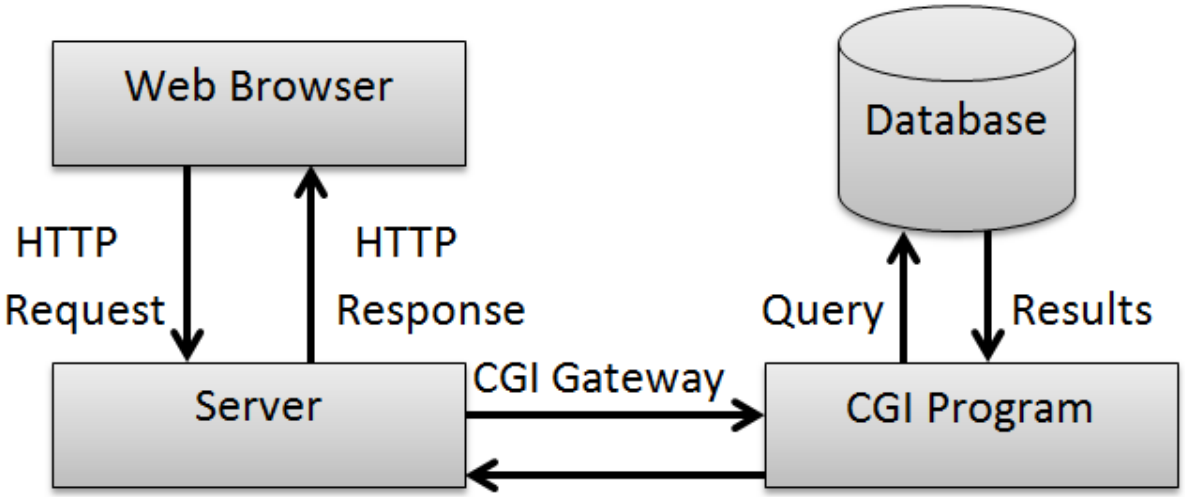
Common Gateway Interface (CGI)

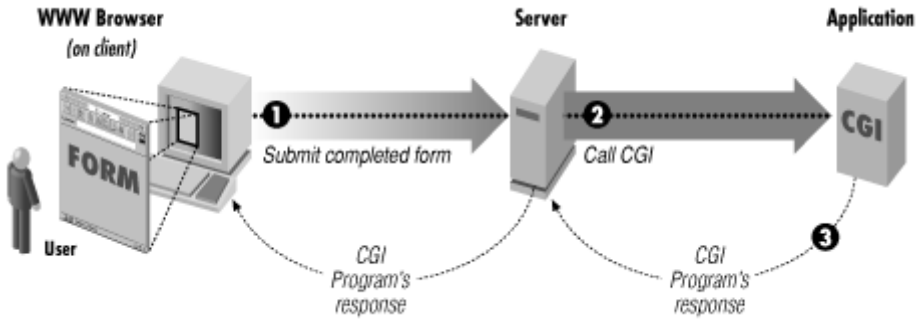
The Common Gateway Interface (CGI) provides the middleware between WWW servers and external databases and information sources. The World Wide Web Consortium (W3C) defined the Common Gateway Interface (CGI) and also defined how a program interacts with a Hyper Text Transfer Protocol (HTTP) server. The Web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This process or convention for passing data back and forth between the server and the application is called the common gateway interface (CGI).

Features of CGI:

It is a very well defined and supported standard.

- CGI scripts are generally written in either Perl, C, or maybe just a simple shell script.
- CGI is a technology that interfaces with HTML.
- CGI is the best method to create a counter because it is currently the quickest
- CGI standard is generally the most compatible with today's browsers





Advantages of CGI:

- The advanced tasks are currently a lot easier to perform in CGI than in Java.
- It is always easier to use the code already written than to write your own.
- CGI specifies that the programs can be written in any language, and on any platform, as long as they conform to the specification.
- CGI-based counters and CGI code to perform simple tasks are available in plenty.

Disadvantages of CGI:

There are some disadvantages of CGI which are given below:

- In Common Gateway Interface each page load incurs overhead by having to load the programs into memory.
- Generally, data cannot be easily cached in memory between page loads.
- There is a huge existing code base, much of it in Perl.
- CGI uses up a lot of processing time.

How CGI Scripting Works

Simple CGI Scripts

Assuming that you have access to a cgi-bin directory (see the previous section), and assuming that you know either the C programming language or PERL, you can do a whole bunch of interesting experiments with CGI to get your feet wet. Let's start by creating the simplest possible CGI script.

It looked something like this:

```
<html>
  <body>
    <h1>Hello there!</h1>
  </body>
</html>
```

The simplest possible CGI script would, upon execution, create this simple, static page as its output. Here is how this CGI program would look if you wrote it in C:

```
#include <stdio.h>

int main()
{
  printf("Content-type: text/html\n\n");
  printf("<html>\n");
  printf("<body>\n");
  printf("<h1>Hello there!</h1>\n");
  printf("</body>\n");
  printf("</html>\n");
  return 0;
}
```

On my Web server, I entered this program into the file simplest.c and then compiled it by saying:

gcc simplest.c -o simplest.cgi

By placing simplest.cgi in the cgi-bin directory, it can be executed. As you can see, all that the script does is generate a page that says, "Hello there!" The only part that is unexpected is the line that says:

```
printf("Content-type: text/html\n\n");
```

The line "Content-type: text/html\n\n" is special piece of text that must be the first thing sent to the browser by any CGI script. As long as you remember to do that, everything will be fine. If you forget, the browser will reject the output of the script.

Active Server Pages (ASP)

Active Server Pages (also known as ASP or classic ASP) is Microsoft’s first server-side script engine that enabled dynamically-generated web pages. While the initial release was an add-on to the Internet Information Services (IIS) component of Windows NT 4.0, it was later incorporated into the Windows Server operating system.

ASP employs server-side scripting to dynamically produce web pages based on a specific request from the client. The result is a HTML webpage sent back to the client for display. VBScript is the default scripting language used for writing ASP, although other scripting languages can be used.

ASP was Microsoft' alternative to Common Gateway Interface (CGI) scripts and Java Server Pages (JSPs), both intended to allow clients to interact with server-side databases and enterprise services. ASP has gone through three major releases: ASP 1.0 in 1996 (included with IIS 3.0), ASP 2.0 in 1997 (IIS 4.0) and ASP 3.0 in 2000 (IIS 5.0). ASP 3.0 becomes part of IIS 6.0 on Windows Server 2003 and part of IIS 7.0 on Windows Server 2008.

