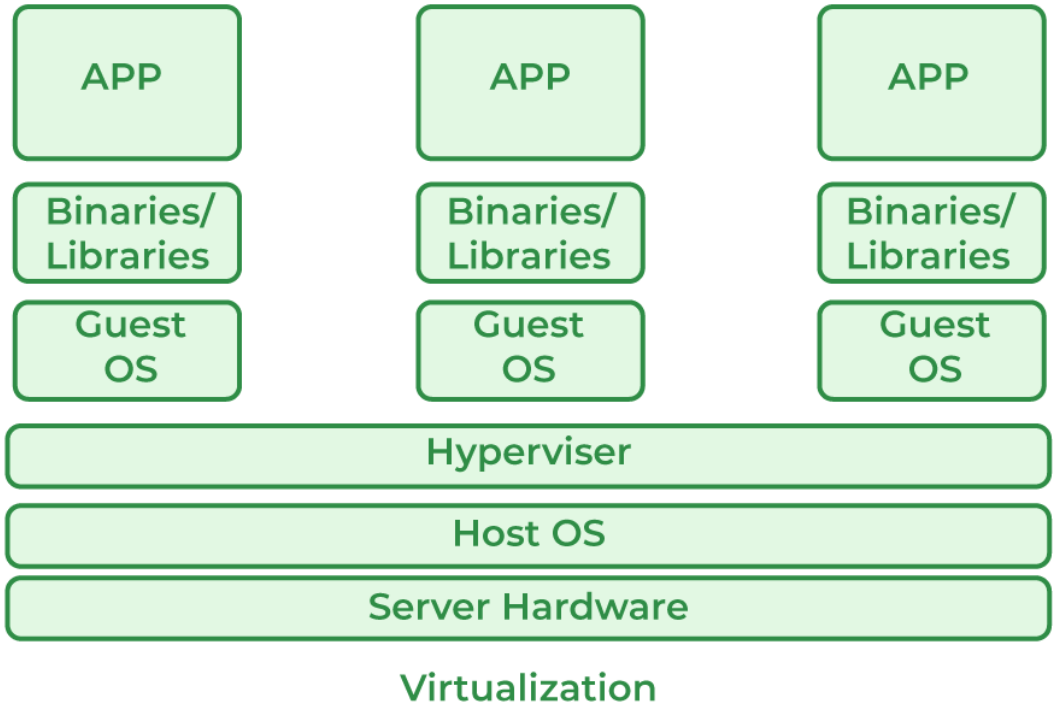
6. **Industrial Control Systems (ICS):** Firewalls are used to safeguard industrial control systems against illegal access and cyberattacks in many vital infrastructures, including power plants, water treatment facilities, and transportation systems.

Virtualization,

Virtualization in Cloud Computing and Types

Virtualization is a technique how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. With the help of Virtualization, multiple operating systems and applications can run on the same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.

In other words, one of the main cost-effective, hardware-reducing, and energy-saving techniques used by cloud providers is Virtualization. Virtualization allows sharing of a single physical instance of a resource or an application among multiple customers and organizations at one time. It does this by assigning a logical name to physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.



Virtualization

- Host Machine: The machine on which the virtual machine is going to be built is known as Host Machine.
- Guest Machine: The virtual machine is referred to as a Guest Machine.

Work of Virtualization in Cloud Computing

Virtualization has a prominent impact on Cloud Computing. In the case of cloud computing, users store data in the cloud, but with the help of Virtualization, users have the extra benefit of sharing the infrastructure. Cloud Vendors take care of the required physical resources, but these cloud providers charge a huge amount for these services which impacts every user or organization. Virtualization helps Users or Organisations in maintaining those services which are required by a company through external (third-party) people, which helps in reducing costs to the company. This is the way through which Virtualization works in Cloud Computing.

Benefits of Virtualization

- More flexible and efficient allocation of resources.
- Enhance development productivity.
- It lowers the cost of IT infrastructure.
- Remote access and rapid scalability.
- High availability and disaster recovery.
- Pay peruse of the IT infrastructure on demand.
- Enables running multiple operating systems.

Drawback of Virtualization

- **High Initial Investment:** Clouds have a very high initial investment, but it is also true that it will help in reducing the cost of companies.
- **Learning New Infrastructure:** As the companies shifted from Servers to Cloud, it requires highly skilled staff who have skills to work with the cloud easily, and for this, you have to hire new staff or provide training to current staff.
- **Risk of Data:** Hosting data on third-party resources can lead to putting the data at risk, it has the chance of getting attacked by any hacker or cracker very easily.

For more benefits and drawbacks, you can refer to the Pros and Cons of Virtualization.

