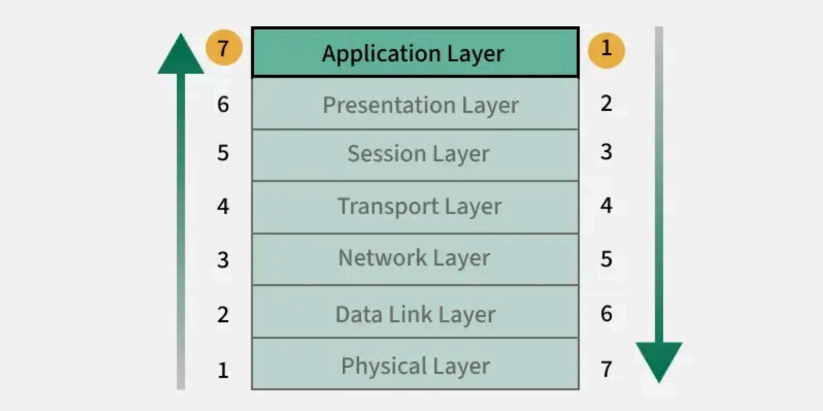
Application Layer in OSI Model

Last Updated : 28 Jan, 2025

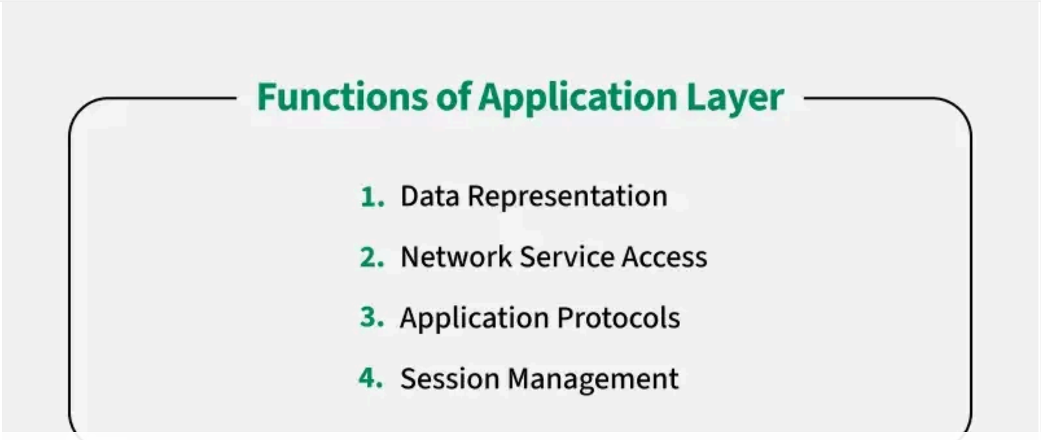
The Application Layer of OSI (Open System Interconnection) model, is the top layer in this model and takes care of network communication. The application layer provides the functionality to send and receive data from users. It acts as the interface between the user and the application. The application provides services like file transmission, mail service, and many more.



Application Layer in OSI Model

Functions of Application Layer

The Application Layer, being topmost layer in OSI model, performs functions required in any kind of application or communication process. Let's have a look into the functions:



Functions of Application Layer

1. Data Representation
2. Network Service Access
3. Application Protocols
4. Session Management

Working of Application Layer

- At first, client sends a command to server and when server receives that command, it allocates port number to client.
- Thereafter, the client sends an initiation connection request to server and when server receives request, it gives acknowledgement (ACK) to client through client has successfully established a connection with the server.
- Therefore, now client has access to server through which it may either ask server to send any types of files or other documents or it may upload some files or documents on server itself.

Services Provided by Application Layer Protocols

The following are some of the services which are provided by Application layer protocols-

- The Application Layer protocol defines process for both parties which are involved in communication.
- These protocols define the type of message being sent or received from any side (either source host or destination host).
- These protocols also define basic syntax of the message being forwarded or retrieved.
- These protocols define the way to send a message and the expected response.
- These protocols also define interaction with the next level.

Read in detail about Services Provided by Application Layer.

Protocols of the Application Layer

The application layer provides several protocols which allow any software to easily send and receive information and present meaningful data to its users. The following are some of the application layer protocols.

- **HTTP:** HTTP stands for Hyper Text Transfer Protocol. It is the foundation of the World Wide Web (WWW). HTTP works on the client server model. This protocol is used for transmitting hypermedia documents like HTML. This protocol was designed particularly for the communications between the web browsers and web servers, but this protocol can also be used for several other purposes. HTTP is a stateless protocol (network protocol in which a client sends requests to server and server responses back as per the given state), which means the server is not responsible for maintaining the previous client's requests. HTTP uses port number 80.

- **DNS:** DNS stands for Domain Name System. The DNS service translates the domain name (selected by user) into the corresponding IP address. For example- If you choose the domain name as www.abcd.com, then DNS must translate it as 192.36.20.8 (random IP address written just for understanding purposes). DNS protocol uses the port number 53.
- **TELNET:** Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows the Telnet clients to access the resources of Telnet server. Telnet uses port number 23.
- **DHCP:** DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.
- **FTP:** FTP stands for File Transfer Protocol. This protocol helps to transfer different files from one device to another. FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer. FTP uses port number 20 for data access and port number 21 for data control.
- **SMTP:** SMTP stands for Simple Mail Transfer Protocol. It is used to transfer electronic mail from one user to another user. SMTP is used by end users to send emails with ease. SMTP uses port numbers 25 and 587. .
- **NFS:** NFS stands for Network File System. This protocol allows remote hosts to mount files over a network and interact with those

file systems as though they are mounted locally. NFS uses the port number 2049.
- **SNMP:** SNMP stands for Simple Network Management Protocol. This protocol gathers data by polling the devices from the network to the management station at fixed or random intervals, requiring them to disclose certain information. SNMP uses port numbers 161 (TCP) and 162 (UDP).

Read in detail about **Protocols in Application Layer**.

Next Article

Protocol and Standard in Computer Networks

Similar Reads

Presentation Layer in OSI model

Presentation Layer is the 6th layer in the Open System Interconnection (OSI) model. This layer is also known as Translation layer, as this layer...

15+ min read

What is OSI Model? - Layers of OSI Model

The OSI (Open Systems Interconnection) Model is a set of rules that explains how different computer systems communicate over a network....

15+ min read

Application Layer Services

The Application Layer is the topmost layer in the OSI (Open Systems Interconnection) model, directly interacting with end-user applications. I...

15+ min read

Protocols in Application Layer

Last Updated : 28 Dec, 2024

The Application Layer is the topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data which enables any type of user to access the network with ease. The Application Layer interface directly interacts with the application and provides common web application services. The application layer performs several kinds of functions that are required in any kind of application or communication process. In this article, we will discuss various application layer protocols.

What are Application Layer Protocols?

Application layer protocols are those protocols utilized at the application layer of the OSI (Open Systems Interconnection) and TCP/IP models. They facilitate communication and data sharing between software applications on various network devices. These protocols define the rules and standards that allow applications to interact and communicate quickly and effectively over a network.

Application Layer Protocol in Computer Network

1. TELNET

Telnet stands for the TELetype NETwork. It helps in terminal emulation. It allows Telnet clients to access the resources of the Telnet server. It is used for managing files on the Internet. It is used for the initial setup of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. The port number of the telnet is 23.

Command

▲
Open In App

```
telnet [\\RemoteServer]
\\RemoteServer
: Specifies the name of the server
to which you want to connect
```

2. FTP

FTP stands for File Transfer Protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. The Port number for FTP is 20 for data and 21 for control.

Command

```
ftp machinename
```

3. TFTP

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it. It's a technology for transferring files between network devices and is a simplified version of FTP. The Port number for TFTP is 69.

Command

```
tftp [ options... ] [host [port]] [-c command]
```

4. NFS

It stands for a Network File System. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network. The Port number for NFS is 2049.

```
service nfs start
```

5. SMTP

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called “store and forward,” SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. The Port number for SMTP is 25.

Command

```
MAIL FROM:<mail@abc.com?
```

6. LPD

It stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A “daemon” is a server or agent. The Port number for LPD is 515.

Command

```
lpd [ -d ] [ -l ] [ -D DebugOutputFile]
```

7. X window

It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes. Port number for X window starts from 6000 and increases by 1 for each server.

Command

```
Run xdm in runlevel 5
```

8. SNMP

It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. The Port number of SNMP is 161(TCP) and 162(UDP).

Command

```
snmpget -mALL -v1 -cpublic snmp_agent_Ip_address sysName.0
```

9. DNS

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4.
The Port number for DNS is 53.

Command

```
ipconfig /flushdns
```

10. DHCP

It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

Command

```
clear ip dhcp binding {address | * }
```

11. HTTP/HTTPS

HTTP stands for Hypertext Transfer Protocol and HTTPS is the more secured version of HTTP, that's why HTTPS stands for Hypertext Transfer Protocol Secure. This protocol is used to access data from the World Wide Web. The Hypertext is the well-organized documentation system that is used to link pages in the text document.

- HTTP is based on the client-server model.
- It uses TCP for establishing connections.
- HTTP is a stateless protocol, which means the server doesn't maintain any information about the previous request from the client.
- HTTP uses port number 80 for establishing the connection.

12. POP

POP stands for Post Office Protocol and the latest version is known as POP3 (Post Office Protocol version 3). This is a simple protocol used by User agents for message retrieval from mail servers.

- POP protocol work with Port number 110.
- It uses TCP for establishing connections.

POP works in dual mode- *Delete mode, Keep Mode*.

In Delete mode, it deletes the message from the mail server once they are downloaded to the local system.

In Keep mode, it doesn't delete the message from the mail server and also facilitates the users to access the mails later from the mail server.

13. IRC

IRC stands for Internet Relay Chat. It is a text-based instant messaging/chatting system. IRC is used for group or one-to-one communication. It also supports file, media, data sharing within the chat. It works upon the client-server model. Where users connect to IRC server or IRC network via some web/ standalone application program.

- It uses TCP or TLS for connection establishment.
- It makes use of port number 6667.

14. MIME

MIME stands for Multipurpose Internet Mail Extension. This protocol is designed to extend the capabilities of the existing Internet email protocol like SMTP. MIME allows non-ASCII data to be sent via SMTP. It allows users to send/receive various kinds of files over the Internet like audio, video, programs, etc. MIME is not a standalone protocol it works in collaboration with other protocols to extend their capabilities.

Conclusion

Application layer protocols are required to enable communication and data exchange between software applications on different network devices. These protocols, which include HTTP, FTP, SMTP, and DNS, specify the rules and standards that enable applications to communicate easily across a network. Each protocol serves a distinct purpose, ranging from file transfer and email management to network device configuration and web page access, providing efficient and effective network connection.

Comment More info

Advertise with us

Next Article

Domain Name System (DNS)

Similar Reads

Application Layer Services

The Application Layer is the topmost layer in the OSI (Open Systems Interconnection) model, directly interacting with end-user applications. I...

15+ min read

Application Layer Protocols in TCP/IP

TCP/IP stands for Transport Control Protocol/Internet Protocol. TCP/IP suite is considered as a basis on which a virtual network exists. TCP/IP...

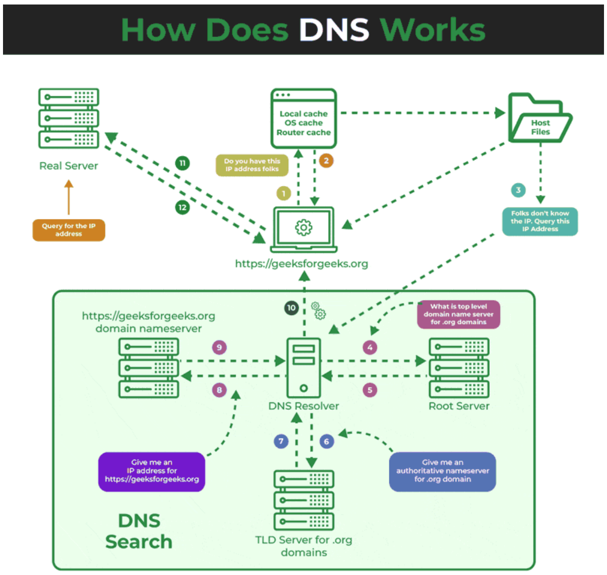
Open In App

Domain Name System (DNS)

Last Updated : 15 Feb, 2025

The Domain Name System (DNS) translates human-readable domain names (e.g., www.google.com) into machine-readable IP addresses (e.g., 142.250.190.14), enabling internet communication

- It enables computers to locate and communicate with each other on the internet.
- Functions as a **hierarchical, distributed database**.
- Queries pass through multiple levels:
  - **Root server**
  - **Top-Level Domain (TLD) server**
  - **Authoritative server** (stores the specific IP address).
- Ensures seamless website access using easy-to-remember names instead of numerical IP addresses.