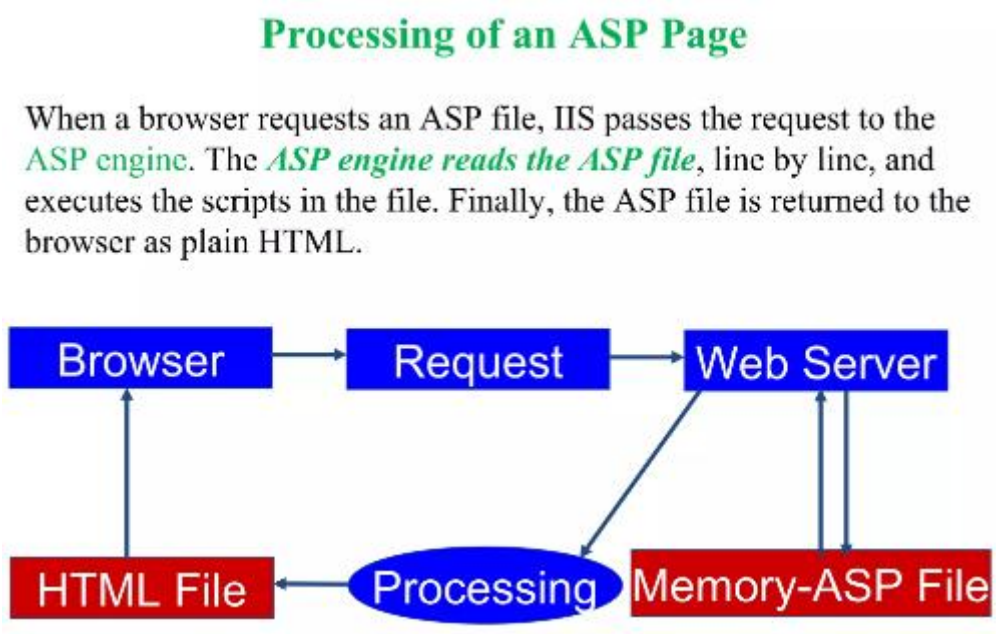
ASP is now obsolete and replaced with ASP.NET. Though, ASP.NET is not strictly an enhanced version of ASP; the two technologies have completely different underlying implementations. ASP.NET is a compiled language and relies on the .NET Framework, while ASP is strictly an interpreted language. As with any older technology, you can certainly find ASP in production, but you'd be hard-pressed to make the case to use it for a new project.

Ex

```
<!DOCTYPE html>
<html>
<body>
<p>ASP can output plain text:</p>
<%response.write("Hello World!")%>
</body>
</html>
```

O/P

ASP can output plain text:
Hello World!



FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

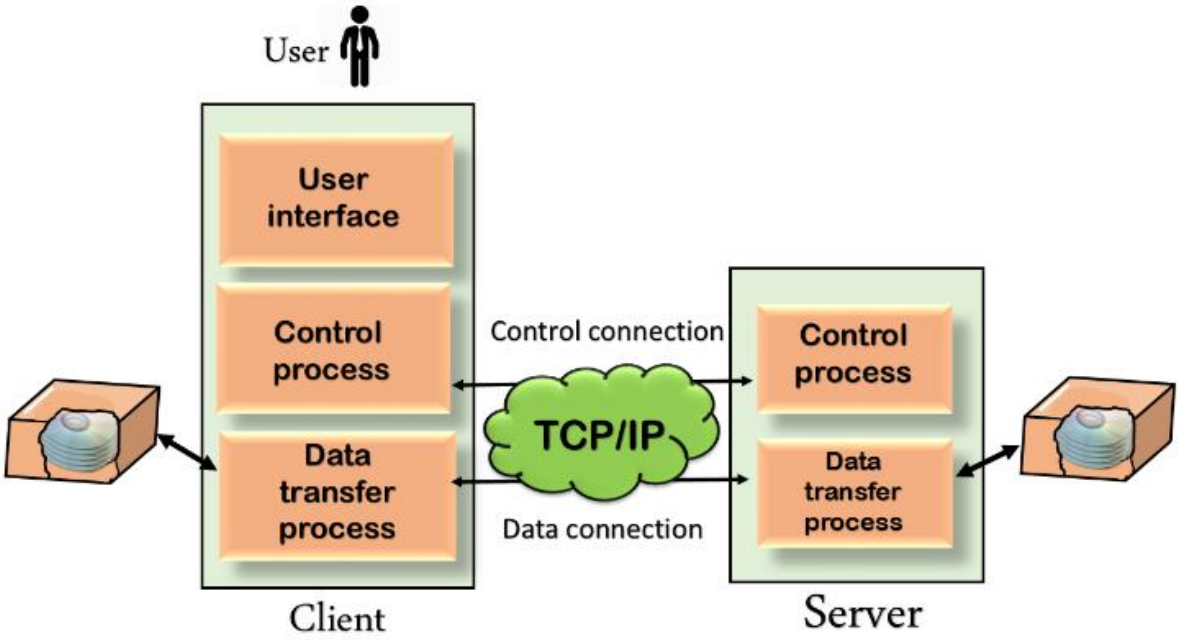
Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Why FTP?

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

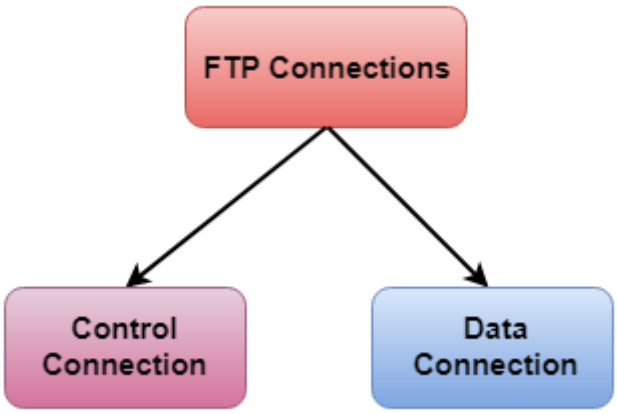
Mechanism of FTP



Computer Network FTP

The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



Computer Network FTP

Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.

It allows a user to connect to a remote host and upload or download the files.

It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.

The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed**: One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient**: It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security**: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement**: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

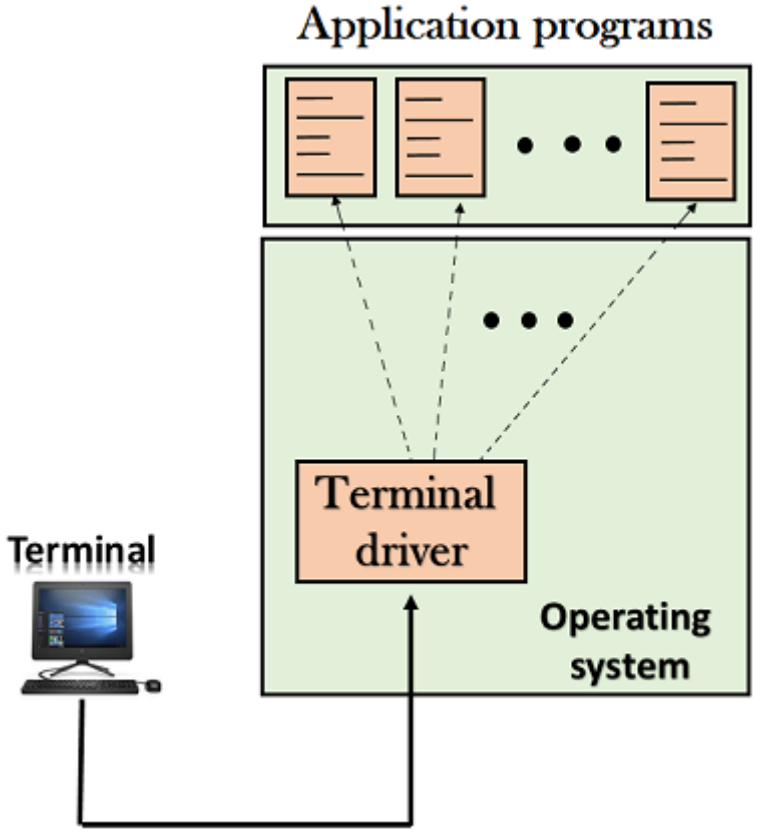
Telnet

The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.

The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for Terminal Network.