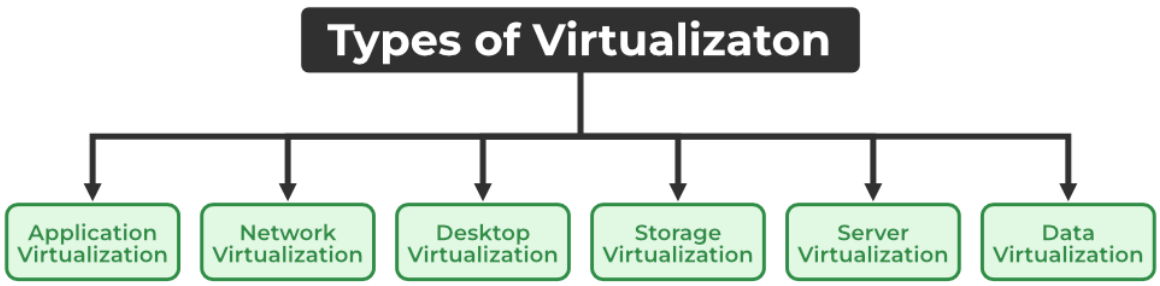
Characteristics of Virtualization

- **Increased Security:** The ability to control the execution of a guest program in a completely transparent manner opens new possibilities for delivering a secure, controlled execution environment. All the operations of the guest programs are generally performed against the virtual machine, which then translates and applies them to the host programs.
- **Managed Execution:** In particular, sharing, aggregation, emulation, and isolation are the most relevant features.
- **Sharing:** Virtualization allows the creation of a separate computing environment within the same host.
- **Aggregation:** It is possible to share physical resources among several guests, but virtualization also allows aggregation, which is the opposite process.

For more characteristics, you can refer to Characteristics of Virtualization.

Types of Virtualization

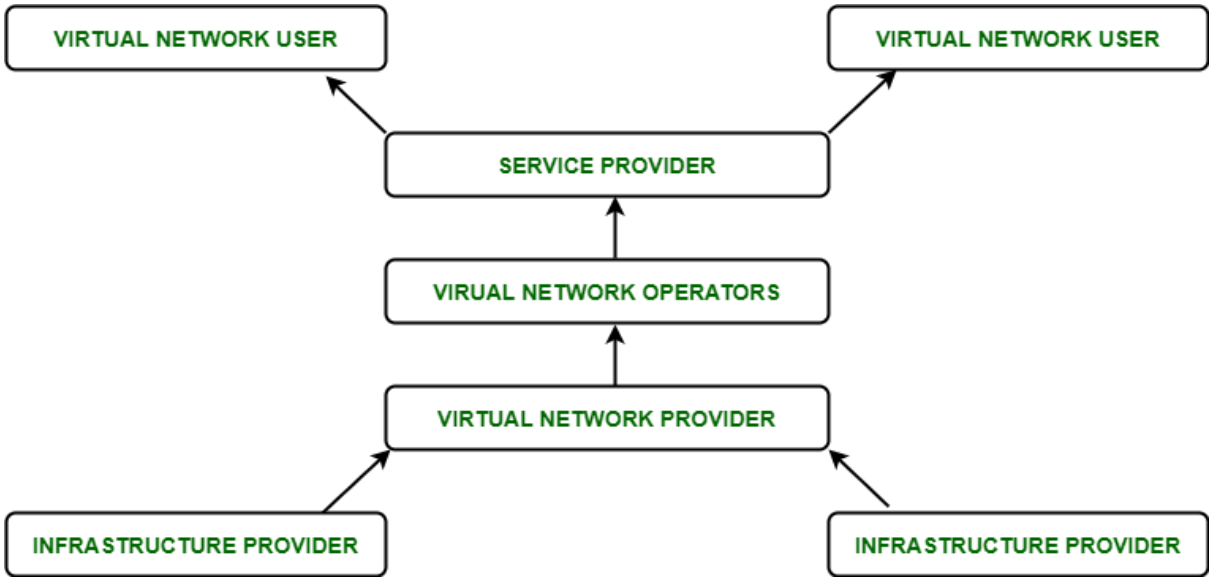
1. Application Virtualization
2. Network Virtualization
3. Desktop Virtualization
4. Storage Virtualization
5. Server Virtualization
6. Data virtualization



Types of Virtualization

1. Application Virtualization: Application virtualization helps a user to have remote access to an application from a server. The server stores all personal information and other characteristics of the application but can still run on a local workstation through the internet. An example of this would be a user who needs to run two different versions of the same software. Technologies that use application virtualization are hosted applications and packaged applications.

2. Network Virtualization: The ability to run multiple virtual networks with each having a separate control and data plan. It co-exists together on top of one physical network. It can be managed by individual parties that are potentially confidential to each other. Network virtualization provides a facility to create and provision virtual networks, logical switches, routers, firewalls, load balancers, Virtual Private Networks (VPN), and workload security within days or even weeks.