How Does DNS Works
Real Server
Query for the IP address
Local cache
OS cache
Router cache
Do you have this IP address folks
Host Files
Folks don't know the IP. Query this IP Address
https://geeksforgeeks.org
1
2
3
11
12
10
https://geeksforgeeks.org domain nameserver
What is top level domain name server for .org domains
9
8
4
5
DNS Resolver
Root Server
7
6
Give me an IP address for https://geeksforgeeks.org
Give me an authoritative nameserver for .org domain
TLD Server for .org domains
DNS Search

How DNS Works

How Does DNS Work?

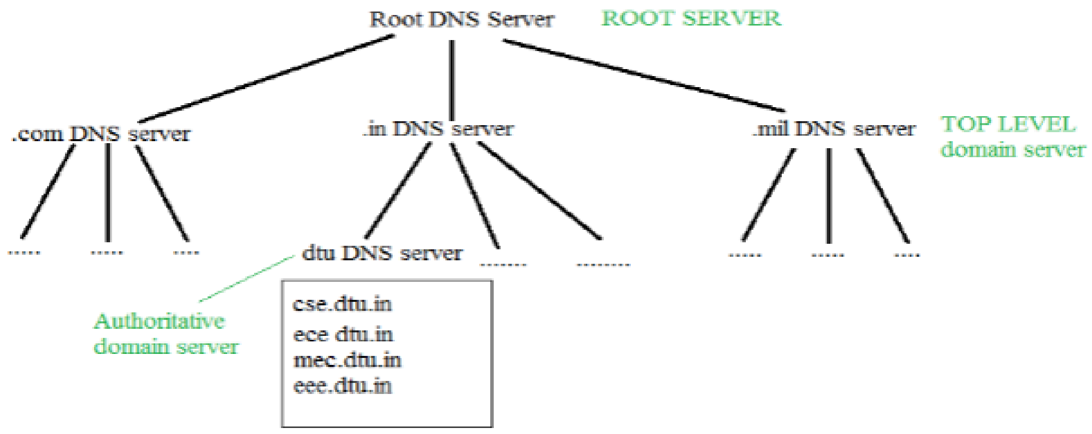
- When we type a website like https://www.geeksforgeeks.org in our browser, our computer tries [illegible] IP address.

- First, it checks the local cache (our browser, operating system, or router) to see if it already knows the IP address.
- If the local cache doesn't have the IP, the query is sent to a DNS resolver to find it.
- DNS resolver may check host files (used for specific manual mappings), but usually, it moves on.
- Resolver sends the query to a Root DNS server, which doesn't know the exact IP address but points to the TLD server (e.g., .org server for this example).
- TLD server then directs the resolver to the authoritative nameserver for geeksforgeeks.org.
- Authoritative nameserver knows the exact IP address for geeksforgeeks.org and sends it back to the resolver.
- Resolver passes the IP address to our computer.
- Our computer uses the IP address to connect to the real server where the website is hosted.
- The website loads in our browser.

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

Structure of DNS

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.

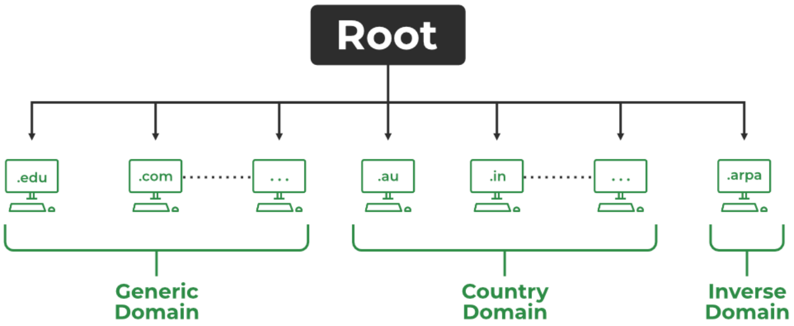
> *DNS = Name service in Internet – A zone is an administrative unit, and a domain is a subtree.*

Types of Domain

There are various kinds of domains:

- **Generic Domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
- **Country Domain:** .in (India) .us .uk
- **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

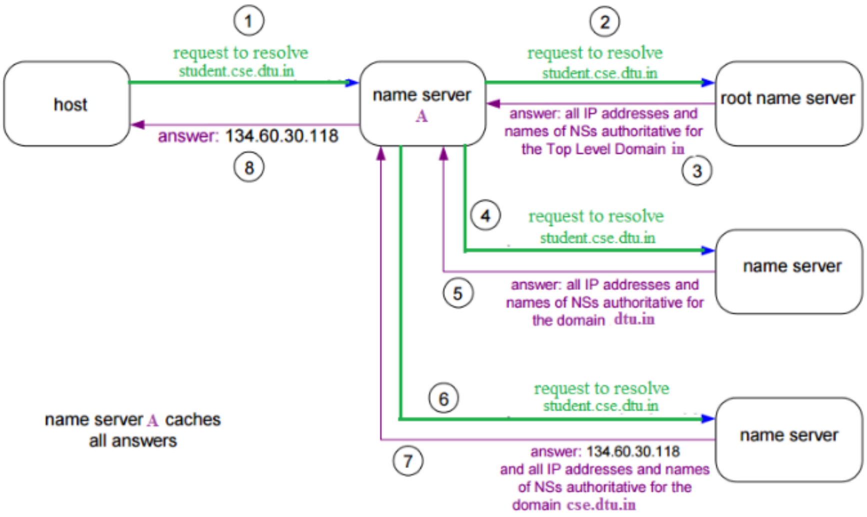
```
nslookup www.geeksforgeeks.org
```



Types of DNS

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.


1
request to resolve student.cse.dtu.in
host
name server A
answer: 134.60.30.118
8
2
request to resolve student.cse.dtu.in
root name server
answer: all IP addresses and names of NSs authoritative for the Top Level Domain in
3
4
request to resolve student.cse.dtu.in
name server
5
answer: all IP addresses and names of NSs authoritative for the domain dtu.in
6
request to resolve student.cse.dtu.in
name server
7
answer: 134.60.30.118 and all IP addresses and names of NSs authoritative for the domain cse.dtu.in
name server A caches all answers

Domain Name Server

DNS Lookup

DNS Lookup, also called DNS Resolution, is the process of translating a human-readable domain name (like www.example.com) into its corresponding IP address (like 192.0.2.1), which computers use to locate and communicate with each other on the internet. It allows users to access websites easily using names instead of remembering numeric IP addresses.

- DNS Lookup starts when a user types a domain name into their browser.
- The query goes through a series of servers: the DNS resolver, Root server, TLD server, and authoritative server.
- Each server plays a role in finding the correct IP address for the domain.
- Once the IP address is found, the browser connects to the website's server and loads the page.

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.

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.

DNS Caching

DNS Caching can be simply termed as the process used by DNS Resolvers for storing the previously resolved information of DNS that contains domain names, and IP Addresses for some time. The main principle of DNS Caching is to speed up the process of future DNS lookup and also help in reducing the overall time of DNS Resolution.

- **Speeds Up Access**: It stores previous website lookups, so your device can quickly load frequently visited sites without asking the network for the IP address each time.
- **Reduces Internet Traffic**: This storage cuts down on the number of requests sent across the internet, helping reduce overall network congestion.
- **Enhances User Experience**: With faster loading times for websites and less waiting, browsing the internet becomes a smoother, more enjoyable experience.

Comment More info

Advertise with us

Next Article

Records in DNS

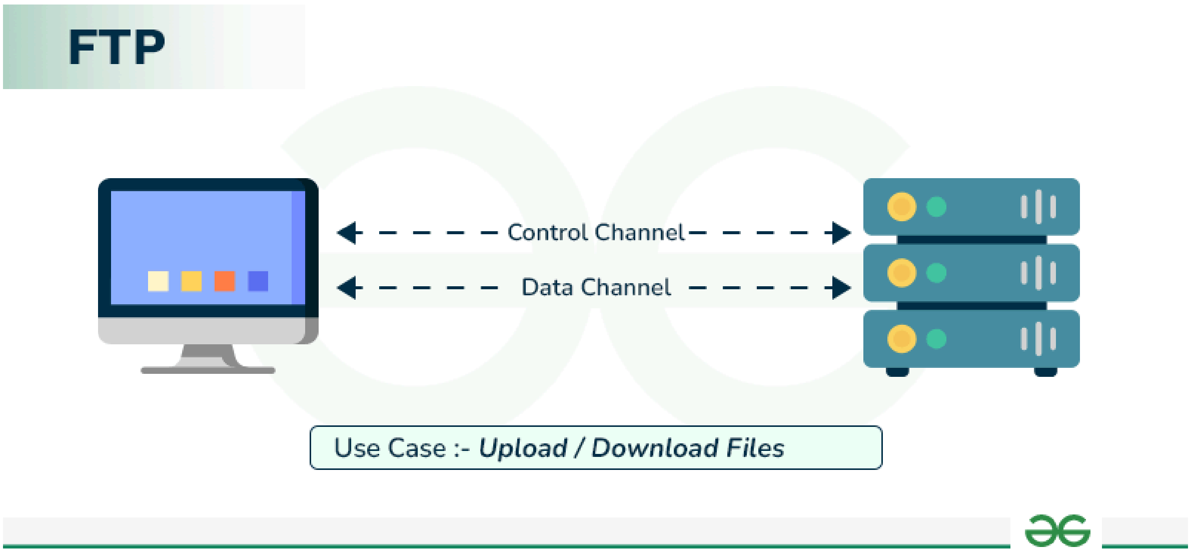
File Transfer Protocol (FTP) in Application Layer

Last Updated : 28 Dec, 2024

FTP or File Transfer Protocol is said to be one of the earliest and also the most common forms of transferring files on the internet. Located in the application layer of the OSI model, FTP is a basic system that helps in transferring files between a client and a server. It is what makes the FTP unique that the system provides a reliable and efficient means of transferring files from one system to another even if they have different file structures and operating systems. Contrary to other protocols such as http that cover hypertexts and web resources in general, ftp is dedicated to the management and the transfer of text, binary, or image files.

What is File Transfer Protocol?

FTP is a standard communication protocol. There are various other protocols like HTTP which are used to transfer files between computers, but they lack clarity and focus as compared to FTP. Moreover, the systems involved in connection are heterogeneous, i.e. they differ in operating systems, directories, structures, character sets, etc the FTP shields the user from these differences and transfers data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files. The ASCII is the default file share format, in this, each character is encoded by NVT ASCII. In ASCII or EBCDIC the destination must be ready to accept files in this mode. The image file format is the default format for transforming binary files.



File Transfer Protocol

The **File Transfer Protocol (FTP)** is widely used in the application layer of networking. It works at the application layer, ensuring that files are sent and received securely.

Types of FTP

There are different ways through which a server and a client do a file transfer using FTP. Some of them are mentioned below:

- **Anonymous FTP:** Anonymous FTP is enabled on some sites whose files are available for public access. A user can access these files without having any username or password. Instead, the username is set to anonymous, and the password is to the guest by default. Here, user access is very limited. For example, the user can be allowed to copy the files but not to navigate through directories.

- **Password Protected FTP:** This type of FTP is similar to the previous one, but the change in it is the use of username and password.

- **FTP Secure (FTPS):** It is also called as FTP Secure Sockets Layer (FTP SSL). It is a more secure version of FTP data transfer. Whenever FTP connection is established, Transport Layer Security (TLS) is enabled.

- **FTP over Explicit SSL/TLS (FTPES):** FTPES helps by upgrading FTP Connection from port 21 to an encrypted connection.

- **Secure FTP (SFTP):** SFTP is not a FTP Protocol, but it is a subset of Secure Shell Protocol, as it works on port 22.

What is FTP Useful For?

FTP is especially useful for:

- **Transferring Large Files:** FTP can transfer large files in one shot; thus applicable when hosting websites, backing up servers, or sharing files in large quantities.
- **Remote File Management:** Files on a remote server can be uploaded, downloaded, deleted, renamed, and copied according to the users' choices.
- **Automating File Transfers:** FTP is a great protocol for the execution of file transfers on predefined scripts and employments.
- **Accessing Public Files:** Anonymous FTP means that everybody irrespective of the identity is allowed to download some files with no permissions needed.

How to Use FTP?

To use FTP, follow these steps:

- **Connect to the FTP Server:** One can connect to the server using the address, username and password through an FTP client or a command line interface. Anonymous Information may not need a username and password.
- **Navigate Directories:** Some commands include ls that is used to list directories and cd that is used to change directories.
- **Transfer Files:** File transfer may be done by using the commands such as get for downloading files, and put for uploading files.
- **Manage Files:** Make operations like deletion (Delete), renaming (Rename) as well as copying (Copy) of files.
- **Close the Connection:** Once file transfer has been accomplished, terminate the connection by giving the bye or quit command.