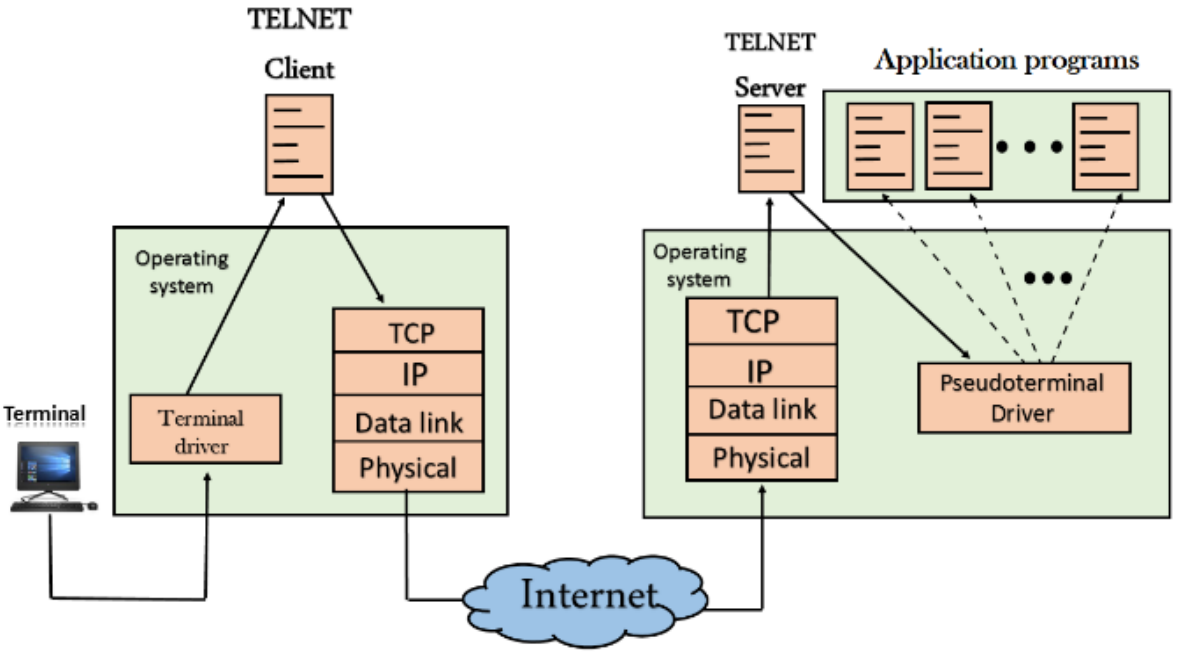
Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

There are two types of login:
Local Login



- When a user logs into a local computer, then it is known as local login.
- When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.
- However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters have special meanings such as control character with "z" means suspend. Such situations do not create any problem as the terminal driver knows the meaning of such characters. But, it can cause the problems in remote login.

Remote login



When the user wants to access an application program on a remote computer, then the user must perform remote login.

How remote login occurs

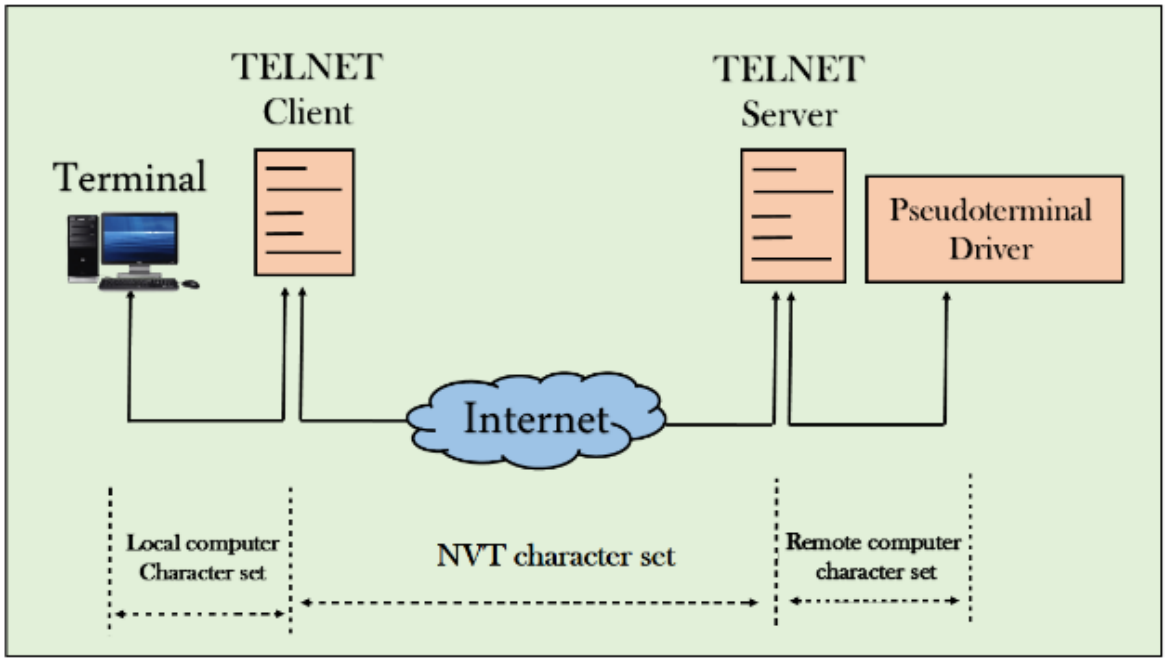
At the local site

The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack

At the remote site

The commands in NVT forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

Network Virtual Terminal (NVT)



The network virtual terminal is an interface that defines how data and commands are sent across the network.

In today's world, systems are heterogeneous. For example, the operating system accepts a special combination of characters such as end-of-file token running a DOS operating system ctrl+z while the token running a UNIX operating system is ctrl+d.

TELNET solves this issue by defining a universal interface known as network virtual interface.

The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then translates the data from NVT form into a form which can be understandable by a remote computer.

E-mail

E-mail is defined as the transmission of messages on the Internet. It is one of the most commonly used features over communications networks that may contain text, files, images, or other attachments. Generally, it is information that is stored on a computer sent through a network to a specified individual or group of individuals.

Email messages are conveyed through email servers; it uses multiple protocols within the TCP/IP suite. For example, SMTP is a protocol, stands for simple mail transfer protocol and used to send messages whereas other protocols IMAP or POP are used to retrieve messages from a mail server. If you want to login to your mail account, you just need to enter a valid email address, password, and the mail servers used to send and receive messages.

Email messages include three components, which are as follows:

- ✓ Message envelope: It depicts the email's electronic format.
- ✓ Message header: It contains email subject line and sender/recipient information.
- ✓ Message body: It comprises images, text, and other file attachments.

Uses of email

- Email can be used to communicate either within an organization or personally, including between two people or a large group of people.
- Users can also use the email to quickly remind all upcoming events or inform the group of a time change.
- Email can also be used to move a latent sale into a completed purchase or turn leads into paying customers.

Advantages of Email

There are many advantages of email, which are as follows:

- Cost-effective
- Speed and simplicity

Disadvantages of Email

- Impersonal
- Misunderstandings
- Malicious Use
- Accidents Will Happen
- Spam
- Information Overload
- Viruses
- Pressure to Respond
- Time Consuming
- Overlong Messages
- Insecure
- Newsletters
- Lead Nurturing: Lead-nurturing emails are a series of related emails that marketers use to take users on a journey that may impact their buying behavior.
- Promotional emails: It is the most common type of B2B (Business to Business) email, which is used to inform the email list of your new or existing products or services.
- Standalone Emails: These emails are popular like newsletters emails, but they contain a limitation.
- Onboarding emails: An onboarding email is a message that is used to strengthen customer loyalty, also known as post-sale emails.
- Transactional: These emails are related to account activity or a commercial transaction and sent from one sender to one recipient.