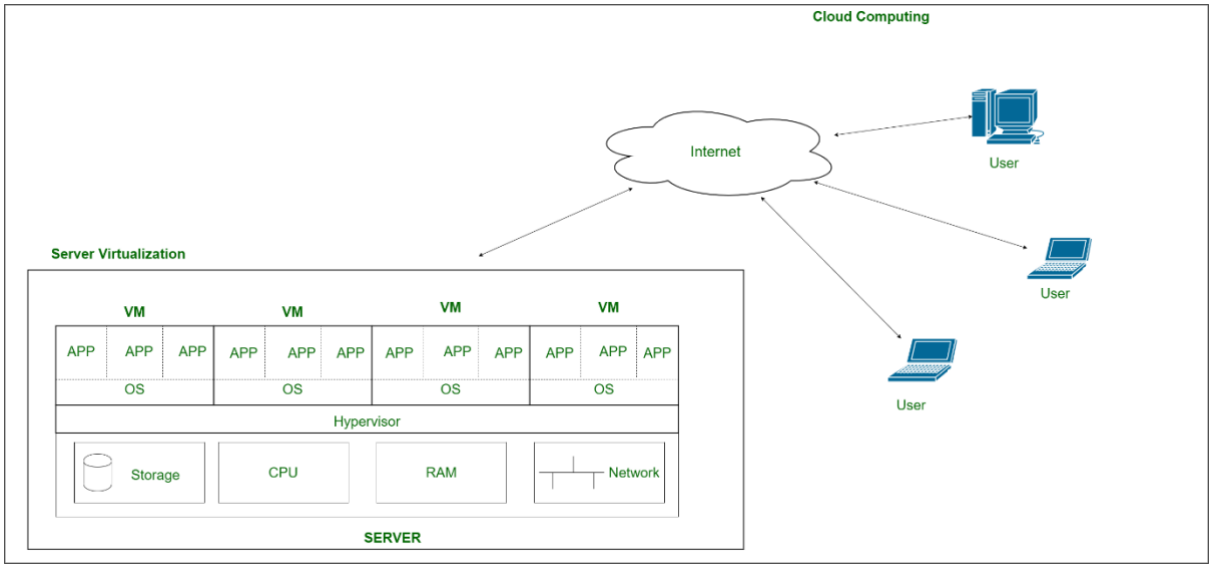
Network Virtualization

3. Desktop Virtualization: Desktop virtualization allows the users' OS to be remotely stored on a server in the data center. It allows the user to access their desktop virtually, from any location by a different machine. Users who want specific operating systems other than Windows Server will need to have a virtual desktop. The main benefits of desktop virtualization are user mobility, portability, and easy management of software installation, updates, and patches.

4. Storage Virtualization: Storage virtualization is an array of servers that are managed by a virtual storage system. The servers aren't aware of exactly where their data is stored and instead function more like worker bees in a hive. It makes managing storage from multiple sources be managed and utilized as a single repository. storage virtualization software maintains smooth operations, consistent performance, and a continuous suite of advanced functions despite changes, breaks down, and differences in the underlying equipment.

5. Server Virtualization: This is a kind of virtualization in which the masking of server resources takes place. Here, the central server (physical server) is divided into multiple different virtual servers by changing the identity number, and processors. So, each system can

operate its operating systems in an isolated manner. Where each sub-server knows the identity of the central server. It causes an increase in performance and reduces the operating cost by the deployment of main server resources into a sub-server resource. It's beneficial in virtual migration, reducing energy consumption, reducing infrastructural costs, etc.



Server Virtualization

6. Data Virtualization: This is the kind of virtualization in which the data is collected from various sources and managed at a single place without knowing more about the technical information like how data is collected, stored & formatted then arranged that data logically so that its virtual view can be accessed by its interested people and stakeholders, and users through the various cloud services remotely. Many big giant companies are providing their services like Oracle, IBM, At scale, Cdata, etc.

Uses of Virtualization

- Data-integration
- Business-integration
- Service-oriented architecture data-services
- Searching organizational data

Features	Cloud Computing	Virtualization
Basic	Pool and automate virtual resources for on demand use	Built multiple simulated environments from one physical hardware system
Scalability	High	Low
Set-up	Tedious	Simple
Cost	Private Cloud : HIGH CAPEX and low OPEX Public Cloud : Low CAPEX and high OPEX	High Capital expenditures (CAPEX) low Operating Expenses (OPEX)
Flexibility	Very flexible	Quite less
Type of service	laas	Saas

Features	Cloud Computing	Virtualization
Dedicated hardware	Multiple	Single can also work
Integration	Future expansion of users, application, etc	Expansion of new machines within the same infrastructure
Workload	stateless	Stateful
Disaster recovery	Depends on multiple machines	Depends upon the single machine
Form	Private and Public cloud	Hardware and application virtualization
Accessibility	Prevalently accessed	Not allowed to be accessed from outside the network
Configuration	In Cloud Computing , Configuration is image based.	In Virtualization, Configuration is template based.

Introduction of Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person. It uses radio frequency to search ,identify, track and communicate with items and people. it is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader. This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes. It is often read outside the road of sight either passive or active RFID.

Kinds of RFID :
There are many kinds of RFID, each with different properties, but perhaps the most fascinating aspect of RFID technology is that most RFID tags have neither an electric plug nor a battery. Instead, all of the energy needed to operate them is supplied in the form of radio waves by RFID readers. This technology is called passive RFID to distinguish it from the(less common) active RFID in which there is a power source on the tag.

UHF RHID (Ultra-High Frequency RFID). It is used on shipping pallets and some driver's licenses. Readers send signals in the 902-928 MHz band. Tags communicate at distances of several meters by changing the way they reflect the reader signals; the reader is able to pick up these reflections. This way of operating is called backscatter.

HF RFID (High-Frequency RFID). It operates at 13.56 MHz and is likely to be in your passport, credit cards, books, and noncontact payment systems. HF RFID has a short-range, typically a meter or less because the physical mechanism is based on induction rather than backscatter.