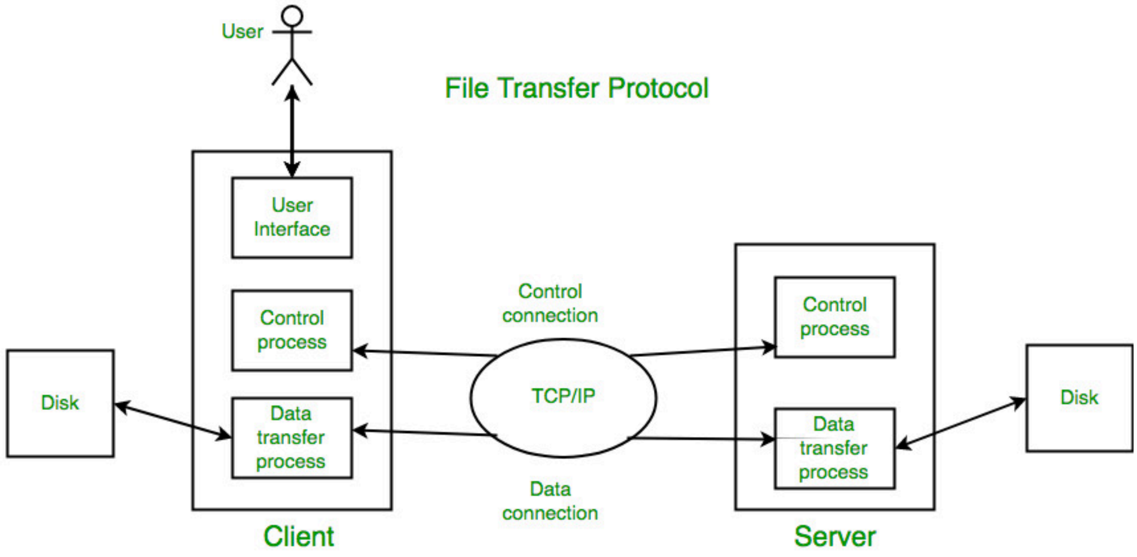
How Does FTP Work?

FTP is a client server protocol that has two communication channel, command channel for conversation control and data channel for file content.

Here are steps mentioned in which FTP works:

- A user has to log in to FTP Server first, there may be some servers where you can access to content without login, known as anonymous FTP.
- Client can start a conversation with server, upon requesting to download a file.
- The user can start different functions like upload, delete, rename, copy files, etc. on server.

FTP can work on different modes like Active and Passive modes. For more, you can refer to Difference between Active and Passive FTP.



Types of Connection in FTP

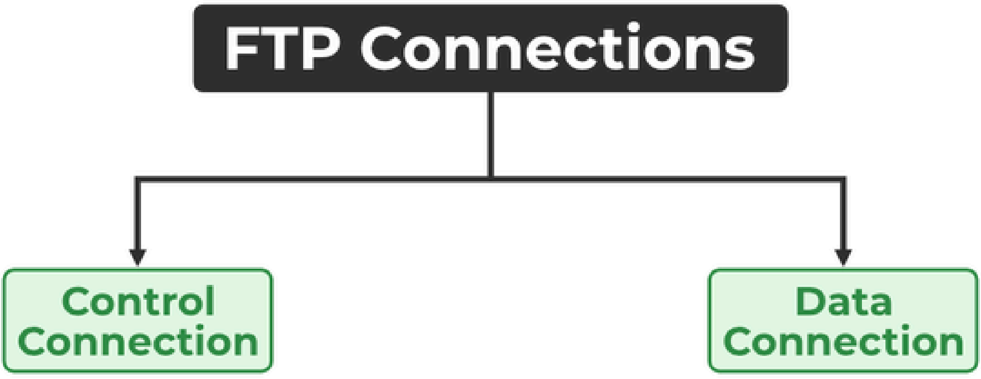
- Control Connection
- Data Connection

Control Connection

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.

Data connection

For sending the actual file, FTP makes use of a data connection. A data connection is initiated on port number 20.
FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.



FTP Session

When an FTP session is started between a client and a server, the client initiates a control TCP connection with the server side. The client sends control information over this. When the server receives this, it initiates a data connection to the client side. But the control connection remains active throughout the user session. As we know HTTP is stateless . But FTP needs to maintain a state about its user throughout the session.

FTP Clients

FTP works on a client-server model. The FTP client is a program that runs on the user's computer to enable the user to talk to and get files from remote computers. It is a set of commands that establishes the connection between two hosts, helps to transfer the files, and then closes the connection.

Some of the commands are:

get the filename(retrieve the file from the server)

get the filename(retrieve multiple files from the server)

ls(list files available in the current directory of the server)

There are also built-in FTP programs, which makes it easier to transfer files and it does not require remembering the commands.

FTP Data Types

The data type of a file, which determines how the file is represented overall, is the first piece of information that can be provided about it. The FTP standard specifies the following four categories of data:

- **ASCII:** Describes an ASCII text file in which each line is indicated by the previously mentioned type of end-of-line marker.
- **EBCDIC:** For files that use IBM's EBCDIC character set, this type is conceptually identical to ASCII.
- **Image:** This is the "black box" mode I described earlier; the file has no formal internal structure and is transferred one byte at a time without any processing.
- **Local:** Files containing data in logical bytes with a bit count other than eight can be handled by this data type.

FTP Replies

Some of the FTP replies are:

- 200 – Command okay.
- 530 – Not logged in.
- 331 – User name okay, need a password.
- 221 – Service closing control connection.

- 551 – Requested action aborted: page type unknown.
- 502 – Command not implemented.
- 503 – Bad sequence of commands.
- 504 – Command not implemented for that parameter.

Characteristics of FTP

- FTP uses TCP as a transport layer protocol.
- It is good for simple file transfers, such as during boot time.
- Errors in the transmission (lost packets, checksum errors) must be handled by the TFTP server.
- It uses only one connection through well-known port 69.
- TFTP uses a simple lock-step protocol (each data packet needs to be acknowledged). Thus the throughput is limited.

FTP’s Security Issues

- Information could not go across a secure tunnel since FTP was not intended to do so. Thus, encryption is not present. A hacker would not need to struggle with encryption to access or alter data that is usable if they could intercept an FTP transaction.
- Even with FTP cloud storage, data can still be intercepted and misused if the service provider’s system is attacked.
- As a result, data sent via FTP is a target for spoofing, sniffing, brute force, and other types of attacks that move somewhat slowly. A hacker might examine an FTP transmission and try to take advantage of any flaws by simply port scanning.
- The fact that FTP uses clear-text passwords—passwords that haven’t been encrypted—is one of its main security flaws. Put differently, “Jerry1992” appears exactly like “Jerry1992.” The real password is hidden via an algorithm in more secure protocols. As a result, “Jerry1992” might appear as “dj18387saksng8937d9d8d7s6a8d89.” Passwords like this are not secured by FTP, which makes them more easily cracked by malicious actors.

What is an FTP Port?

FTP operates using two ports:

- **Port 21:** As mentioned earlier this is where the commands are issued.
- **Port 20:** This is the special port required for data connection where the real transfer of file is made.

How to Change FTP Port Numbers

To change the default FTP port numbers, follow these steps:

- **Access Server Configuration:** Connect the control panel of your FTP server well as the FTP server configuration file used.
- **Modify the Port Number:** Find out the possible port settings from the configuration file. Alter the control port, default port is 21 and that of the data is 20.
- **Restart the FTP Service:** Finally once you have saved your changes you need to stop and restart the FTP service so that the new port settings can be implemented.
- **Update Client Settings:** Make certain that all the FTP clients that connect with the server are notified of the new port numbers.

Advantages of FTP

- File sharing also comes in the category of advantages of FTP in this between two machines files can be shared on the network.
- Speed is one of the main benefits of FTP.
- Since we don’t have to finish every operation to obtain the entire file, it is more efficient.
- Using the username and password, we must log in to the FTP server. As a result, FTP might be considered more secure.
- We can move the files back and forth via FTP. Let’s say you are the firm manager and you provide information to every employee, and they all reply on the same server.

Disadvantages of FTP

- File size limit is the drawback of FTP only 2 GB size files can be transferred.

- More then one receivers are not supported by FTP.
- FTP does not encrypt the data this is one of the biggest drawbacks of FTP.
- FTP is unsecured we use login IDs and passwords making it secure but they can be attacked by hackers.

Difference Between FTP and SFTP

FTP	SFTP
It stands for File Transfer Protocol.	It stands for Secure File Transfer Protocol.
In FTP, secure channel is not provided to transfer the files between the hosts.	In SFTP, a secure channel is provided to transfer the files between the hosts.
It usually runs on port no-21.	It usually runs on port no-22.
It does not encrypt the data before sending	It encrypted data before sending.
It makes uploading and downloading of files without any security.	It maintains full security of the data by using SSH keys.

FTP Security Challenges

FTP was not designed with security in mind, leading to several vulnerabilities:

- **Lack of Encryption:** This is because data such as usernames and passwords are transmitted without encryption and hence easily vulnerable to different attacks.

- **Vulnerabilities to Attacks:** FTP transmissions are vulnerable to attacks such as spoofing, sniffing, brute force , and the likes are slow attacks. They suggested that the data can be intercepted and changed easily by hackers .
- **Clear-Text Passwords:** Unfortunately, FTP client authentication employs non encrypted passwords, which makes them vulnerable to hacking.

Conclusion

FTP is still a powerful and effective method for transferring files between systems and still prevails in cases of transferring large files, and in the course of automated systems. Nevertheless, it does not come with security enhancements making it fairly inadequate for sensitive information exchange. In the case of transfers, safer modes like SFTP or FTPS should be encouraged since they make transfers secure. Hence, despite these drawbacks, FTP remains useful to this day since it is simple and stabilized.

Comment More info

Advertise with us

Next Article

Basics of Wi-Fi

Similar Reads

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer mechanism (SMTP) is a mechanism for exchanging email messages between servers. It is an essential component of the...

15+ min read

What is TFTP (Trivial File Transfer Protocol)?

The network is made up of various devices. These devices are either connected by ethernet or by any wireless means. The communication fo...

Open In App

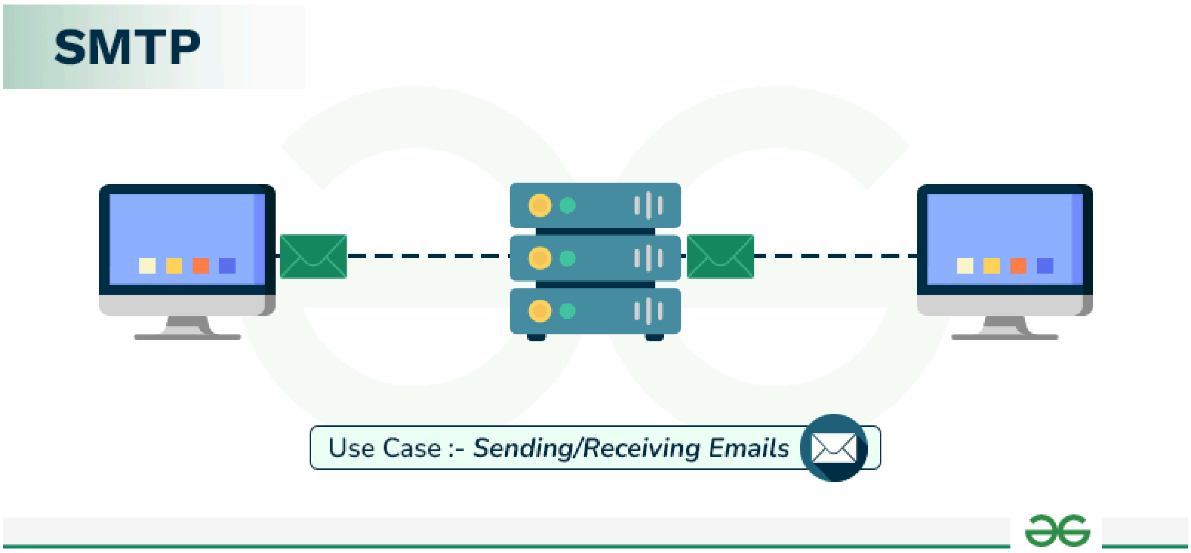
Simple Mail Transfer Protocol (SMTP)

Last Updated : 08 Apr, 2025

Simple Mail Transfer mechanism (SMTP) is a mechanism for exchanging email messages between servers. It is an essential component of the email communication process and operates at the application layer of the TCP/IP protocol stack. SMTP is a protocol for transmitting and receiving email messages. In this article, we are going to discuss every point about SMTP.

What is Simple Mail Transfer Protocol?

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.



SMTP

SMTP Protocol

The SMTP model is of two types:

- End-to-End Method
- Store-and-Forward Method

The end-to-end model is used to communicate between different organizations whereas the store and forward method is used within an organization. An SMTP client who wants to send the mail will contact the destination's host SMTP directly, to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.
The client SMTP is the one that initiates the session so let us call it the client-SMTP and the server SMTP is the one that responds to the session request so let us call it receiver-SMTP. The client-SMTP will start the session and the receiver SMTP will respond to the request.

Before diving deeper into the **Model of SMTP System**, it's important to understand how SMTP is leveraged by service providers like **SMTP.com** in the real-world scenario.