- Plain-Text Emails: It is a simple email that does not include images or graphics and no formatting; it only contains the text.
- Welcome emails: It is a type of B2B email and common parts of onboarding emails that help users get acquainted with the brand.

Examples of email attacks

Phishing: A form of fraud in which the attacks are the practice of sending fraudulent communications that appear to come from a reputable entity or person in email or other communication channels.

Spamming: Spam email is unsolicited bulk messages sent without explicit consent from the recipient, which is also known as junk email.

Spoofing: Email spoofing is an email message that could be obtained from someone or somewhere other than the intended source.

Business email compromise (BEC): A BEC is an exploit in which an authorized person or attacker hacks to a business email account and spoofs the owner's identity to defraud the company, its customers, partners of money.

Spear-phishing: Email spoofing is an attack where hackers target an individual or specific organization to gain sensitive information through unauthorized access.

Ransomware: It is a subset of malware that is used to encrypt a victim's files. Typically, it locks data by encryption on the victim's system. Typically, it locks data by encryption on the victim's system, and attackers demand payments before the ransomed data is decrypted.

Chat

- Chat refers to the process of communicating, interacting and/or exchanging messages over the Internet. It involves two or more individuals that communicate through a chat-enabled service or software.
- Chat is also known as chatting, online chat or Internet chat.
- Chat may be delivered through text, verbal, audio, visual or audio-visual (A/V) communication via the Internet. If conducted through a desktop, chat requires software that supports Internet Relay Chat (IRC) or an instant messenger application, where a central server manages chat communication between different end user clients.
- There are also online chat services that require users to sign up with a valid email address. After signing up, a user may join a group chat room or send a private message to another individual. Online chat services have purpose-built chat interfaces that manage the entire communication processes.

Following are the most common type of chatting:

Instant Messaging: It is the most common way of chatting. It is text-based communication. It happens between two people or groups of people.

Internet Relay Chat: It is known as IRC. It is also a text-based chat. It is not owned by any company and to use IRC we need a client program. Using IRC we can participate in discussion channels or can communicate with only two partners or users.

ICQ: It is known as I seek you. It is the most useful communication program. Using ICQ we can send files, URLs, and more. It is just like instant messaging but allows you to enter into the chat room and can chat with multiple people at a time.

Voice Chatting: We can chat not only with text but also with sounds as well. It is known as voice chatting. Voice chatting can be used with the internet just as a phone call. Internet voice call is free and unlimited, it only needs a good internet connection.

Video chatting: Video chatting is also a kind of chatting which is also done with the help of the internet and it also requires a webcam as it is a face to face chatting. Internet speed required by video chatting is higher as compared to text and video chatting. And a good quality camera too.

Chat Room

A chat room is a part of an online service where users can have conversations with each other through the internet. It can also be termed a virtual room. First users need to register to the server after registration users can log in with the help of a username and password.

Chatting Platforms

Nowadays there are many chatting platforms available for users. Some of them are mentioned below:

- Facebook
- WhatsApp
- Skype
- Telegram
- Snapchat
- Hike

World Wide Web

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc

The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP.

A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., www.facebook.com, www.google.com, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

Small websites store all of their WebPages on a single server, but big websites or organizations place their WebPages on different servers in different countries so that when users of a country search their site they could get the information quickly from the nearest server.

Difference between World Wide Web and Internet:

Internet

Internet is a worldwide network of devices like computers, laptops, tablets, etc. It enables users to send emails to other users and chat with them online. For example, when you send an email or chatting with someone online, you are using the internet.

World Wide Web

But, when you have opened a website like google.com for information, you are using the World Wide Web; a network of servers over the internet. You request a webpage from your computer using a browser, and the server renders that page to your browser. Your computer is called a client who runs a program (web browser), and asks the other computer (server) for the information it needs.

Hypertext Markup Language (HTML):

HTML is a standard markup language which is used for creating web pages. It describes the structure of web pages through HTML elements or tags. These tags are used to organize the pieces of content such as 'heading,' 'paragraph,' 'table,' 'Image,' and more.

Hypertext Transfer Protocol (HTTP):

Hyper Text Transfer Protocol (HTTP) is an application layer protocol which enables WWW to work smoothly and effectively. It is based on a client-server model. The client is a web browser which communicates with the web server which hosts the website. This protocol defines how messages are formatted and transmitted and what actions the Web Server and browser should take in response to different commands. When you enter a URL in the browser, an HTTP command is sent to the Web server, and it transmits the requested Web Page.

Search Engines

- A search engine is an online answering machine, which is used to search, understand, and organize content's result in its database based on the search query (keywords) inserted by the end-users (internet user).
- To display search results, all search engines first find the valuable result from their database, sort them to make an ordered list based on the search algorithm, and display in front of end-users.
- The process of organizing content in the form of a list is commonly known as a Search Engine Results Page (SERP).
- Google, Yahoo!, Bing, YouTube, and DuckDuckGo are some popular examples of search engines.

A list of advantages of search engines is given below -

1. Time-Saving
2. Variety of information
3. Precision
4. Free Access
5. Advanced Search
6. Relevance

Disadvantages of Search Engine

There are the following disadvantages of Search Engines -

- Sometimes the search engine takes too much time to display relevant, valuable, and informative content.
- Search engines, especially Google, frequently update their algorithm, and it is very difficult to find the algorithm in which Google runs.
- It makes end-users effortless as they all time use search engines to solve their small queries also.

Components of Search Engine

There are the following four basic components of Search Engine -

1. Web Crawler

Web Crawler is a software component that traverses on the web, then downloads and collects all the information over the Internet.

2. Database

The search engine database is a type of Non-relational database. It is the place where all the web information is stored.

3. Search Interfaces

Search Interface is an interface between the user and the database. It basically helps users to search for queries using the database.

4. Ranking Algorithms

The ranking algorithm is used by Google to rank web pages according to the Google search algorithm.

How do search engines work

There are the following tasks done by every search engines -

1. Crawling

Crawling is the first stage in which a search engine uses web crawlers to find, visit, and download the web pages on the WWW (World Wide Web). Crawling is performed by software robots, known as "spiders" or "crawlers." These robots are used to review the website content.

2. Indexing

Indexing is an online library of websites, which is used to sort, store, and organize the content that we found during the crawling. Once a page is indexed, it appears as a result of the most valuable and most relevant query.

3. Ranking and Retrieval

The ranking is the last stage of the search engine. It is used to provide a piece of content that will be the best answer based on the user's query. It displays the best content at the top rank of the website.

Search Engine Processing

There are following two major Search Engine processing functions -

1. Indexing process

Indexing is the process of building a structure that enables searching.

2. Query process

The query is the process of producing the list of documents based on a user's search query.

E-Commerce or Electronic Commerce

E-commerce is the meeting of buyers and sellers on the internet. This involves the transaction of goods and services, the transfer of funds and the exchange of data.

Types of E-Commerce Models

Electronic commerce can be classified into four main categories. The basis for this simple classification is the parties that are involved in the transactions. So the four basic electronic commerce models are as follows,

1. Business to Business(B2B)

This is Business to Business transactions. Here the companies are doing business with each other. The final consumer is not involved. So the online transactions only involve the manufacturers, wholesalers, retailers etc.

