How HTTPS improves security over HTTP

Compared to HTTP (HyperText Transfer Protocol), HTTPS (HyperText Transfer Protocol Secure) greatly improves the security of data transferred over the internet. The main distinction is that HTTPS protects the data sent between a web server and a user's browser by using encryption.

Protocols like TLS (Transport Layer Security) are used to encrypt data when a user connects to a website via HTTPS. This encryption makes sure that the data cannot be read by unauthorized persons, even if it is intercepted during transit. This is essential for protecting sensitive data, including login credentials, payment information, and personal information.

Digital certificates from reliable Certificate Authorities (CAs) are another way that HTTPS offers authentication. This procedure reduces the danger of phishing and man-in-the-middle (MITM) attacks by confirming that users are interacting with the intended website.

Additionally, data integrity is supported by HTTPS, guaranteeing that sent and received data cannot be changed or manipulated covertly. HTTPS provides a secure surfing experience by safeguarding data confidentiality, authenticity, and integrity, which builds user confidence and promotes safe online interactions. Consequently, any website that handles sensitive data must make the switch from HTTP to HTTPS.