SMTP.com is a platform that caters to all your **transaction, email relay and email delivery needs** at a very affordable price. With decades of experience, SMTP.com is regarded as the most trusted sender in the industry by ISPs. SMTP.com had been trusted by over 100,000 customers over the years.

SMTP.com is extremely intuitive and easy to set up. It can be integrated seamlessly into your current business system. If you need to migrate from another provider, SMTP.com makes it effortless.

Features

- **Dedicated IP**
- **Email API:** Integrating SMTP.com with your business can be easy with the email API feature. They have complete API documentation on their website that can help you integrate your business in just 5 minutes.

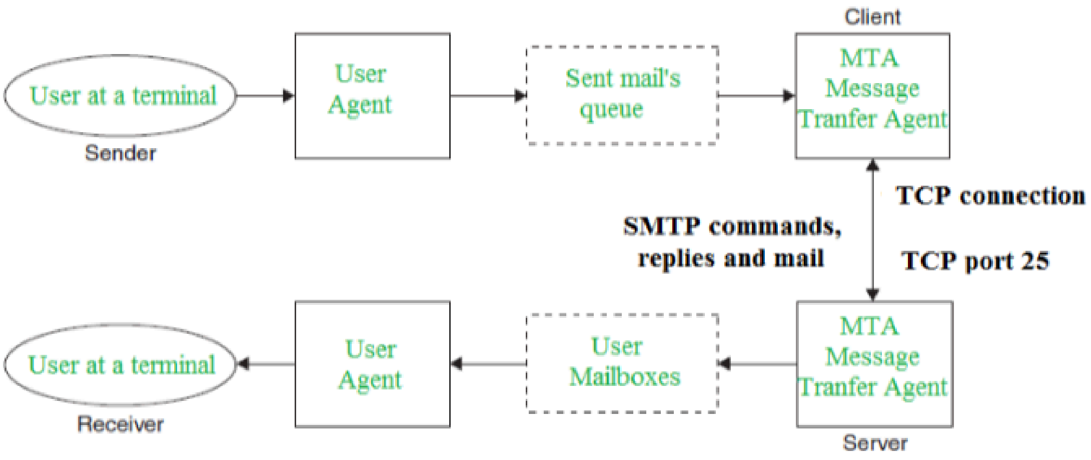
- **24×7 Customer Support:** The round-the-clock support is one of the best features of SMTP.com. Support is available both on the website and also for paid customers. 24×7, all human support is available for all customers across all plans. No third party is involved and solutions are provided fast for easy implementation. Online chat support is also available for those who are looking for more information about SMTP.com
- **High Volume Sending Solutions:** This newly launched feature is great for those businesses who want to send more than **250 million emails a month**. Customized quotations and solutions are available.
- **Reputation Defender:** This is an add-on feature that helps clean up your email lists. It doesn't need any integration but actively monitors your lists and provides a report.

Pricing

SMTP.com offers affordable delivery services and caters to all kinds of businesses. Their plans range from **$25 to $500 and above**. The best part about this platform is that all the features are available in all the plans. The prices change only based on the volume of emails sent monthly. Even with the lowest price pack, users can get access to **24×7 customer support** and all the SMTP tools. The Reputation Defender for list cleaning is an add-on feature available for all users.

Model of SMTP System

In the SMTP model user deals with the user agent (UA), for example, Microsoft Outlook, Netscape, Mozilla, etc. To exchange the mail using TCP, MTA is used. The user sending the mail doesn't have to deal with MTA as it is the responsibility of the system admin to set up a local MTA. The MTA maintains a small queue of mail so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



SMTP Model

Components of SMTP

- **Mail User Agent (MUA):** It is a computer application that helps you in sending and retrieving mail. It is responsible for creating email messages for transfer to the mail transfer agent(MTA).
- **Mail Submission Agent (MSA):** It is a computer program that receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.
- **Mail Transfer Agent (MTA):** It is software that has the work to transfer mail from one system to another with the help of SMTP.
- **Mail Delivery Agent (MDA):** A mail Delivery agent or Local Delivery Agent is basically a system that helps in the delivery of mail to the local system.

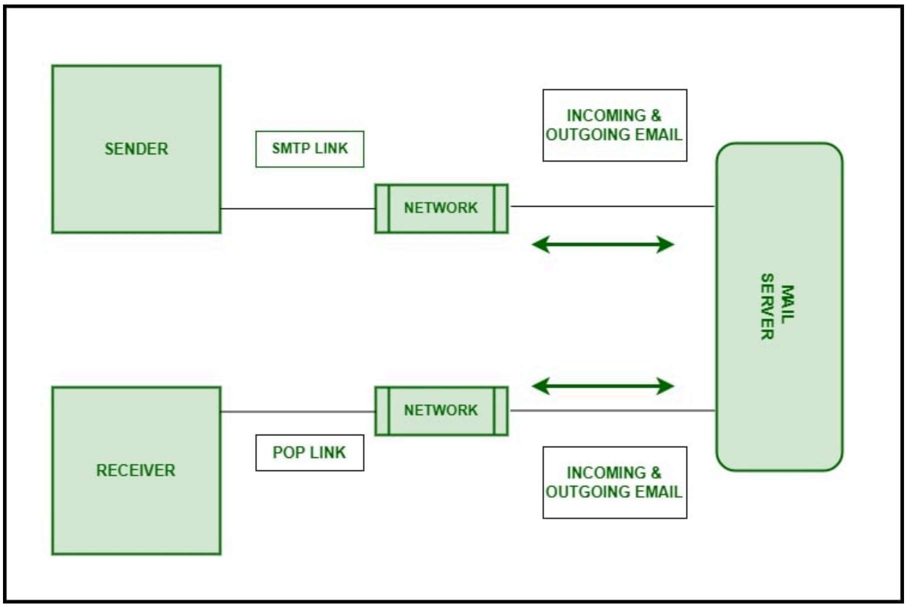
How does SMTP Work?

- **Communication between the sender and the receiver:** The sender's user agent prepares the message and sends it to the MTA. The MTA's responsibility is to transfer the mail across the network to the receiver's MTA. To send mail, a system must have a client MTA, and to receive mail, a system must have a server MTA.
- **Sending Emails:** Mail is sent by a series of request and response messages between the client and the server. The message which is sent across consists of a header and a body. A null line is used to terminate the mail header and everything after the null line is

Open In App

considered the body of the message, which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

- **Receiving Emails:** The user agent on the server-side checks the mailboxes at a particular time of intervals. If any information is received, it informs the user about the mail. When the user tries to read the mail it displays a list of emails with a short description of each mail in the mailbox. By selecting any of the mail users can view its contents on the terminal.



Working of SMTP

What is an SMTP Envelope?

- **Purpose**
    - The SMTP envelope contains information that guides email delivery between servers.
    - It is distinct from the email headers and body and is not visible to the email recipient.
- **Contents of the SMTP Envelope**
    - **Sender Address**: Specifies where the email originates.
    - **Recipient Addresses**: Indicates where the email should be delivered.
    - **Routing Information**: Helps servers determine the path for email delivery.
- **Comparison to Regular Ma**

    - Think of the SMTP envelope as the **address on a physical envelope** for regular mail.
    - Just like an envelope guides postal delivery, the SMTP envelope directs email servers on where to send the email.

What are SMTP Commands?

S.No.	Keywor	Command form	Description	Usage
1.	HELO	HELO<SP><domain><CRLF>	It provides the identification of the sender i.e. the host name.	Mandatory
2.	MAIL	MAIL<SP>FROM : <reverse-path><CRLF>	It specifies the originator of the mail.	Mandatory
3.	RCPT	RCPT<SP>TO : <forward-path><CRLF>	It specifies the recipient of mail.	Mandatory
4.	DATA	DATA<CRLF>	It specifies the beginning of the mail.	Mandatory
5.	QUIT	QUIT<CRLF>	It closes the TCP connection.	Mandatory

S.No.	Keywor	Command form	Description	Usage
6.	RSET	RSET<CRLF>	It aborts the current mail transaction but the TCP connection remains open.	Highly recommended
7.	VRFY	VRFY<SP><string><CRLF>	It is use to confirm or verify the user name.	Highly recommended
8.	NOOP	NOOP<CRLF>	No operation	Highly recommended
9.	TURN	TURN<CRLF>	It reverses the role of sender and receiver.	Seldom used
10.	EXPN	EXPN<SP><string><CRLF>	It specifies the mailing list to be expanded.	Seldom used
11.	HELP	HELP<SP><string><CRLF>	It send some specific documentation to the system.	Seldom used
12.	SEND	SEND<SP>FROM : <reverse-path><CRLF>	It send mail to the terminal.	Seldom used

S.No.	Keywor	Command form	Description	Usage
13.	SOML	SOML<SP>FROM : <reverse-path> <CRLF>	It send mail to the terminal if possible; otherwise to mailbox.	Seldom used
14.	SAML	SAML<SP>FROM : <reverse-path> <CRLF>	It send mail to the terminal and mailbox.	Seldom used

What port does SMTP use?

The **Simple Mail Transfer Protocol (SMTP)** commonly uses **port 587** for **secure transmission** via **TLS**. While **port 465** was previously supported by many providers, it is no longer an accepted standard. Additionally, **port 25** is mainly used for **SMTP relay**, not for SMTP submission. Although **port 2525** is not an official SMTP port, it can serve as a good alternative

Difference Between SMTP and Extended SMTP

SMTP	Extended SMTP
Users were not verified in SMTP as a result of massive-scale scam emails being sent.	In Extended SMTP, authentication of the sender is done.
We cannot attach a Multimedia file in SMTP directly without the help of MMIE.	We can directly attach Multimedia FIle in ESMTP.
We cannot reduce the size of the email in SMTP.	We can reduce the size of the email in Extended SMTP.

SMTP	Extended SMTP
SMTP clients open transmission with the command HELO.	The main identification feature for ESMTP clients is to open a transmission with the command EHLO (Extended HELLO).

Advantages of SMTP

- If necessary, the users can have a dedicated server.
- It allows for bulk mailing.
- Low cost and wide coverage area.
- Offer choices for email tracking.
- Reliable and prompt email delivery.

Disadvantages of SMTP

- SMTP's common port can be blocked by several firewalls.
- SMTP security is a bigger problem.
- Its simplicity restricts how useful it can be.
- Just 7-bit ASCII characters can be used.
- If a message is longer than a certain length, SMTP servers may reject the entire message.
- Delivering your message will typically involve additional back-and-forth processing between servers, which will delay sending and raise the likelihood that it won't be sent.

SMTP vs POP vs IMAP

SMTP	POP	IMAP
Stands for Simple mail transfer protocol	Stands for Post Office Protocol.	Stands for Internet Message Access Protocol.

SMTP	POP	IMAP
Used for sending mail.	Used for retrieving mail.	Used for retrieving mail.
it is push protocol.	it is pull protocol.	it is pull protocol.
It work between sender's mail server to receiver's mail server and sender and sender's mail server.	It work between receiver and receiver's mail server.	It works between receiver and receiver's mail server.
It does not store mail on server it just send the mail.	It download all the mail when it connected to internet.	It store all mail on server and download when it get request to download.
Works on TCP port number 25.	Works on TCP port number 110.	Works on TCP port number 143.
Connection oriented protocol.	Connection oriented protocol.	Connection oriented protocol.
It has persistence TCP connection.	It has persistence TCP connection.	It has persistence TCP connection.
Stateless protocol.	Stateful protocol.	Stateful protocol.
It is in band protocol.	It is in band protocol.	It is in band protocol.
Not used at receiver side.	Used at receiver side.	Used at receiver side.

Conclusion

SMTP is a fundamental part of email communication that allows messages to be reliably transmitted between email servers. Despite its drawbacks, such as security problems and the possibility of spam, SMTP is still widely used due to its simplicity, efficiency, and broad support across various email systems. Enhancements such as encryption and authentication may solve some of its security issues, making it an appropriate choice for email delivery in a variety of applications.

Next Article

Introduction to TELNET

Similar Reads

Presentation Layer Services

The Presentation layer is the 6th layer in the Open System Interconnection (OSI) model. It receives data from the Application layer...

15+ min read

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a widely used protocol for network management that provides a standardized framework for...

15+ min read

Difference Between SMTP and HTTP

A network protocol is an accepted set of rules that govern data communication between different devices in the network. SMTP and...

15+ min read

HTTP Full Form – Hypertext Transfer Protocol

Last Updated : 08 Apr, 2025

HTTP is the primary method through which web browsers and servers communicate to share information on the internet. It was invented by Tim Berners-Lee. HyperText refers to text that is specially coded using a standard coding language called HyperText Markup Language (HTML). HTTP/2 is the updated version of HTTP, while HTTP/3 is the latest version, which was published in 2022.

In this article, we will discuss the Full form of HTTP along with its working, advantages, and disadvantages.

What is the Full Form of HTTP?