2. Business to Consumer(B2C)

Business to Consumer. Here the company will sell their goods and/or services directly to the consumer. The consumer can browse their websites and look at products, pictures, read reviews. Then they place their order and the company ships the goods directly to them. Popular examples are Amazon, Flipkart, Jabong etc.

3. Consumer to Consumer(C2C)

Consumer to consumer, where the consumers are in direct contact with each other. No company is involved. It helps people sell their personal goods and assets directly to an interested party. Usually, goods traded are cars, bikes, electronics etc. OLX, Quikr etc follow this model.

4. Consumer to Business(C2B)

This is the reverse of B2C, it is a consumer to business. So the consumer provides a good or some service to the company. Say for example an IT freelancer who demos and sells his software to a company. This would be a C2B transaction.

Examples of E-Commerce

- Amazon
- Flipkart
- eBay
- Fiverr
- Upwork
- Olx
- Quikr

Advantages of E-Commerce

- E-commerce provides the sellers with a global reach.
- Electronic commerce will substantially lower the transaction cost
- It provides quick delivery of goods with very little effort on part of the customer.
- One other great advantage is the convenience it offers. A customer can shop 24×7. The website is functional at all times, it does not have working hours like a shop.
- Electronic commerce also allows the customer and the business to be in touch directly, without any intermediaries.

Disadvantages of E-Commerce

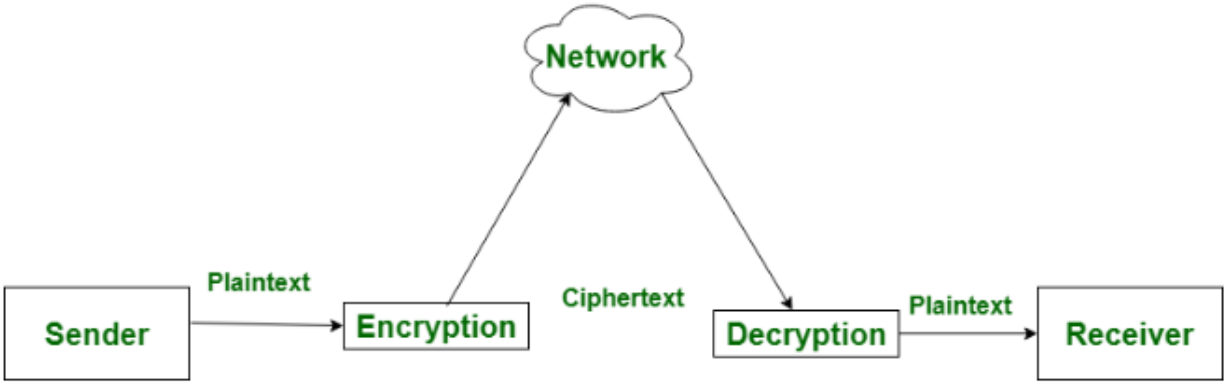
- The start-up costs of the e-commerce portal are very high.
- The e-commerce industry has a high risk of failure.
- It lacks the warmth of an interpersonal relationship which is important for many brands and products.
- Security is another area of concern. Only recently, we have witnessed many security breaches where the information of the customers was stolen. Credit card theft, identity theft etc. remain big concerns with the customers.
- Then there are also fulfillment problems. Even after the order is placed there can be problems with shipping, delivery, mix-ups etc. This leaves the customers unhappy and dissatisfied.

Principles of network security

- **Confidentiality**
  The function of "Confidentiality" is in protecting precious business data (in storage or in motion) from unauthorized persons. Confidentiality part of Network Security makes sure that the data is available OLNY to intended and authorized persons.
- **Integrity**
  Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need.
- **Availability**
  Availability is the assertion that a computer system is available or accessible by an authorized user whenever it is needed. Systems have high order of availability to ensures that the system operates as expected when needed. Availability provides building of fault tolerance system in the products.
- **Authentication**
  Authentication is the process of recognizing a user‘s identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user‘s information on a local operating system or within an authentication server.
- **Nonrepudiation**
  Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communicationin the presence of third parties called adversaries.



Encryption

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext).

Decryption

Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).

Symmetric Key Encryption

It only requires a single key for both encryption and decryption.

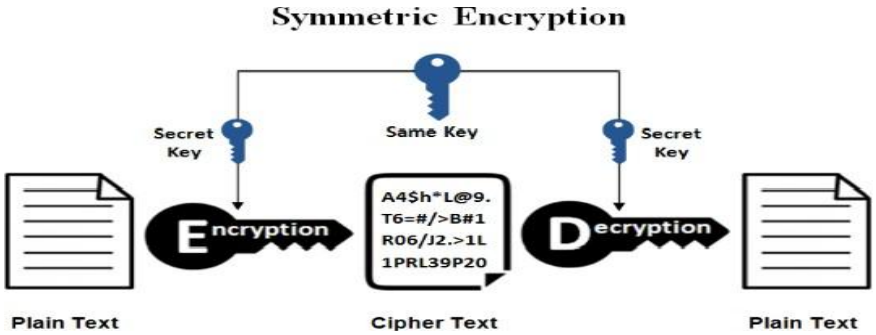
Asymmetric Key Encryption

It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.

Three types of cryptographic techniques used in general.

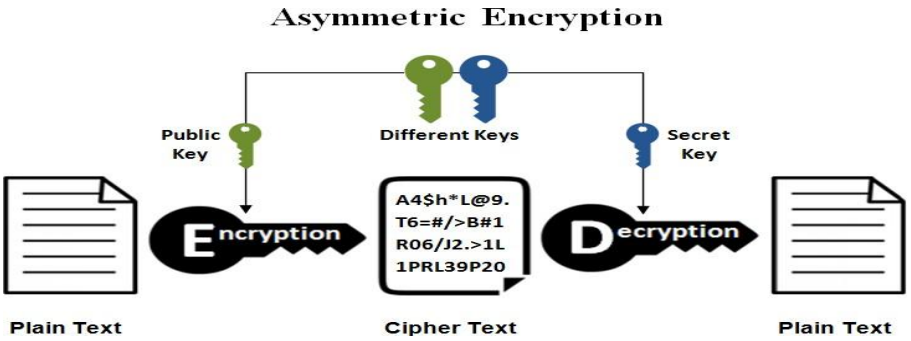
Symmetric-key Cryptography:

Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

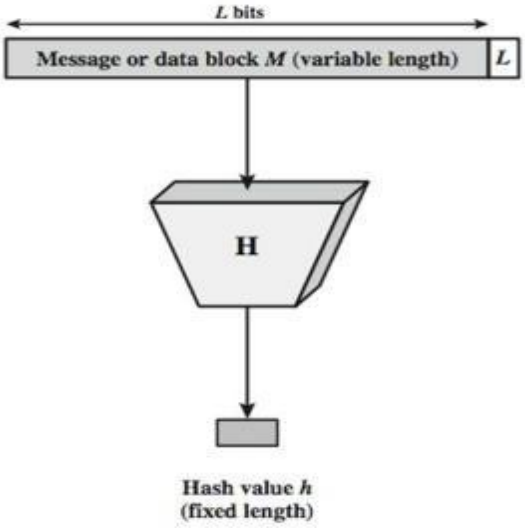


Public-Key/Asymmetric Key Cryptography:

This is the most revolutionary concept in the last 300-400 years. In Public- Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. **The public key is used for encryption and for decryption private key is used.**