There are also other forms of RFID using other frequencies, such as LF RFID(Low-Frequency RFID), which was developed before HF RFID and used for animal tracking

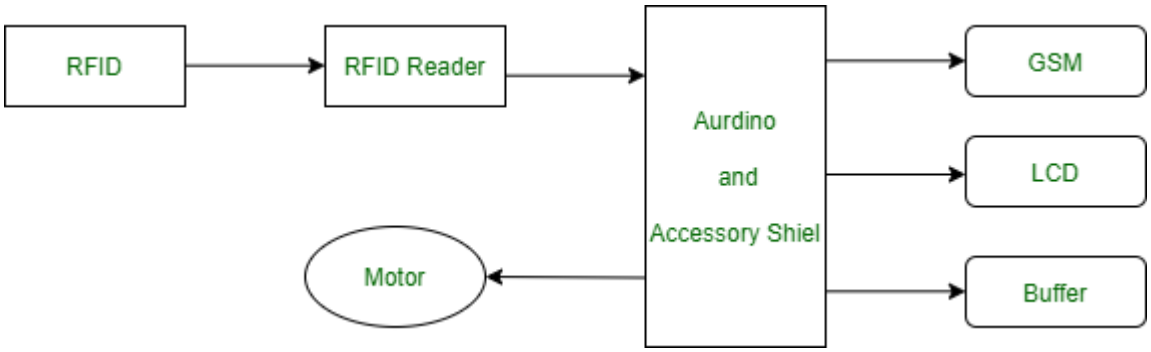
There are two types of RFID :

1. **Passive RFID –**
   Passive RFID tags does not have their own power source. It uses power from the reader. In this device, RF tags are not attached by a power supply and passive RF tag stored their power. When it is emitted from active antennas and the RF tag are used specific frequency like 125-134KHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.

2. **Active RFID –**
   In this device, RF tags are attached by a power supply that emits a signal and there is an antenna which receives the data. means, active tag uses a power source like battery. It has it's own power source, does not require power from source/reader.

Working Principle of RFID :
Generally, RFID uses radio waves to perform AIDC function. AIDC stands for Automatic Identification and Data Capture technology which performs object identification and collection and mapping of the data.

An antenna is an device which converts power into radio waves which are used for communication between reader and tag. RFID readers retrieve the information from RFID tag which detects the tag and reads or writes the data into the tag. It may include one processor, package, storage and transmitter and receiver unit.



Working of RFID System :

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers — fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

Features of RFID :

- An RFID tag consists of two-part which is an microcircuit and an antenna.
- This tag is covered by protective material which acts as a shield against the outer environment effect.
- This tag may active or passive in which we mainly and widely used passive RFID.

Application of RFID :

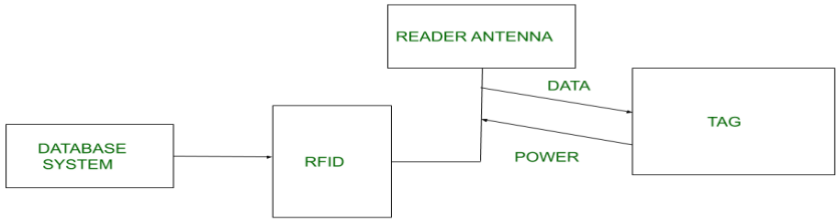
- It utilized in tracking shipping containers, trucks and railroad, cars.
- It uses in Asset tracking.
- It utilized in credit-card shaped for access application.
- It uses in Personnel tracking.
- Controlling access to restricted areas.
- It uses ID badging.
- Supply chain management.
- Counterfeit prevention (e.g., in the pharmaceutical industry).

Advantages of RFID :

- It provides data access and real-time information without taking to much time.
- RFID tags follow the instruction and store a large amount of information.
- The RFID system is non-line of sight nature of the technology.
- It improves the Efficiency, traceability of production.
- In RFID hundred of tags read in a short time.

Disadvantages of RFID :

- It takes longer to program RFID Devices.
- RFID intercepted easily even it is Encrypted.
- In an RFID system, there are two or three layers of ordinary household foil to dam the radio wave.
- There is privacy concern about RFID devices anybody can access information about anything.
- Active RFID can costlier due to battery.



What is Security Audit For Windows?

A security audit is a process where manual or automated techniques are used for vulnerability analysis of any system and a report is generated. Manual audit includes the process of interviewing staff, performing vulnerability scans without using any automated tools, reviewing all installed applications and OS access controls, and analyzing physical access to the systems. In a security audit of an operating system comes windows audit, Linux audit, etc. Windows auditing is one of the methods to make the system secure after knowing about the weakness of the system. Windows auditing system consists of tracking events and logs and what events were triggered in the system.

Two important areas where operating system audits can be performed are **all the directories** that are active or running in the background and **various policies of windows and privacy settings**. Active Directory provides information about specific applications, folders, and files, based on their identity. Because it is an extensively used method in the authentication and authorization of users, it is often prone to cyber-attacks. Therefore, monitoring and auditing of changes in Active Directory should be considered an essential part of security audits. Another vital area is Windows Policy changes.