HTTP stands for "Hypertext Transfer Protocol." It is a set of rules for sharing data on the World Wide Web (WWW). When you visit a website, HTTP helps your browser request and receive the data needed to display the web pages you see. It is a fundamental part of how the internet works, making it possible for us to browse and interact with websites.

- **Basic Structure**: HTTP forms the foundation of the web, enabling data communication and file sharing.
- **Web Browsing**: Most websites use HTTP, so when you click on a link or download a file, HTTP is at work.
- **Client-Server Model**: HTTP works on a request-response system. Your browser (client) asks for information, and the website's server responds with the data.
- **Application Layer Protocol**: HTTP operates within the Internet Protocol Suite, managing how data is transmitted and received.

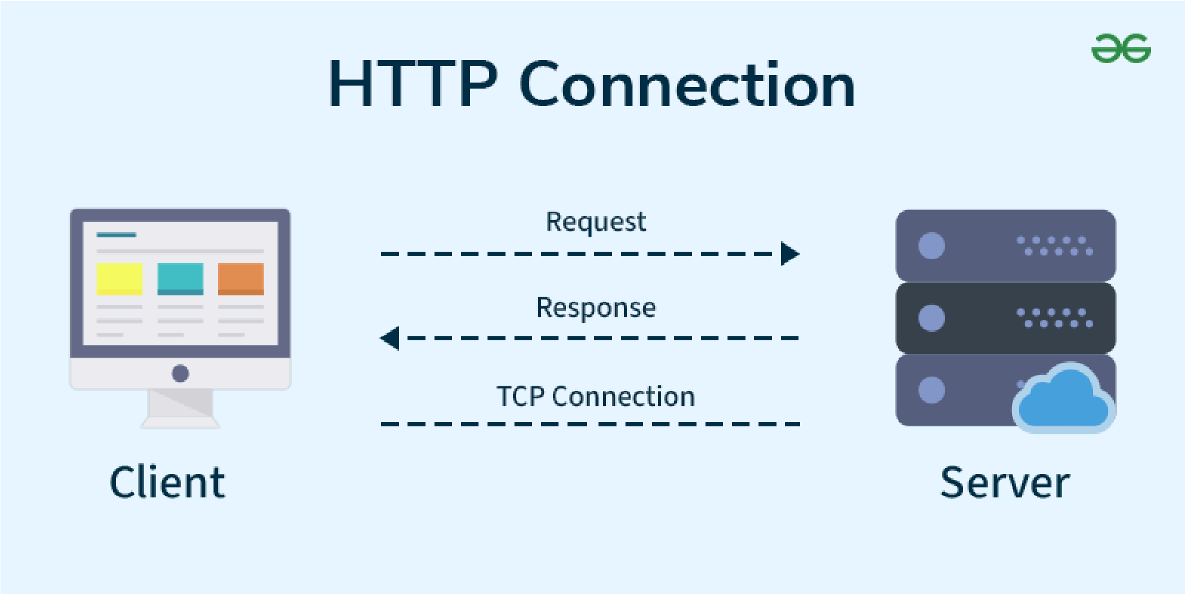
What is HyperText?

The protocol used to transfer hypertext between two computers is known as HyperText Transfer Protocol. HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.

Working of HTTP [HyperText Transfer Protocol]

First of all, whenever we want to open any website, we first open a web browser. after that we will type the URL of that website (e.g., www.facebook.com). This URL is now sent to the Domain Name Server (DNS). Then DNS first checks records for this URL in their database, and then DNS will return the IP address to the web browser corresponding to this URL. Now, the browser can send requests to the actual server.

After the server sends data to the client, the connection will be closed. If we want something else from the server, we should have to re-establish the connection between the client and the server.



Working off HTTPs

What is an HTTP Request?

HTTP request is simply termed as the information or data that is needed by Internet browsers for loading a website. This is simply known as HTTP Request.

There is some common information that is generally present in all HTTP requests. These are mentioned below.

- HTTP Version
- URL
- HTTP Method
- HTTP Request Headers
- HTTP Body

HTTP Request Headers

HTTP Request Headers generally store information in the form of key-value pairs and must be present in each HTTP Request. The use of this Request Header is to provide core information about the client's information, etc.

HTTP Request Body

HTTP Request Body simply contains the information that has to be transferred. HTTP Request has the information or data to be sent to these browsers.

HTTP Method

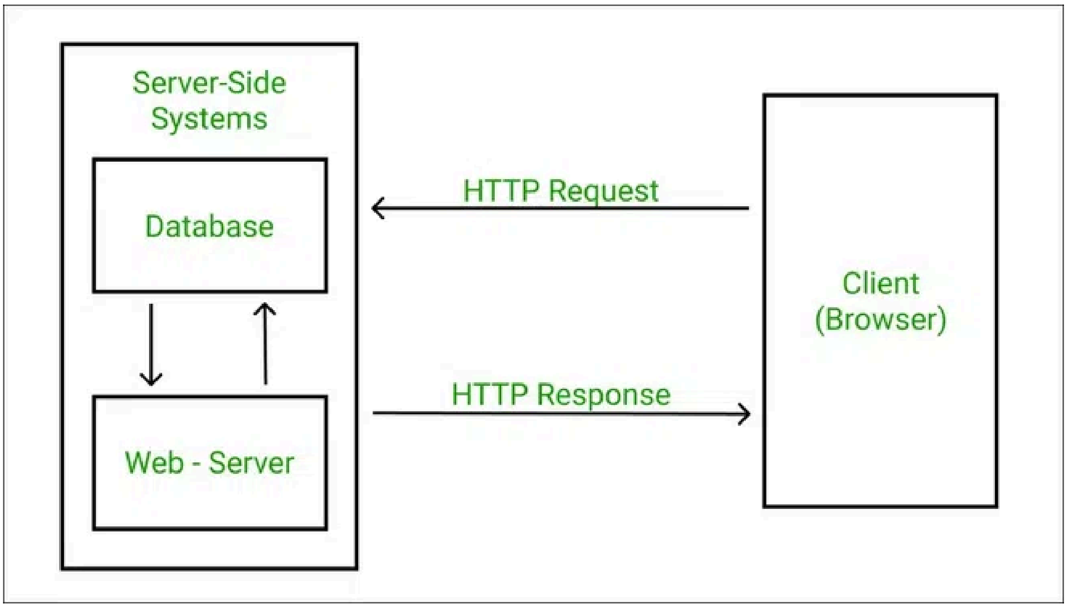
HTTP Methods are simply HTTP Verbs. In spite of being presentin so many HTTP Methods, the most common HTTP Methods are HTTP GET and HTTP POST. These two are generally used in HTTP cases. In HTTP GET, the information is received in the form of a website.

What is HTTP Response?

HTTP Response is simply the answer to what a Server gets when the request is raised. There are various things contained in the HTTP Response, some of them are listed below.

- HTTP Status Code
- HTTP Headers

- HTTP Body



HTTP Response

HTTP Response Headers

HTTP Response headers are simply like an HTTP Request where it has that work to send some important files and data to the HTTP Response Body.

HTTP Response Body

HTTP Responses are the responses that are received successfully upon the request. Generally, it comes under the requests generated by the web. In most cases, the request is to transfer the HTML data into a webpage.

What is an HTTP Status Code?

HTTP Status Codes are the 3-digit codes that tell the message or simply tell us about the HTTP Request whether it has been completed or not. There are simply 5 types of status codes.

- Informational
- Successful
- Re-directional
- Client-Error

- Server-Error

History of HTTP

Tim Berners-Lee and his team at CERN get credit for inventing the original HTTP and associated technologies.

- **HTTP version 0.9:** This was the first version of HTTP, which was introduced in 1991.
- **HTTP version 1.0:** In 1996, RFC 1945 (Request For Comments) was introduced in HTTP version 1.0.
- **HTTP version 1.1:** In January 1997, RFC 2068 was introduced in HTTP version 1.1. Improvements and updates to the HTTP version 1.1 standard were released under RFC 2616 in June 1999.
- **HTTP version 2.0:** The HTTP version 2.0 specification was published as RFC 7540 on May 14, 2015.
- **HTTP version 3.0:** HTTP version 3.0 is based on the previous RFC draft. It is renamed as Hyper-Text Transfer Protocol QUIC which is a transport layer network protocol developed by Google.

Characteristics of HTTP

HTTP is an IP-based communication protocol that is used to deliver data from server to client or vice versa.

- The server processes a request, which is raised by the client, and als, theo server and client know each other only during the current bid and response period.
- Any type of content can be exchanged as long as the server and client are compatible with it.
- Once data is exchanged, servers and clients are no longer connected.
- It is a request and response protocol based on client and server requirements.
- It is a connection-less protocol because after the connection is closed, the server does not remember anything about the client,t and the client does not remember anything about the server.

- It is a stateless protocol because both client and server do not expect anything from each other,r but they are still able to communicate.

Cookies in HTTP

An HTTP cookie (web cookie, browser cookie) is a little piece of data that a server transmits to a user's web browser. When making subsequent queries, the browser may keep the cookie and transmit it back to the same server. An HTTP cookie is typically used, for example, to maintain a user's login state and to determine whether two requests originate from the same browser.Thee stateless HTTP protocol, retains stateful information.

HTTP status code

Three-digit codes, known as HTTP status codes, are most frequently used to show if an HTTP request has been fulfilled successfully. The five blocks below represent the breakdown of status codes:

- 1x Informative
- 2xx Achievement
- 3xx Reorientation
- 4xx Client Mistake
- 5xx Error on the Server

Different numbers between 00 and 99 are denoted by the "xx". Status codes that begin with "2" denote a successful outcome. For instance, the most typical answers sent after a client requests a webpage have a status code of "200 OK," which denotes that the request was successfully fulfilled.

Can DDoS attacks be launched over HTTP?

Remember that because HTTP is a "stateless" protocol, every command executed over it operates independently of every other operation. Each HTTP request opened and terminated a TCP connection according to the original specification. Multiple HTTP requests can now flow over a persistent TCP connection in HTTP 1.1

and later versions of the protocol, which improves resource use. Large-scale HTTP requests are regarded as application layer or layer 7 attacks in the context of DoS or DDoS attacks, and they can be used to mount an attack on a target device.

Advantages of HTTP

- Memory usage and CPU usage are low because of fewer simultaneous connections.
- Since there are few TCP connections, network congestion is less.
- Since handshaking is done at the initial connection stage, latency is reduced because there is no further need for handshaking for subsequent requests.
- The error can be reported without closing the connection.
- HTTP allows HTTP pipe-lining of requests or responses.

Disadvantages of HTTP

- HTTP requires high power to establish communication and transfer data.
- HTTP is less secure because it does not use any encryption method like HTTPS and uses TLS to encrypt regular HTTP requests and responses.
- HTTP is not optimized for cellular phones, and it is too gabby.
- HTTP does not offer a genuine exchange of data because it is less secure.
- The client does not close the connection until it receives complete data from the server; hence, the server needs to wait for data completion and cannot be available for other clients during this time.

Conclusion

In summary, HTTP stands for “Hypertext Transfer Protocol” and is essential for web communication. It enables your browser to request and receive information from websites, making online browsing possible. HTTP is the basic method used by web browsers and servers to communicate and share information on the internet, making it possible for us to browse and interact with websites.

Introduction to TELNET

Last Updated : 24 Jun, 2024

TELNET stands for Teletype Network. It is a **client/server application protocol** that provides access to virtual terminals of remote systems on local area networks or the Internet. The local computer uses a telnet client program and the remote computers use a telnet server program. In this article, we will discuss every point about TELNET.

What is Telnet?

TELNET is a type of protocol that enables one computer to connect to the local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the **local computer**. The computer which is being connected to i.e. which accepts the connection known as the **remote computer**. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle.

History of TELNET

The **Telnet protocol** originated in the late 1960s, it was created to provide remote terminal access and control over mainframes and minicomputers. Initially, it was designed to be a simple and secure method of connecting to a remote system. This protocol allowed users to access remote computers using a terminal or command-line interface. Over time, Telnet's use has diminished due to security concerns, and alternatives like SSH are now preferred for secure remote management

Logging in TELNET

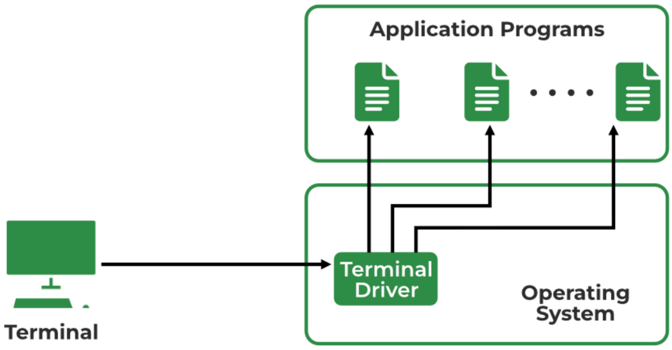
The logging process can be further categorized into two parts:

- Local Login

- Remote Login

1. Local Login

Whenever a user logs into its local system, it is known as local login.