Hash Functions:
No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

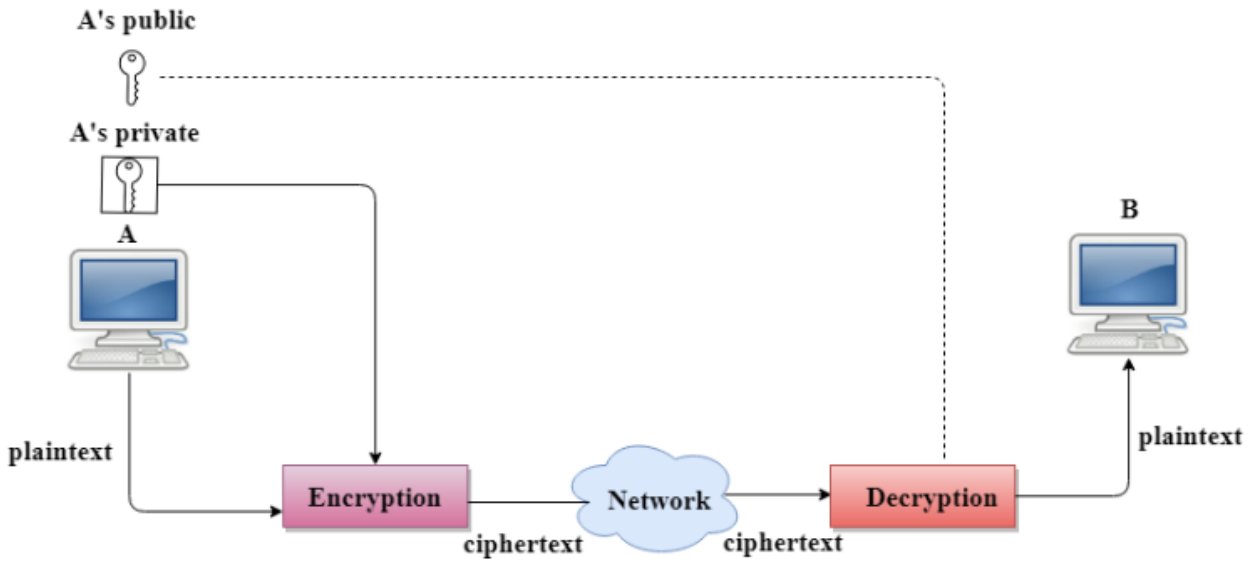


Digital Signature
The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.

The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

Signing the Whole Document

- In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
- In Digital Signature, the private key is used for encryption while the public key is used for decryption.
- Digital Signature cannot be achieved by using secret key encryption.



Digital Signature is used to achieve the following three aspects:

- **Integrity:** The Digital Signature preserves the integrity of a message because, if any malicious attack intercepts a message and partially or totally changes it, then the decrypted message would be impossible.
- **Authentication:** We can use the following reasoning to show how the message is authenticated. If an intruder (user X) sends a message pretending that it is coming from someone else (user A), user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore this makes the message unreadable. Encryption with X's private key and decryption with A's public key results in garbage value.
- **Non-Repudiation:** Digital Signature also provides non-repudiation. If the sender denies sending the message, then her private key corresponding to her public key is tested on the plaintext. If the decrypted message is the same as the original message, then we know that the sender has sent the message.

Note: Digital Signature does not provide privacy. If there is a need for privacy, then another layer of encryption/decryption is applied.

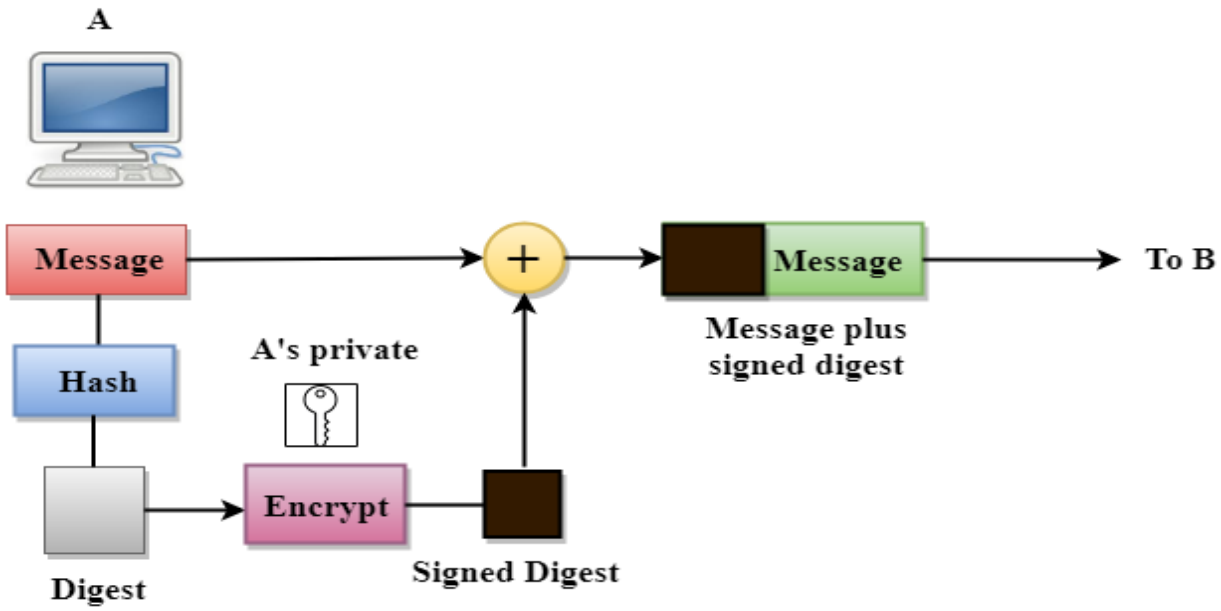
Signing the Digest

- Public key encryption is efficient if the message is short. If the message is long, a public key encryption is inefficient to use. The solution to this problem is to let the sender sign a digest of the document instead of the whole document.
- The sender creates a miniature version (digest) of the document and then signs it, the receiver checks the signature of the miniature version.
- The hash function is used to create a digest of the message. The hash function creates a fixed-size digest from the variable-length message.
- The two most common hash functions used: MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1). The first one produces 120-bit digest while the second one produces a 160-bit digest.
- A hash function must have two properties to ensure the success:
    - ✓ First, the digest must be one way, i.e., the digest can only be created from the message but not vice versa.
    - ✓ Second, hashing is a one-to-one function, i.e., two messages should not create the same digest.