Events that can be audited in the Windows operating system for vulnerability assessment of systems are listed below:

- **Audit Account Logon Events:** Audit of each login and logout instances with the exact date and time of users.
- **Audit Account Management:** Audit of every instance of account management operations on a machine such as altering passwords, usernames of accounts, number of users, etc.
- **Audit Objects Access:** Audit the event of a user accessing an object with its system access control list (SACL) specified. A few examples of objects are files, folders, registry keys, printers, etc.
- **Audit Policy Change:** Audit every incident where user rights were changed, or change in audit policies or modifying trust policies.
- **Audit Privilege and Use:** Audit each instance of a user.
- **Audit Process Tracking:** Audit and track detailed information of events such as program activation, process exit, handle duplication, and indirect object access.
- **Audit System Events:** Audit all the patch updates, unknown connections being established.

Audit Life Cycle: The audit framework consists of four major steps. The first step is *Planning* in which the auditors plan according to the requirements of the organization's needs. The second part consists of an *Assessment* in which the old audits are assessed and results are reviewed and then accordingly the new audit checklist is planned. The third step consists of *Follow-Up* which is performing the audit tasks. And the last part consists of the *Report Phase* in which a detailed report of the audit is created and the expected solutions are given.

Commands to Perform Audit: These are needed to be executed in the windows command prompt under administrator mode. To access the command prompt, click on the start button, search cmd, right-click on it and click on run as administrator option.

- **Systeminfo:** To get the full details of the system like installation date, users and accounts, last log activity, etc. command used is *systeminfo* that gives the complete details of a system.
- **ipconfig:** To get the IP address of a machine this command can be used.
- **Secpol.msc:** To retrieve the configuration of security policies of a system secpol.msc command is used that helps to know about account policies, Firewall policies, etc.
- **getmac:** To get the mac address of the machine.
- **netstat:** To check network statistics and analyze the foreign or unknown server that has successful connections established.
- **compmgmt.msc:** To check external devices that were used in the system and their logs etc.

How does the Token-Based Authentication work ?

Digital transformation brings security concerns for users to protect their identity from bogus eyes. According to US Norton, on average 8 lakh accounts are being hacked every year. There is a demand for high-security systems and cybersecurity regulations for authentication.

Traditional methods rely on single-level authentication with username and password to grant access to the web resources. Users tend to keep easy passwords or reuse the same password on multiple platforms for their convenience. The fact is, there is always a wrong eye on your web activities to take unfair advantage in the future.

Due to the rising security load, two-factor authentication (2FA) come into the picture and introduced Token-based authentication. This process reduces the reliance on password systems and added a second layer to security. Let's straight jump on to the mechanism.

But first of all, let's meet the main driver of the process: a T-O-K-E-N !!!

What is an Authentication 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 token is classified into two types: A Physical token and a Web token. Let's understand them and how they play an important role in security.

- **Physical token**: A Physical token use a tangible device to store the information of a user. Here, the secret key is a physical device that can be used to prove the user's identity. Two elements of physical tokens are hard tokens and soft tokens. Hard tokens use smart cards and USB to grant access to the restricted network like the one used in corporate offices to access the employees. Soft tokens use mobile or computer to send the encrypted code (like OTP) via authorized app or SMS.
- **Web token**: The authentication via web token is a fully digital process. Here, the server and the client interface interact upon the user's request. The client sends the user credentials to the server and the server verifies them, generates the digital signature, and sends it back to the client. Web tokens are popularly known as JSON Web Token (JWT), a standard for creating digitally signed tokens.

A token is a popular word used in today's digital climate. It is based on decentralized cryptography. Some other token-associated terms are Defi tokens, governance tokens, Non Fungible tokens, and security tokens. Tokens are purely based on encryption which is difficult to hack.

What is a Token-based Authentication?

Token-based authentication is a two-step authentication strategy to enhance the security mechanism for users to access a network. The users once register their credentials, receive a unique encrypted token that is valid for a specified session time. During this session, users can directly access the website or application without login requirements. It enhances the user experience by saving time and security by adding a layer to the password system.

A token is stateless as it does not save information about the user in the database. This system is based on cryptography where once the session is complete the token gets destroyed. So, it gets the advantage against hackers to access resources using passwords.

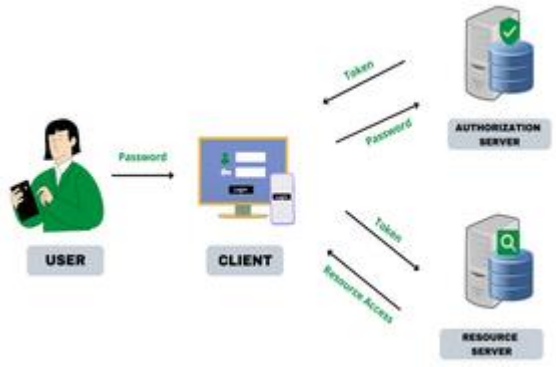
The most friendly example of the token is OTP (One Time password) which is used to verify the identity of the right user to get network entry and is valid for 30-60 seconds. During the session time, the token gets stored in the organization's database and vanishes when the session expired.