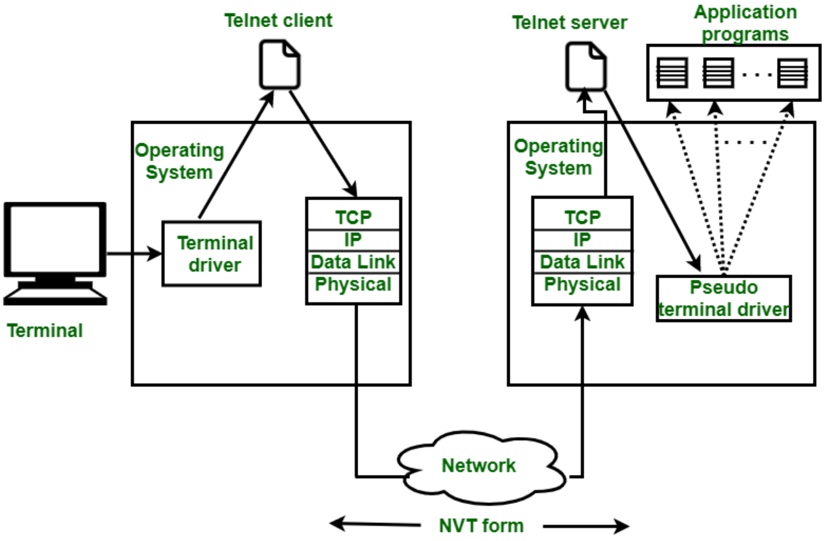
Local Login

The Procedure of Local Login

- Keystrokes are accepted by the terminal driver when the user types at the terminal.
- Terminal Driver passes these characters to OS.
- Now, OS validates the combination of characters and opens the required application.

2. Remote Login

Remote Login is a process in which users can log in to a remote site i.e. computer and use services that are available on the remote computer. With the help of remote login, a user is able to understand the result of transferring the result of processing from the remote computer to the local computer.



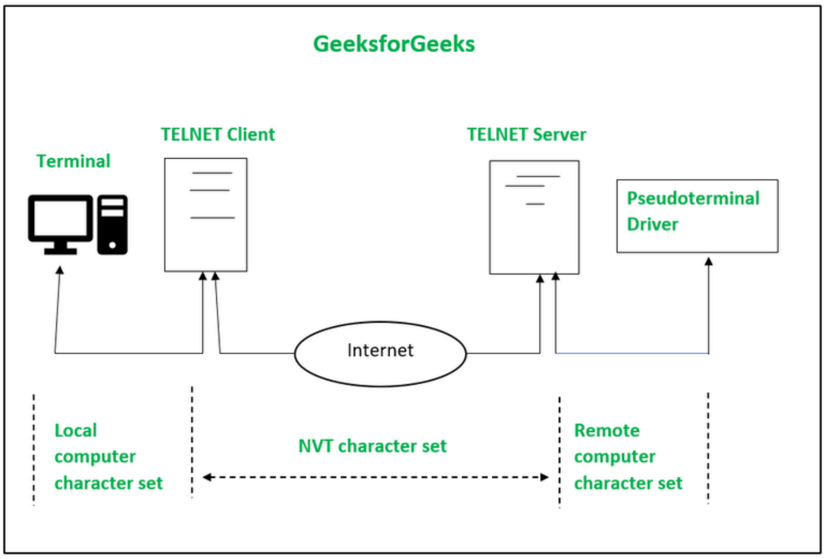
Remote Login in Logging

The Procedure of Remote Login

- When the user types something on the local computer, the local operating system accepts the character.
- The local computer does not interpret the characters, it will send them to the TELNET client.
- TELNET client transforms these characters to a universal character set called Network Virtual Terminal (NVT) characters and it will pass them to the local TCP/IP protocol Stack.
- Commands or text which are in the form of NVT, travel through the Internet and it will arrive at the TCP/IP stack at the remote computer.
- Characters are then delivered to the operating system and later on passed to the TELNET server.
- Then TELNET server changes those characters to characters that can be understandable by a remote computer.
- The remote operating system receives characters from a pseudo-terminal driver, which is a piece of software that pretends that characters are coming from a terminal.
- The operating system then passes the character to the appropriate application program.

Network Virtual Terminal(NVT)

NVT (Network Virtual Terminal) is a virtual terminal in TELNET that has a fundamental structure that is shared by many different types of real terminals. NVT (Network Virtual Terminal) was created to make communication viable between different types of terminals with different operating systems.



Network Virtual Terminal(NVT) in Telnet

How TELNET Works?

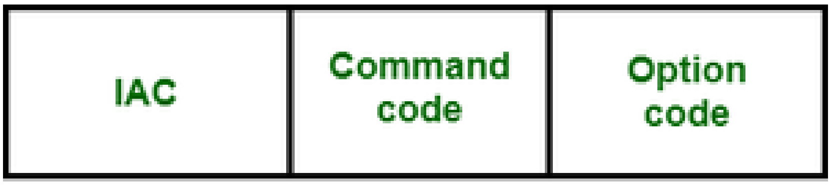
- **Client-Server Interaction**
  - The **Telnet client** initiates the connection by sending requests to the Telnet server.
  - Once the connection is established, the client can send **commands** to the server.
  - The server processes these commands and responds accordingly.
- **Character Flow**
  - When the user types on the **local computer**, the local operating system accepts the characters.
  - The Telnet client transforms these characters into a universal character set called **Network Virtual Terminal (NVT)** characters.
  - These NVT characters travel through the Internet to the remote computer via the local TCP/IP protocol stack.
  - The remote Telnet server converts these characters into a format understandable by the remote computer.
  - The remote operating system receives the characters from a pseudo-terminal driver and passes them to the

appropriate application program[3].

- **Network Virtual Terminal (NVT)**
  - NVT is a virtual terminal in Telnet that provides a common structure shared by different types of real terminals.
  - It ensures communication compatibility between various terminals with different operating systems.

TELNET Commands

Commands of Telnet are identified by a prefix character, Interpret As Command (IAC) with code 255. IAC is followed by command and option codes. The basic format of the command is as shown in the following figure :



IAC	Command code	Option code

TELNET Command Format

Following are some of the important TELNET commands:

Character	Decimal	Binary	Meaning
WILL	251	11111011	1. Offering to enable. 2. Accepting a request to enable.
WON'T	252	11111100	1. Rejecting a request to enable. 2. Offering to disable. 3. Accepting a request to disable.
DO	253	11111101`	1. Approving a request to enable. 2. Requesting to enable.

Character	Decimal	Binary	Meaning
DON'T	254	11111110	1. Disapproving a request to enable. 2. Approving an offer to disable. 3. Requesting to disable.

Following are some common options used with the telnet:

Code	Option	Meaning
0	Binary	It interprets as 8-bit binary transmission.
1	Echo	It will echo the data that is received on one side to the other side.
3	Suppress go ahead	It will suppress go ahead signal after data.
5	Status	It will request the status of TELNET.
6	Timing mark	It defines the timing marks.
8	Line width	It specifies the line width.
9	Page size	It specifies the number of lines on a page.
24	Terminal type	It set the terminal type.
32	Terminal speed	It set the terminal speed.
34	Line mode	It will change to the line mode.

Uses of TELNET

- Remote Administration and Management
- Network Diagnostics
- Understanding Command-Line Interfaces
- Accessing Bulletin Board Systems (BBS)
- Automation and Scripting

Advantages of TELNET

- It provides remote access to someone's computer system.
- Telnet allows the user for more access with fewer problems in data transmission.
- Telnet saves a lot of time.
- The oldest system can be connected to a newer system with telnet having different operating systems.

Disadvantages of TELNET

- As it is somehow complex, it becomes difficult to beginners in understanding.
- Data is sent here in form of plain text, that's why it is not so secured.
- Some capabilities are disabled because of not proper interlinking of the remote and local devices.

Modes of Operation

- **Default Mode:** If no other modes are invoked then this mode is used. Echoing is performed in this mode by the client. In this mode, the user types a character and the client echoes the character on the screen but it does not send it until the whole line is completed.
- **Character Mode:** Each character typed in this mode is sent by the client to the server. A server in this type of mode normally echoes characters back to be displayed on the client's screen.
- **Line Mode:** Line editing like echoing, character erasing, etc. is done from the client side. The client will send the whole line to the server.

Conclusion

Introduction to Blockchain technology | Set 1

Last Updated : 14 May, 2024

Blockchain could be a data structure that could be a growing list of information blocks. The knowledge blocks area unit coupled along, such recent blocks can't be removed or altered. Blockchain is the backbone Technology of the Digital CryptoCurrency BitCoin.

What is Blockchain?

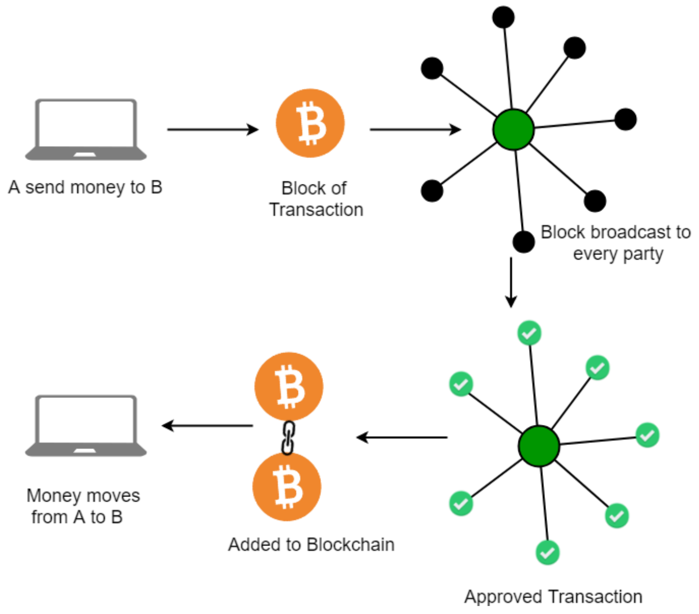
The blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system.

It contains every single record of each transaction. Bitcoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or group of individuals name 'Satoshi Nakamoto' published a white paper on "*BitCoin: A peer-to-peer electronic cash system*" in 2008.

Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction.

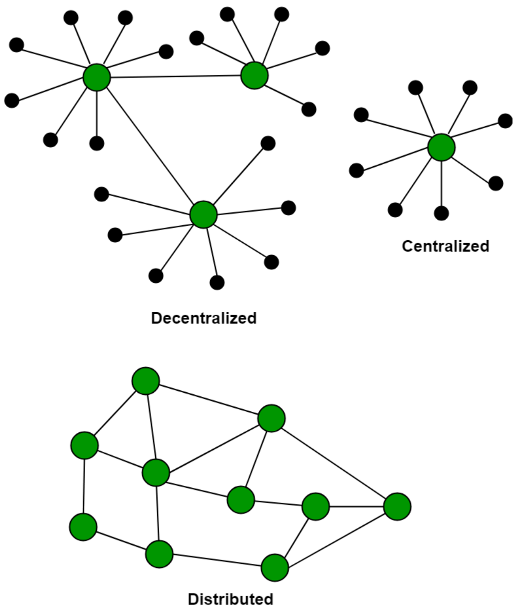
How does Blockchain Technology Work?

One of the famous use of Blockchain is Bitcoin. Bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the Internet. Each transaction protects through a digital signature.



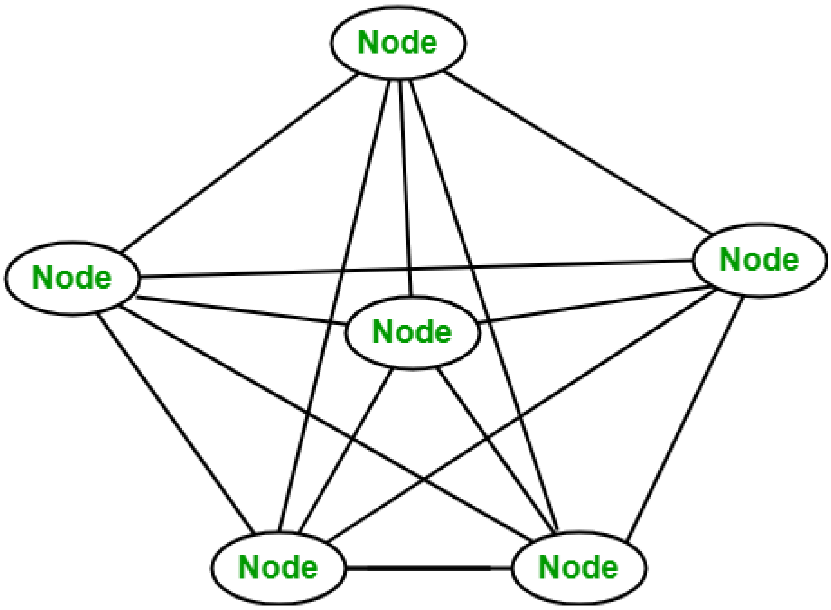
Blockchain Decentralization

There is no Central Server or System which keeps the data of the Blockchain. The data is distributed over Millions of Computers around the world which are connected to the Blockchain. This system allows the Notarization of Data as it is present on every Node and is publicly verifiable.