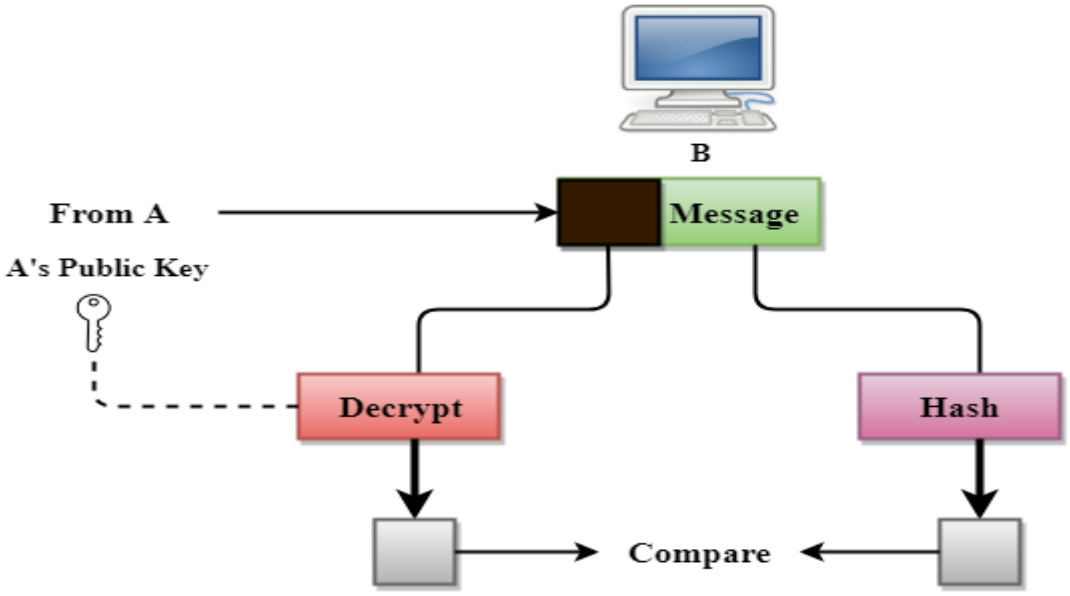
Following are the steps taken to ensure security:

- The miniature version (digest) of the message is created by using a hash function.
- The digest is encrypted by using the sender's private key.
- After the digest is encrypted, then the encrypted digest is attached to the original message and sent to the receiver.
- The receiver receives the original message and encrypted digest and separates the two. The receiver implements the hash function on the original message to create the second digest, and it also decrypts the received digest by using the public key of the sender. If both the digests are same, then all the aspects of security are preserved.

At the Sender site



At the Receiver site



Internet Telephony

Internet telephony is a type of communications technology that allows voice calls and other telephony services like fax, SMS and other voice-messaging applications to be transmitted using the Internet as a connection medium.
Internet telephony is also called IP telephony or broadband telephony.

Even though **Internet telephony** and **Voice over IP (VoIP)** are used synonymously, they mean two different things. ***Internet telephony*** *is defined as the umbrella technology, the one that encompasses all use of Internet Protocols (IP) for voice and telephone-like communications transmitted over the public Internet*. ***VoIP,*** *on the other hand, is simply one technology under Internet telephony*.

Internet telephony includes a wide range of communication involving various digital phone systems based on numerous IP addresses. It was developed in order to increase productivity by taking advantage of the Internet and various applications attached to it. In contrast, VoIP is merely a digital medium for voice calls offering cheap or free voice calls while adding more voice communication features.

Pros	Cons
• Lower costs	• Reliable internet connection required
• Increased accessibility	• Latency and jitter
• Complete portability	• No location tracking for emergency calls
• Higher scalability	
• Advanced features for small and large teams	
• Clearer voice quality	
• Support multitasking	
• More flexibility with softphones	

Virtual Reality

Virtual Reality (VR) is a computer-generated environment with scenes and objects that appear to be real, making the user feel they are immersed in their surroundings. This environment is perceived through a device known as a Virtual Reality headset or helmet. VR allows us to immerse ourselves in video games as if we were one of the characters, learn how to perform heart surgery or improve the quality of sports training to maximise performance.

Virtual Reality over the Web

VR is carving a path to the web and is set to affect web design in many interesting new ways.

VR is Integrating with Browsers (WebVR)

WebVR is the open standard that allows you to experience virtual reality in your browser. Many big name web browsers are now on board and in support of the whole WebVR experience. The whole VR experience will be available to the average consumer soon, making it possible to experience VR with just the click of a button, no downloads needed. The WebVR API is now available in several browsers; Firefox Nightly, Chrome 56+ for Android, Chromium for Windows (Experimental), and Samsung Internet Browser for Gear.

VR is Being Developed for Apps

Developers are beginning to create real apps using VR that can be helpful and useful for people. Developers are creating web apps for businesses that allow potential customers to have a virtual experience with a business's product or service. VR can be helpful when it comes to virtual tours and other simulated experiences that give users a chance to experience something before they actually purchase a product or service.

VR Could be Used for a Variety of Circumstances

WebVR is now being considered as useful in a wide variety of areas. The businessman who wants to give potential customers a more personal view of his services can use VR to give customers an avenue to walk down the halls in his hotel or to try on clothes from his establishment, all through virtual experiences that would closely simulate real life. On the other end of the spectrum, WebVR might even be useful in hospital trials that might experiment with escapists VR as a way of managing pain. The possibilities are endless. There are a myriad of different ways that VR could make using the web easier, more functional, and personal for the user, all while simulating reality closely enough to give the user a real glimpse into an actual experience without having to actually experience it in reality. WebVR would both challenge and expand the job of web designers/developers with all the unique nuances that make up VR.

Types of Internetwork:

1. **Extranet**:
   An extranet is a communication network based on the internet protocol such as Transmission Control protocol and internet protocol. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as MAN, WAN or other computer networks. An extranet cannot have a single LAN, atleast it must have one connection to the external network.
2. **Intranet**:
   An intranet is a private network based on the internet protocol such as Transmission Control protocol and internet protocol. An intranet belongs to an organization which is only accessible by the organization's employee or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

Communication:

It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.

Time-saving:

Information on the intranet is shared in real time, so it is time-saving.

Collaboration:

Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.

Platform independency:

It is a neutral architecture as the computer can be connected to another device with different architecture.

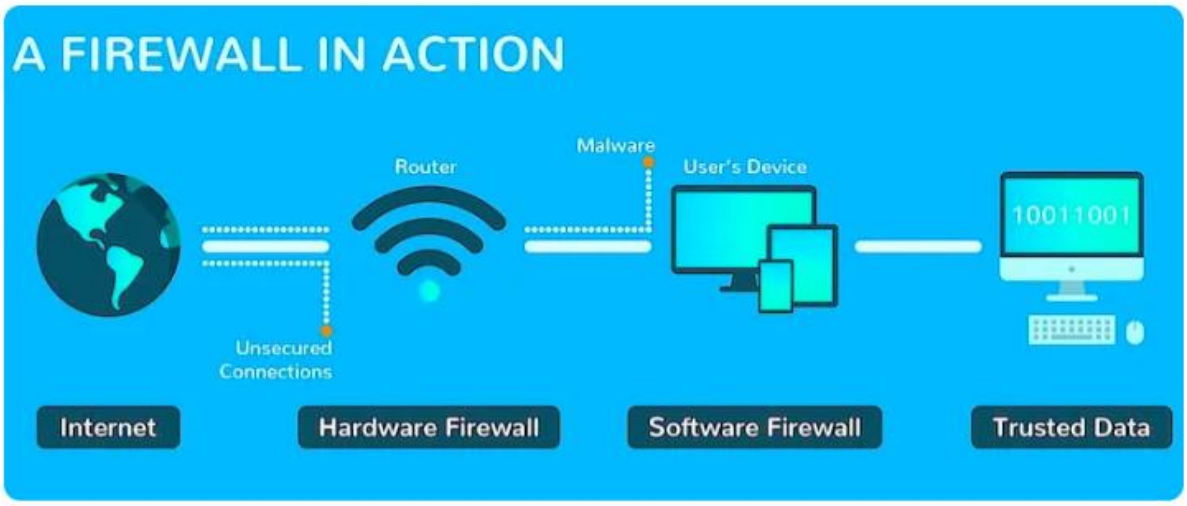
Cost effective:

People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

Firewall

A firewall is a network security system designed to prevent unauthorized access to or from a private network. In other words, it prevents unauthorized internet users from accessing private networks connected to the internet, especially intranets.

