# HTTP(Hyper Text Transfer Protocol)

Http is a application layer protocol which is underlying protocol under World Wide Web(WWW).It is a request-response protocol. This protocol is used to define how messages are formatted and transmitted and what actions web servers and browsers should take in response to various commands.

For example when you enter an URL in your bowser this actually sends an HTTP command to Web Server directing it to fetch and transmit the requested Web Page.The webpages which are displayed as per the request they can be controlled by HTML.

HTTP is a stateless protocol because each command is executed independently with any knowledge of the commands that came before it. The shortcoming of HTTP coming in various technologies such as JavaScript,Java and cookies.

HTTP Request Methods:

HTTP requests methods to indicate the desired action to be performed on the identified resource.What this resource represents, Whether pre-existing data or data that is generated automatically,depends on implementation of the server. Some of the methods include GET,HEAD,POST,PUT,TRACE,CONNECT etc..

**1.GET:**

The GET method requests for a resource.Requests using GET Should only be used to retrieve data but has no other effect.

**2.HEAD:**

The HEAD method asks for a response like GET method,but does not contain any body.

**3.POST:**

The POST method requests the server to store the information that needed to be added extra to the server.

**4.DELETE:**

The DELETE method delete the specified resource.

**5.TRACE:**

The TRACE method echoes the received request so that the client can see what actions or changes or additions done by intermediate servers.

**6.CONNECT**:

It is used to establish a connection for the TCP/IP connection.

**HTTP error messages:**

Error messages are the status codes which are generated as response codes given by web servers and help identify the cause of the problem.

1.Informational 100

2.Successful 200

3.Redirection 300

4.Client Error 400

5.Server Error 500

**HTTPS**

It is an extension of HTTP protocol for a secure communication on a computer network which is widely used on the Internet.

The principal motivation for HTTPS is authentication of the accessed website and protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks. The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication In practice, this provides a reasonable assurance that one is communicating without interference by attackers with the website that one intended to communicate with, as opposed to an impostor.

Historically, HTTPS connections were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems. HTTPS is used more often by webusers than the original non-secure HTTP, primarily to protect page authenticity on all types of websites; secure accounts; and keep user communications, identity, and web browsing private.

The Uniform Resource Identifier (URI) scheme HTTPS has identical usage syntax to the HTTP scheme. However, HTTPS signals the browser to use an added encryption layer of SSL/TLS to protect the traffic. SSL/TLS is especially suited for HTTP, since it can provide some protection even if only one side of the communication is authenticated. This is the case with HTTP transactions over the Internet, where typically only the server is authenticated .

We use several cryptographic algorithms for the security and the protection based on the usage.But depends on implementation on both server side and client side.

**Difference between HTTP and HTTPS:**

HTTPS URLs begin with "https://" and use port 443 by default, whereas HTTP URLs begin with "http://" and use port 80 by default.

HTTP is not encrypted and is vulnerable to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information, and modify webpages to inject malware or advertisements. HTTPS is designed to withstand such attacks and is considered secure against them (with the exception of older, deprecated versions of SSL).