Blockchain nodes

A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. The client helps in validating and propagating transactions onto the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.



Disadvantages of the current transaction system:

- Cash can only be used in low-amount transactions locally.
- The huge waiting time in the processing of transactions.
- The need for a third party for verification and execution of Transactions makes the process complex.
- If the Central Server like Banks is compromised, the whole system is affected including the participants.
- Organizations doing validation charge high process thus making the process expensive.

Building trust with Blockchain: Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with it's that you don't need to when operating on a Blockchain network. Blockchain builds trust through the following five attributes:

- **Distributed:** The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain.

All this is done in real time as there is no central server controlling the data.

- **Secure:** There is no unauthorized access to Blockchain made possible through Permissions and Cryptography.
- **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.
- **Consensus-based:** All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
- **Flexible:** Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Networks can evolve in pace with business processes.

What are the benefits of Blockchain?

- **Time-saving:** No central Authority verification is needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of the shared ledger.
- **Tighter security:** No one can tamper with Blockchain Data as it is shared among millions of Participants. The system is safe against cybercrimes and Fraud.
- **Collaboration:** It permits every party to interact directly with one another while not requiring third-party negotiation.
- **Reliability:** Blockchain certifies and verifies the identities of every interested party. This removes double records, reducing rates and accelerating transactions.

Application of Blockchain

- Leading Investment Banking Companies like Credit Suisse, JP Morgan Chase, Goldman Sachs, and Citigroup have invested in

Blockchain and are experimenting to improve the banking experience and secure it.

- Following the Banking Sector, the Accountants are following the same path. Accountancy involves extensive data, including financial statements spreadsheets containing lots of personal and institutional data. Therefore, accounting can be layered with blockchain to easily track confidential and sensitive data and reduce human error and fraud. Industry Experts from Deloitte, PwC, KPMG, and EY are proficiently working and using blockchain-based software.
- Booking a Flight requires sensitive data ranging from the passenger's name, credit card numbers, immigration details, identification, destinations, and sometimes even accommodation and travel information. So sensitive data can be secured using blockchain technology. Russian Airlines are working towards the same.
- Various industries, including hotel services, pay a significant amount ranging from 18-22% of their revenue to third-party agencies. Using blockchain, the involvement of the middleman is cut short and allows interaction directly with the consumer ensuring benefits to both parties. Winding Tree works extensively with Lufthansa, AirFrance, AirCanada, and Etihad Airways to cut short third-party operators charging high fees.
- Barclays uses Blockchain to streamline the Know Your Customer (KYC) and Fund Transfer processes while filling patents against these features.
- Visa uses Blockchain to deal with business-to-business payment services.
- Unilever uses Blockchain to track all their transactions in the supply chain and maintain the product's quality at every stage of the process.
- Walmart has been using Blockchain Technology for quite some time to keep track of their food items coming right from farmers to the customer. They let the customer check the product's history right from its origin.

- DHL and Accenture work together to track the origin of medicine until it reaches the consumer.
- Pfizer, an industry leader, has developed a blockchain system to keep track of and manage the inventory of medicines.
- The government of Dubai looking forward to making Dubai the first-ever city to rely on entirely and work using blockchain, even in their government office.
- Along with the above organizations, leading tech companies like Google, Microsoft, Amazon, IBM, Facebook, TCS, Oracle, Samsung, NVIDIA, Accenture, and PayPal, are working on Blockchain extensively.

Is Blockchain Secure?

Nowadays, as the blockchain industry is increasing day by day, a question arises is Blockchain safe? or how safe is blockchain? As we know after a block has been added to the end of the blockchain, previous blocks cannot be changed. If a change in data is tried to be made then it keeps on changing the Hash blocks, but with this change, there will be a rejection as there are no similarities with the previous block.

Just imagine there is a who hacker runs a node on a blockchain network, he wants to alter a blockchain and steal cryptocurrency from everyone else. With a change in the copy, they would have to convince the other nodes that their copy was valid.

They would need to control a majority of the network to do this and insert it at just the right moment. This is known as a 51% attack because you need to control more than 50% of the network to attempt it.

Timing would be everything in this type of attack—by the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter.

Blockchain project ideas

Here are a few project ideas for beginners looking to learn more about blockchain technology:

1. **Cryptocurrency Wallet:** Create a simple cryptocurrency wallet application that allows users to send and receive digital assets.
2. **Blockchain Explorer:** Develop a web-based application that allows users to view and search the transactions on a specific blockchain.
3. **Smart Contract:** Implement a simple smart contract on the Ethereum blockchain that can be used to manage a digital token or asset.
4. **Voting System**: Create a blockchain-based voting system that allows for secure and transparent voting while maintaining voter anonymity.
5. **Supply Chain Management:** Develop a blockchain-based system for tracking the movement of goods and services through a supply chain, providing greater transparency and traceability.
6. **Decentralized marketplace:** Create a decentralized marketplace using blockchain technology where the goods and services can be directly bought by the customers without any intermediary.
7. **Identity Management:** Create a decentralized digital identity management system that allows users to control their personal information and share it securely with others.

These are just a few examples, there are many other possibilities to explore within Blockchain technology.

Future Scope of Blockchain Technology

Finance, supply chain management, and the Internet of Things are just a few of the sectors that blockchain technology has the power to upend (IoT). The following are some potential uses for blockchain in the future:

- Digital Identity: Blockchain-based digital IDs might be used to store personal data safely and securely as well as offer a means of establishing identity without the need for a central authority.
- Smart Contracts: A variety of legal and financial transactions could be automated using smart contracts, self-executing contracts with the terms of the agreement put straight into lines of code.

- Decentralized Finance (DeFi): Using blockchain technology, decentralized financial systems might be built that support peer-to-peer transactions and do away with conventional intermediaries like banks.
- Supply Chain Management: Blockchain technology can be applied to a permanent record of how goods and services have been moved, enabling improved openness and traceability across the whole supply chain.
  -Internet of Things (IoT): Blockchain technology may be used to build decentralized, secure networks for IoT devices, enabling them to exchange data and communicate with one another in an anonymous, safe manner.

In general, blockchain technology is still in its early stages and has a wide range of potential applications.

Advantages of Blockchain Technology:

1. Decentralization: The decentralized nature of blockchain technology eliminates the need for intermediaries, reducing costs and increasing transparency.
2. Security: Transactions on a blockchain are secured through cryptography, making them virtually immune to hacking and fraud.
3. Transparency: Blockchain technology allows all parties in a transaction to have access to the same information, increasing transparency and reducing the potential for disputes.
4. Efficiency: Transactions on a blockchain can be processed quickly and efficiently, reducing the time and cost associated with traditional transactions.
5. Trust: The transparent and secure nature of blockchain technology can help to build trust between parties in a transaction.

Disadvantages of Blockchain Technology:

1. Scalability: The decentralized nature of blockchain technology can make it difficult to scale for large-scale applications.

2. Energy Consumption: The process of mining blockchain transactions requires significant amounts of computing power, which can lead to high energy consumption and environmental concerns.
3. Adoption: While the potential applications of blockchain technology are vast, adoption has been slow due to the technical complexity and lack of understanding of the technology.
4. Regulation: The regulatory framework around blockchain technology is still in its early stages, which can create uncertainty for businesses and investors.
5. Lack of Standards: The lack of standardized protocols and technologies can make it difficult for businesses to integrate blockchain technology into their existing systems.
6. Overall, the advantages of blockchain technology are significant and have the potential to revolutionize many industries. However, there are also several challenges and disadvantages that must be addressed before the technology can reach its full potential.

Comment More info

Advertise with us

Next Article

History of Blockchain

Similar Reads

Introduction to Blockchain technology | Set 2

Blockchain technology has been garnering great hype recently. It gained popularity after the introduction of Bitcoin in 2009 by the person or grou…

15+ min read

Features of Blockchain

Here In this article, we will discuss the features of blockchain technology and how they make it a revolutionary and highly desirable platform for…

15+ min read

Cryptography in Blockchain

Last Updated : 20 Sep, 2022

One of the important questions that always comes to our mind is How blockchain is secure? and What makes blockchain secure? Blockchain security is built on two concepts Cryptography and Hashing. This article focuses on discussing these two important concepts in detail.

Cryptography in Blockchain

Cryptography is a method of securing data from unauthorized access. In the blockchain, cryptography is used to secure transactions taking place between two nodes in a blockchain network. As discussed above, in a blockchain there are two main concepts cryptography and hashing. Cryptography is used to encrypt messages in a P2P network and hashing is used to secure the block information and the link blocks in a blockchain.

Cryptography primarily focuses on ensuring the security of participants, transactions, and safeguards against double-spending. It helps in securing different transactions on the blockchain network. It ensures that only the individuals for whom the transaction data is intended can obtain, read and process the transaction.

Role of Cryptography in Blockchain

Blockchain is developed with a range of different cryptography concepts. The development of cryptography technology promotes restrictions for the further development of blockchain.

- In the blockchain, cryptography is mainly used to protect user privacy and transaction information and ensure data consistency.

- The core technologies of cryptography include symmetric encryption and asymmetric encryption.
- Asymmetric cryptography uses digital signatures for verification purposes, every transaction recorded to the block is signed by the sender by digital signature and ensures that the data is not corrupted.

Cryptography plays a key role in keeping the public network secure, so making it fit to maintain the integrity and security of blockchain.

Cryptography

Cryptography is a technique or a set of protocols that secure information from any third party during a process of communication. It is also made up of two Greek terms, Kryptos term meaning “hidden” and Graphein, a term meaning “to write”. Some terminologies related to Cryptography:

- **Encryption:** Conversion of normal text to a random sequence of bits.
- **Key:** Some amount of information is required to get the information of the cryptographic algorithm.
- **Decryption:** The inverse process of encryption, conversion of a Random sequence of bits to plaintext.
- **Cipher:** The mathematical function, i.e. a cryptographic algorithm which is used to convert plaintext to ciphertext(Random sequence of bits).

Types of Cryptography

The two types of cryptography are:

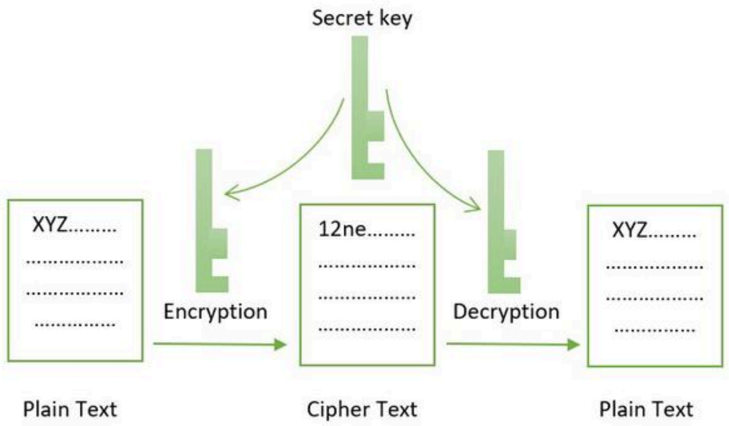
- **Symmetric-key cryptography.**
- **Asymmetric-key cryptography.**

Let’s discuss each of these topics in detail.

1. Symmetric-key Encryption: It focuses on a similar key for encryption as well as decryption. Most i the symmetric key encryption method is also applicable to secure website connections or encryption of data. It is also referred to as secret-key cryptography. The only problem is that the sender and receiver exchange keys in a secure manner. The popular symmetric-key cryptography system is Data Encryption System(DES). The cryptographic algorithm utilizes the key in a cipher to encrypt the data and the data must be accessed. A person entrusted with the secret key can decrypt the data. Examples: AES, DES, etc.

Features:

- It is also known as Secret key cryptography.
- Both parties have the same key to keeping secrets.
- It is suited for bulk encryptions.
- It requires less computational power and faster transfer.



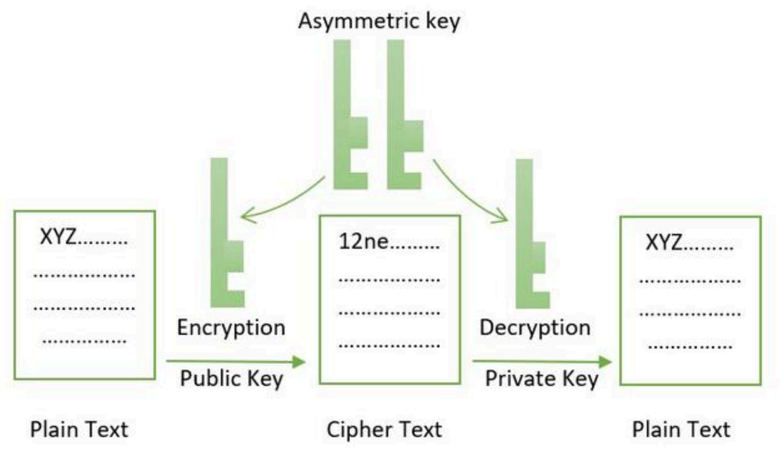
Symmetric Cryptography

2. **Asymmetric-key Encryption:** This cryptographic method uses different keys for the encryption and decryption process. This encryption method uses public and private key methods. This public key method help completely unknown parties to share information between them like email id. private key helps to decrypt the messages and it also helps in the verification of the digital signature. The mathematical relation between the keys is that the private key cannot be derived from the public key, but the public key can be derived from the private key. **Example:** ECC,DSS etc.