Let's understand some important drivers of token-based authentication-

- **User**: A person who intends to access the network carrying his/her username & password.
- **Client-server**: A client is a front-end login interface where the user first interacts to enroll for the restricted resource.
- **Authorization server**: A backend unit handling the task of verifying the credentials, generating tokens, and send to the user.
- **Resource server**: It is the entry point where the user enters the access token. If verified, the network greets users with a welcome note.

How does Token-based Authentication work?

Token-based authentication has become a widely used security mechanism used by internet service providers to offer a quick experience to users while not compromising the security of their data. Let's understand how this mechanism works with 4 steps that are easy to grasp.



How Token-based Authentication works?

1. Request: The user intends to enter the service with login credentials on the application or the website interface. The credentials involve a username, password, smartcard, or biometrics

2. Verification: The login information from the client-server is sent to the authentication server for verification of valid users trying to enter the restricted resource. If the credentials pass the verification the server generates a secret digital key to the user via HTTP in the form of a code. The token is sent in a JWT open standard format which includes-

- **Header**: It specifies the type of token and the signing algorithm.
- **Payload**: It contains information about the user and other data
- **Signature**: It verifies the authenticity of the user and the messages transmitted.

3. Token validation: The user receives the token code and enters it into the resource server to grant access to the network. The access token has a validity of 30-60 seconds and if the user fails to apply it can request the Refresh token from the authentication server. There's a limit on the number of attempts a user can make to get access. This prevents brute force attacks that are based on trial and error methods.

4. Storage: Once the resource server validated the token and grants access to the user, it stores the token in a database for the session time you define. The session time is different for every website or app. For example, Bank applications have the shortest session time of about a few minutes only.

So, here are the steps that clearly explain how token-based authentication works and what are the main drivers driving the whole security process.

Note: Today, with growing innovations the security regulations are going to be strict to ensure that only the right people have access to their resources. So, tokens are occupying more space in the security process due to their ability to tackle the store information in the encrypted form and work on both website and application to maintain and scale the user experience. Hope the article gave you all the know-how of token-based authentication and how it helps in ensuring the crucial data is being misused.

What is a Message Queues?

A Message Queue is a form of communication and data transfer mechanism used in computer science and system design. It functions as a temporary storage and routing system for messages exchanged between different components, applications, or systems within a larger software architecture.

Example:

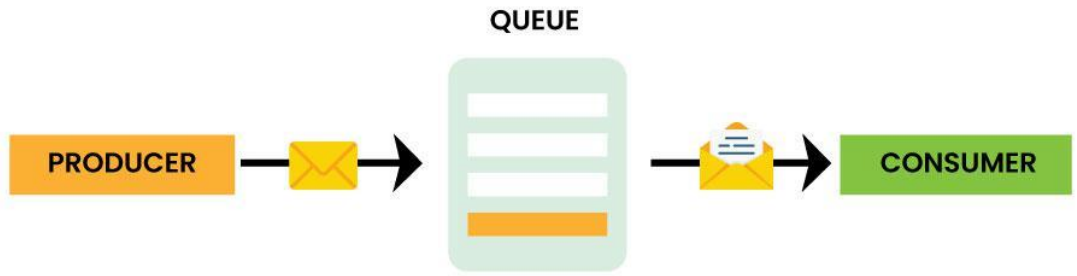
Think about your favorite pizza place, where they make and deliver pizzas. Behind the scenes, there's a magical system that ensures everything runs smoothly. This magic is called a **Message Queue.** It's like a special to-do list that helps the chefs and delivery drivers know exactly what pizzas to make and where to deliver them, especially when things get super busy.

Primary Purpose of Message Queues

The primary purpose of a Message Queue are:

- It enable loosely coupled communication, ensuring that different parts of a system can exchange data without being directly connected or dependent on one another.
- It provides a reliable, scalable, and resilient method for inter-process communication, allowing systems to handle varied workloads, manage system components independently, and maintain a buffer for messages in case the sender and receiver are not synchronized in real-time.

Key Components of a Message Queues System



Message Queue

- **Message Producer:** The message producer is responsible for creating and sending messages to the message queue. This can be any application or component withing a system that generates data to be shared.
- **Message Queue:** The message queue is a data structure or service that stores and manages the messages until they are consumed by the message consumers. It acts as a buffer or intermediary between producers and consumers.
- **Message Consumer:** The message consumer is responsible for retrieving and processing messages from the message queue. Multiple consumers can read messages concurrently from the queue.
- **Message Broker (Optional):** In some message queue systems, a message broker acts as an intermediary between producers and consumers, providing additional functionality like message routing, filtering, and message transformation.

How Message Queues Work

- **Sending Messages:** The message producer creates a message and sends it to the message queue. The message typically contains data or instructions that need to be processed or communicated.

- **Queuing Messages:** The message queue stores the message temporarily, making available for one or more consumers. Messages are typically stored in a first-in, first out (FIFO) order.

- **Consuming Messages:** Message consumers retrieve messages from the queue when they are ready to process them. They can do this at their own pace, which enables asynchronous communication.

- **Acknowledgment (Optional):** In some message queue systems, consumers can send acknowledgments back to the queue, indicating that they have successfully processed a message. This is essential for ensuring message delivery and preventing message loss.

