HTTP(S)

HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) are **the primary protocols used for communication between web browsers and servers**, commonly operating **over ports 80 and 443**, respectively.

HTTP (Port 80)

- HTTP is the foundation of data communication on the web. It is a **stateless**, application-layer protocol used to transfer hypertext (such as HTML) from web servers to web browsers.
- **Port 80 is the default port** for HTTP traffic. When a user accesses a website without specifying HTTPS, the browser communicates with the server over port 80, and the data is **transmitted in plaintext**. This means that any information sent, including personal data or passwords, is not encrypted and can be intercepted by attackers.

HTTPS (Port 443)

- HTTPS is **the secure version of HTTP**. It combines HTTP with TLS (Transport Layer Security) or SSL (Secure Sockets Layer) encryption to protect the data being transmitted.
- **Port 443 is the default port** for HTTPS traffic. When a user accesses a website over HTTPS, the browser and server establish a secure, encrypted connection using TLS. This ensures that the data exchanged between the browser and server cannot be easily intercepted or tampered with, **providing confidentiality and integrity**.
- HTTPS is widely used for secure online transactions, including banking, shopping, and any website that handles sensitive information.

Key Differences:

- HTTP (Port 80): Unencrypted communication, vulnerable to eavesdropping and man-in-the-middle attacks.
- HTTPS (Port 443): Encrypted communication, protecting data from interception and ensuring secure transmission.

Summary

HTTP (port 80) is used for non-secure communication, while HTTPS (port 443) provides a secure channel by encrypting the data.