Features:

Open In App

- It is also known as Public-key cryptography.
- It is often used for sharing secret keys of symmetric cryptography.
- It requires a long processing time for execution.
- Plays a significant role in website server authenticity.



Asymmetric Cryptography

Wallets And Digital Signatures

A blockchain wallet is a special software or a hardware device that is used to keep the transaction information and personal information of the user. Blockchain wallets do not contain the actual currency. The wallets are used to keep private keys and maintain a transaction balance.
Wallets are only a communication tool to communicate to carry out transactions with other users. The real data or currency is stored in blocks in the blockchain.

Digital signatures are like proofs that the user gives to the recipient and other nodes in the network to prove that it is a legitimate node in the network to carry out transactions. While initiating a transaction with other nodes in the blockchain network, the user first has to create a unique digital signature by combining the transaction data with the user’s private key using a special algorithm. This process will guarantee the authenticity of the node and the integrity of the data.

Cryptography Hash Function in Blockchain

One of the most notable uses of cryptography is cryptographic hashing. Hashing enables immutability in the blockchain. The encryption in cryptographic hashing does not involve any use of keys. When a transaction is verified hash algorithm adds the hash to the block, and a new unique hash is added to the block from the original transaction. Hashing continues to combine or make new hashes, but the original footprint is still accessible. The single combined hash is called the root hash. Hash Function helps in linking the block as well as maintaining the integrity of data inside the block and any alteration in the block data leads to a break of the blockchain. Some commonly used hashed function is MD5 and SHA-1.

Properties of Cryptographic Hash:

- For a particular message hash function does not change.
- Every minor change in data will result in a change in a major change in the hash value.
- The input value cannot be guessed from the output hash function.
- They are fast and efficient as they largely rely on bitwise operations.

Benefits of Hash function in Blockchain:

1. Reduce the bandwidth of the transaction.
2. Prevent the modification in the data block.
3. Make verification of the transaction easier.

Use of Cryptographic Hash Functions

As the blockchain is also public to everyone it is important to secure data in the blockchain and keeps the data of the user safe from malicious hands. So, this can be achieved easily by cryptography.

- When the transaction is verified through a hash algorithm, it is added to the blockchain, and as the transaction becomes confirmed it is added to the network making a chain of blocks.
- Cryptography uses mathematical codes, it ensures the users to whom the data is intended can obtain it for reading and processing the transaction.

- Many new tools related to the application of cryptography in blockchain have emerged over the years with diverse functionalities.

Benefits of Cryptography in Blockchain

There are a huge number of benefits of cryptography in blockchain some of them are stated below:

- **Encryption:** Cryptography uses asymmetric encryption to ensure that the transaction on their network guards the information and communication against unauthorized revelation and access to information.
- **Immutability:** This feature of cryptography makes it important for blockchain and makes it possible for blocks to get securely linked by other blocks and also to ensure the reliability of data stored in the blockchain, it also ensures that no attacker can derive a valid signature for unposed queries from previous queries and their corresponding signatures.
- **Security:** Cryptography makes the records of transactions easier using encryption of data, and accessing of data using public and private keys. Cryptographic hashing tampering with data is not possible, making blockchain more secure.
- **Scalability:** Cryptography makes the transaction irreversible giving the assurance that all users can rely on the accuracy of the digital ledger. It allows limitless transactions to be recorded securely in the network.
- **Non-repudiation:** The digital signature provides the non-repudiation service to guard against any denial of a message passed by the sender. This benefit can be associated with collision resistance i.e.; since every input value has a unique hash function so there is no clash between the messages that are sent and one message can be easily differentiated from the other.
- **Prevent hackers:** The digital signature prevents hackers from altering the data because if the data changes, the digital signature becomes invalid. With the help of cryptography, it protects the data from hackers and makes cryptography in blockchain unstoppable.

Limitations of Cryptography in Blockchain

Below are some of the limitations of cryptography in the blockchain:

- **Information difficult to access:** Strongly encrypted and digitally signed information can be difficult to access even for a legitimate user at the most critical time of decision-making. The network can be attacked and rendered non-functional by an intruder.
- **High availability:** It is one of the fundamental aspects of information security, and cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of the information systems.
- **No protection against vulnerabilities:** Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of protocols, procedures, and systems. These issues need to be fixed with the proper design of the defense infrastructure.
- **Expensive:** Cryptography needs huge time and money investments. Public key cryptography needs setting up and maintenance of public key infrastructure which requires huge investment. Addition of cryptographic techniques while sending messages and information processing adds to the delay.
- **Vulnerability:** The security of cryptographic techniques depends on the complexity and difficulty of the mathematical problem. Any breakthrough in solving such mathematical problems can make cryptographic techniques vulnerable.

Comment More info

Advertise with us

Next Article

Hot Wallets vs Cold Wallets in Blockchain

Similar Reads

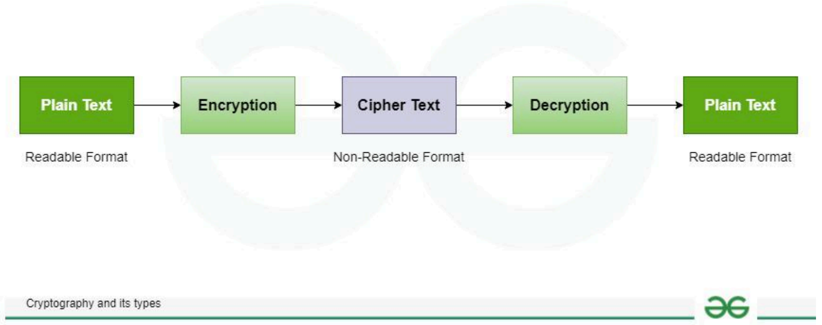
Blockchain - Private Key Cryptography

Open In App

Cryptography and its Types

Last Updated : 05 Feb, 2025

Cryptography is a technique of securing information and communications through the use of codes so that only those persons for whom the information is intended can understand and process it. Thus, preventing unauthorized access to information. The prefix “crypt” means “hidden” and the suffix “graphy” means “writing”. In Cryptography, the techniques that are used 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 them. These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.



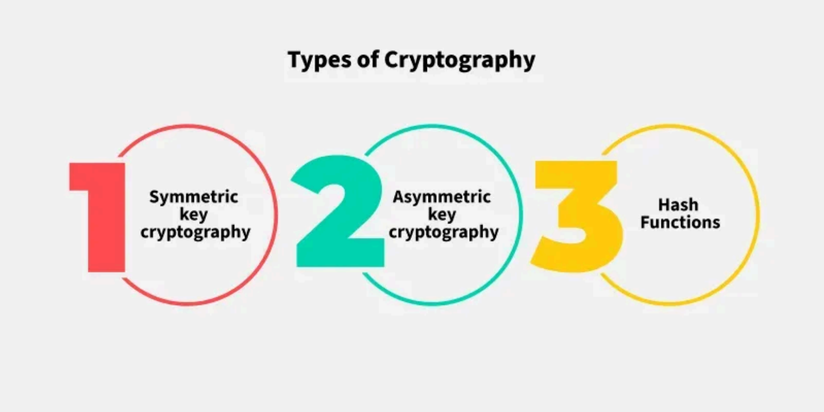
Features Of Cryptography

- **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at a later stage.

Open In App

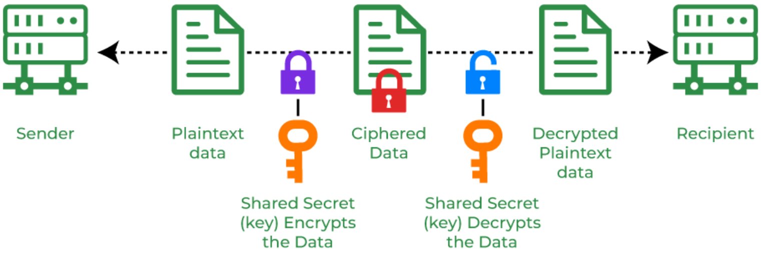
- **Authentication:** The identities of the sender and receiver are confirmed. As well destination/origin of the information is confirmed.
- **Interoperability:** Cryptography allows for secure communication between different systems and platforms.
- **Adaptability:** Cryptography continuously evolves to stay ahead of security threats and technological advancements.

Types Of Cryptography



1. Symmetric Key Cryptography

It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric Key cryptography is faster and simpler but the problem is that the sender and receiver have to somehow exchange keys securely. The most popular symmetric key cryptography systems are Data Encryption Systems (DES) and Advanced Encryption Systems (AES) .


Sender
Plaintext data
Ciphered Data
Decrypted Plaintext data
Recipient
Shared Secret (key) Encrypts the Data
Shared Secret (key) Decrypts the Data

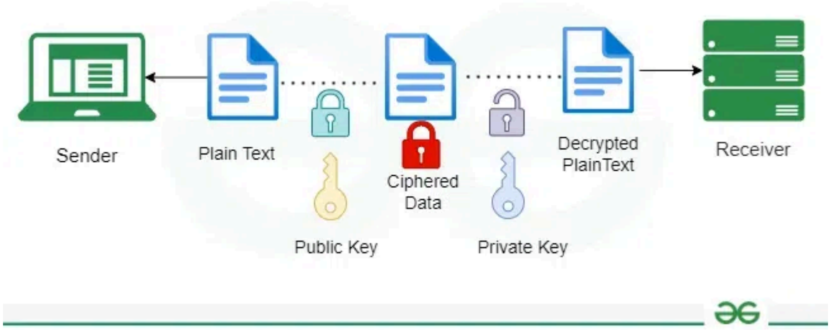
Symmetric Key Cryptography

2. Hash Functions

There is no usage of any key in this algorithm. A hash value with a fixed length is calculated as per the plain text which makes it impossible for the contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. Asymmetric Key Cryptography

In Asymmetric Key Cryptography, a pair of keys is used to encrypt and decrypt information. A sender's public key is used for encryption and a receiver's private key is used for decryption. Public keys and Private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows his private key. The most popular asymmetric key cryptography algorithm is the RSA algorithm.



Asymmetric Key Cryptography

Applications of Cryptography

- **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.

- **Digital Currencies:** To protect 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.

- **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.

- **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.

- **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.

- **Cryptocurrencies:** Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum to protect 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.

- **End-to-end Internet 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.

Types of Cryptography Algorithm

- **Advanced Encryption Standard (AES):** AES (Advanced Encryption Standard) is a popular encryption algorithm which uses the same key for encryption and decryption It is a symmetric block cipher algorithm with block size of 128 bits, 192 bits or 256 bits. AES algorithm is widely regarded as the replacement of DES (Data encryption standard) algorithm.

- **Data Encryption Standard (DES):** DES (Data encryption standard) is an older encryption algorithm that is used to convert 64-bit plaintext data into 48-bit encrypted ciphertext. It uses symmetric keys (which means same key for encryption and decryption). It is kind of old by today's standard but can be used as a basic building block for learning newer encryption algorithms.

- **RSA:** RSA is an basic asymmetric cryptographic algorithm which uses two different keys for encryption. The RSA algorithm works on a block cipher concept that converts plain text into cipher text and vice versa.

- **Secure Hash Algorithm (SHA):** SHA is used to generate unique fixed-length digital fingerprints of input data known as hashes**.** SHA variations such as **SHA-2** and **SHA-3** are commonly used to ensure data integrity and authenticity. The tiniest change in input data drastically modifies the hash output, indicating a loss of integrity. Hashing is the process of storing key value pairs with the help of a hash function into a hash table.

Advantages of Cryptography

- Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource.
- For secure online communication, it offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the Internet.

- It helps in the defense against various types of assaults including replay and man-in-the-middle attacks.
- Cryptography can help firms in meeting a variety of legal requirements including data protection and privacy legislation.

Comment More info

Advertise with us

Next Article

Cryptography and Network Security Principles

Similar Reads

Cryptography and Network Security Principles

In the present-day scenario security of the system is the sole priority of any organization. The main aim of any organization is to protect their...

15+ min read

Basics of Cryptographic Algorithms

Cryptography is a process of hiding transmitted information by the sender such that it may be read only by the intended recipient. In this article, we...

15+ min read

Cryptanalysis and Types of Attacks

Cryptology has two parts namely, Cryptography which focuses on creating secret codes and Cryptanalysis which is the study of the...

15+ min read

Public Key Encryption

Public key cryptography provides a secure way to exchange information and authenticate users by using pairs of keys. The public key is used for...

15+ min read

Open In App