Need of Message Queues

Message Queue are needed to address a number of challenges in distributed systems, including:

- **Asynchronous Communication:** Message queue allow applications to send and receive messages without having to wait for a response. This is essential for building scalable and reliable systems.

- **Decoupling:** Message queues decouple applications from each other, allowing them to be developed independently. This makes systems more flexible and easier to maintain.

- **Scalability:** Message queues can be scaled to handle large volumes of messages by adding more servers. This makes them ideal for high-traffic applications.

- **Reliability:** Message queues can be designed to be highly reliable, with features such as message persistence, retries, and dead letter queues. This ensures that messages are not lost even in the event of failures.

- **Workflow Management:** Message queues can be used to implement complex workflows, such as order processing and payment processing. This can help improve the efficiency and accuracy of these processes.

Use Cases of Message Queues

Message Queues are used in a wide variety of applications, including:

- **Ecommerce:** Message Queues are used to process orders, payments, and shipping notifications.

- **Financial Services:** Message Queues are used to process transactions, fraud detection, and risk management systems.

- **Gaming:** Message queues are used to synchronize game servers and clients.
- **Social Media:** Message queues are used to distribute messages and notifications to users.
- **Internet of Things (IoT):** Message Queues are used to collect and process data from IoT devices.

Example for Message Queues

Problem Statement:

A simple example of a message queue is an email inbox. When you send an email, it is placed in the recipient's inbox. The recipient can then read the email at their convenience. This email inbox acts as a buffer between the sender and the recipient, decoupling them from each other.

Implementation of Message Queues

Message Queues can be implemented in a variety of ways, but they typically follow a simple pattern:

1. **Producer:** An application that sends messages to a queue.
2. **Message Broker:** A server that stores and forwards messages between producers and consumers.
3. **Consumer:** An application that receives messages from a queue.

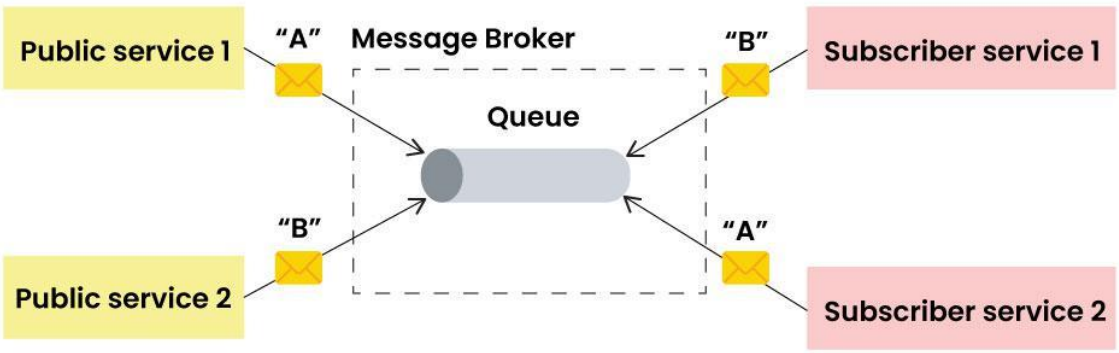
The message broker is responsible for routing messages to consumers and ensuring that they are delivered in the correct order. It also provides features such as message persistence, retries, and dead letter queues.

Types of Message Queues

There are two main types of message queues in system design:

1. **Point-to-point Message Queue**
2. **Publish-Subscribe Message Queue**

Point-to-Point Message Queues



Message Queue Point to Point

Point-to-point message queues are the simplest type of message queue. When a producer sends a message to a point-to-point queue, the message is stored in the queue until a consumer retrieves it. Once the message is retrieved by a consumer, it is removed from the queue and cannot be processed by any other consumer.

Point-to-point message queues can be used to implement a variety of patterns such as:

- **Request-Response:** A producer sends a request message to a queue, and a consumer retrieves the message and sends back a response messages.
- **Work Queue:** Producers send work items to a queue, and consumers retrieve the work items and process them.
- **Guaranteed Delivery:** Producers send messages to a queue, and consumers can be configured retry retrieving messages until they are successfully processed.

Publish-Subscribe Message Queues

Publish-Subscribe Message Queues are more complex than point-to-point message queues. When a producer publishes a message to publish/subscribe queue, the message is routed to all consumers that are subscribed to the queue. Consumers can subscribe to multiple queues, and they can also unsubscribe from queues at any time.

Publish-Subscribe Message Queues are often used to implement real-time streaming applications, such as social media and stock market tickers. They can also be used to implement event-driven architecture, where components of a system communicate with each other by publishing and subscribing to events.

Message Serialization

Message Serialization is the process of converting complex data structures or objects into a format that can be easily transmitted, stored, or reconstructed. Message Serialization formats include:

- **JSON (JavaScript Object Notation):** A lightweight data interchange format used for structured data, commonly supported by many programming languages.
- **XML (eXtensible Markup Language):** A format that uses tags to define data structure, often used in web services and configuration files.
- **Protocol Buffers (protobuf):** A binary serialization format developed by Google that is highly efficient and language-agnostic.
- **Binary Serialization:** Custom binary formats are used for performance-critical applications due to their compactness and speed.