A firewall is not necessarily a standalone device, but servers or routers integrated with special software to provide security features. One can implant a firewall in either software or hardware form, or a combination of both.



The implementation must be done in such a way that all incoming/outgoing packets to/from the local network (Intranet) pass through the firewall.

How Does A Firewall Work?

Firewalls analyze each block of data packets entering or leaving the Intranet or the host computer. Based on a defined set of security rules, a firewall can perform three actions:

- **Accept**: allow the transmission of data packets.
- **Drop**: block data packets with no reply.
- **Reject**: Block data packets and send "unreachable error" to the source.

Different Types of Firewalls

Firewalls can be categorized into two groups: **host-based firewalls** and **network firewalls**. While both play a major role in data security, each has advantages and disadvantages.

- ✓ **Host-Based Firewalls** are placed directly on the computer to control data packets coming in and out of the machine. It could be a service or a program running in the background process as a part of agent applications or the operating system.
- ✓ **Network-based Firewalls** are placed on LANs, WANs, and Intranets. They filter traffic between two or more networks. They could be hardware-based computer appliances or software programs running on general-purpose hardware.

There are various types of firewalls that provide different levels of protection to networks and host computers.

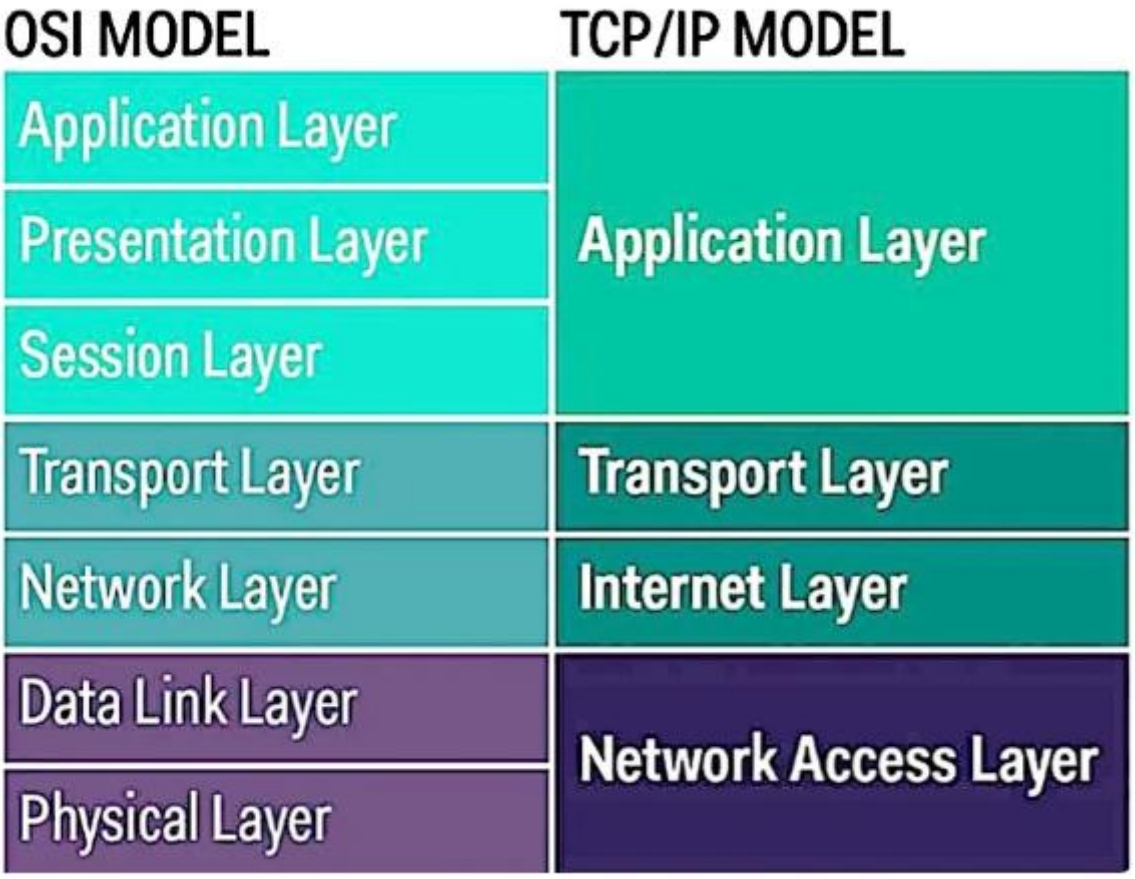
1. Packet Filters

Packet filters are the first-generation firewalls. They analyze data packets transmitted between computers. If any packet doesn't fulfill the filtering criteria, the firewall either rejects or drops the packet.

Since it operates at a lower level of the TCP/IP (a set of communication protocols used in the Internet), it is also called the Network layer firewall.

Packet filters are used in many versions of Unix, OpenBSD, Linux, and Mac OS X. For example, ipfirewall is used in FreeBSD, iptables in Linux, NPF in NetBSD, and PF in Mac OS X (>10.4).

2. Stateful Filters



Stateful filters are second-generation firewalls developed in the late 1980s. They track the operating state as well as the characteristics of network connections traversing it.

More specifically, the stateful filters track IP addresses and ports involved in the connection, as well as the sequence numbers of the packets traversing the connection. This allows them to examine particular conversations between two endpoints.

These firewalls are, however, vulnerable to DoS attacks, which involve flooding the targeted machine with superfluous requests in an attempt to overload the host computer and prevent legitimate requests from being fulfilled.

3. Application Firewalls

Applications firewalls are the third generation firewalls that can understand certain applications and protocols, such as HTTP, DNS, and FTP. It acts as an enhancement to the standard firewall by providing services up to the application layer (the top layer of the OSI model).

It works by analyzing the process ID of data packets against predefined rules of data transmission for the local network or host computer. The firewall hooks into socket calls to filter connections between application layers and lower layers in the OSI model.

Some services performed by application firewalls include data handling, execution of applications, blocking malicious programs from being executed, and more. Modern application firewalls are also capable of offloading encryption from servers, consolidating authentication, and blocking content that violates policies.

4. Next-generation Firewalls

A Next-generation firewall is an advanced part of the application firewall that combines a traditional firewall with other network device filtering functions. Its goal is to incorporate more layers of the OSI model and improve network traffic filtering based on packet contents.

In simple terms, next-generation firewalls include several additional features, such as integrated intrusion prevention, cloud-delivered threat intelligence, and application awareness and control.

They use a more thorough inspection style, analyzing packet payloads and matching signatures for malware, exploitable attacks, and other harmful activities.

5. Proxies

A proxy server can also act as a firewall by hiding the user's IP address and transmitting the data forward. It is mostly used to make requests from users and machines on the local network anonymous.

Unlike traditional firewalls, proxy firewalls filter network traffic at the application level. They monitor traffic for layer-7 protocols, such as FTP and HTTP, and use both stateful and deep packet inspection to analyze malicious traffic.

In addition to security, modern proxies also provide better performance (by caching frequency requested resources) and error correction facility (by automatically repairing errors in the proxied content).

6. Network Address Translation

As firewalls were becoming more popular, another issue was rising: the number of available IPv4 addresses was decreasing with a threat of exhaustion. Researchers developed various mechanisms to deal with this problem. One of those mechanisms was Network Address Translation (NAT).