Message Structure

A typical message structure consists of two main parts:

- **Headers:** These contain metadata about the message, such as unique identifier, timestamp, message type, and routing information.
- **Body:** The body contains the actual message payload or content. It can be in any format, including text, binary data, or structured data like JSON.

Message Routing

Message Routing involves determining how messages are directed to their intended recipients. The following methods can be employed:

- **Topic-Based Routing:** Messages are sent to topics or channels, and subscribers express interest in specific topics. Messages are delivered to all subscribers of a particular topic.
- **Direct Routing:** Messages are sent directly to specific queues or consumers based on their addresses or routing keys.
- **Content-Based Routing:** The routing decision is based on the content of the message. Filters or rules are defined to route messages that meet specific criteria.

Scalability of Message Queues

Scalability is essential to ensure that a message queue system can handle increased loads efficiently. To achieve scalability:

- **Distributed Queues:** Implement the message queue as a distributed system with multiple nodes, enabling horizontal scaling.

- **Partitioning:** Split queues into partitions to distribute message processing across different nodes or clusters.

- **Load Balancing:** Use load balancers to evenly distribute incoming messages to queue consumers.

Dead Letter Queues

Dead Letter Queues (DLQs) are a mechanism for handling messages that cannot be processed successfully. This includes:

- Messages with errors in their content or format.

- Messages that exceed their time-to-live (TTL) or delivery attempts.

- Messages that cannot be delivered to any consumer.

DLQs provide way to investigate and potentially reprocess failed messages while preventing them from blocking the system.

Securing Message Queues

Securing Message Queues is crucial to protect sensitive data and ensure the integrity of the messaging system:

- **Access Control:** Enforce access controls to restrict who can send, receive, or administer the message queue.

- **Encryption:** Implement data encryption in transit and at rest to protect messages from eavesdropping.

- **Authentication:** Ensure that only authorized users or systems can connect to the message queue.

- **Authorization:** Definer granular permissions to control what actions users or systems can perform withing the messaging system.

Message Prioritization

Message Prioritization is the process of assigning priority levels to messages to control their processing order. Prioritization criteria can include:

- **Urgency:** Messages with higher priority may need to processed before lower-priority messages.

- **Message Content:** Messages containing critical information or commands may receive higher priority.

- **Business Rules:** Custom business rules or algorithms may be used to determine message priority.

Load Balancing of Messages

Load Balancing ensures even distribution of message processing workloads across consumers. Strategies for load balancing include:

- **Round-Robin:** Messages are distributed to consumers in a cyclic manner.
- **Weighted Load Balancing:** Assign different weights to consumers to control the distribution of messages.
- **Dynamic Load Balancing:** Analyze the load on consumers in real-time and direct messages to less loaded consumers.

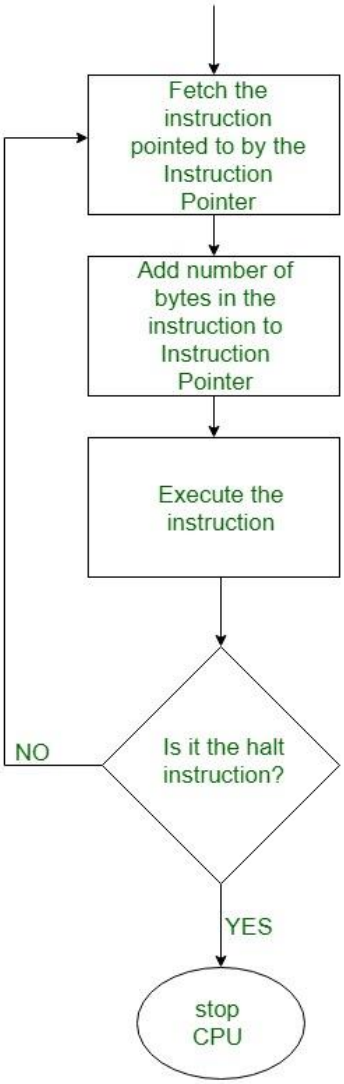
These aspects are essential for designing, implementing, and managing message queues, which are fundamental in building scalable, reliable, and efficient distributed systems and microservice architectures. The specific approach may vary based on the message system or technology used and the requirements of the application.

Program Execution in the CPU

You may be speculative however the central processor is programmed. It contains a special register — the instruction register — whose bit pattern determines what the central processor unit can do. Once that action has been completed, the bit pattern within the instruction register may be modified, and also the central processor unit can perform the operation nominative by this next bit pattern.

Since directions are simply bit patterns, they will be kept in memory. The instruction pointer register continuously has the memory address of (points to) the next instruction to be executed. so as for the management unit to execute this instruction, it's derived into the instruction register. the case is as follows:

1. A sequence of instructions is stored in memory.
2. The memory address wherever the first instruction is found is copied to the instruction pointer.
3. The CPU sends the address within the instruction pointer to memory on the address bus.
4. The CPU sends a "read" signal to the control bus.
5. Memory responds by sending a copy of the state of the bits at that memory location on the
   data bus, that the CPU then copies into its instruction register.
6. The instruction pointer is automatically incremented to contain the address of the next instruction in memory.
7. The CPU executes the instruction within the instruction register.
8. Go to step 3



The instruction execution cycle