**BLOG WRITING**

**HTTPS**

HTTPS (Hypertext Transfer Protocol Secure) is a secure protocol that helps protect the integrity and privacy of data exchanged between web servers and browsers. It is the most widely used protocol for securing websites, ensuring that all communication between the server and the browser is encrypted. HTTPS also offers authentication, which helps protect against the malicious activity such as phishing attacks. By using HTTPS, website owners can ensure that their visitors' data is kept safe and secure.

It works by encrypting the data sent between the two parties, thus preventing any malicious third-party from intercepting or tampering with the data. HTTPS also ensures that the client is connected to the intended server and not a malicious one. This is done through a process called SSL/TLS certificate validation which verifies that the server has been issued a valid certificate by a trusted Certificate Authority. With HTTPS, users can be sure that their data remains safe and secure while being transmitted across the internet.

**HTTP**

HTTP (Hypertext Transfer Protocol) is one of the most widely used protocols on the internet. It is a communication protocol that allows for the transfer of data between web servers and clients. HTTP is used by web browsers to request and display web pages, as well as by applications that need to communicate with other applications over the internet. HTTP has been around since 1989 and is still in use today, making it one of the oldest protocols in use on the internet. It has enabled a variety of different applications, from simple websites to complex distributed systems, and has become an essential part of our everyday lives. With its importance only increasing over time, understanding how HTTP works will be an important skill for anyone who wants to work with or develop for the web.

It is a request-response protocol that enables a client to send a request to the server and receive a response back. HTTP works by sending requests from the client side to the server side, and then sending responses back. These requests can include information like what type of resource is being requested, what type of data format should be used for the response, and other details. By understanding how HTTP works, it becomes easier to build websites that are more efficient and secure.

**API**

APIs (Application Programming Interfaces) are a set of instructions that allow applications to communicate with each other. They are used to connect different systems, databases, and services together in order to create powerful applications. APIs allow developers to access data and services from third-party sources in order to build new applications or extend existing ones.

API calls are requests sent by an application or website to a server in order to retrieve data or perform an action. The server then responds with the requested information in the form of JSON (JavaScript Object Notation) objects, which can be used by the application for further processing.

In summary, APIs provide a simple way for developers to access data and services from third-party sources without having to write code from scratch. This allows them to quickly build powerful applications that can be integrated with existing systems and databases.

**HOW ARE APIs RELATED TO HTTPS**

APIs (Application Programming Interfaces) are essential for modern web development, as they allow developers to create applications that interact with other services. APIs use the HTTPS protocol to securely communicate between services, allowing data to be exchanged quickly and securely. This is especially important when dealing with sensitive information, such as user data or financial transactions. By using HTTPS, developers can ensure that their communication is secure and that no malicious actors can intercept or modify the data being transferred. APIs are thus vital for creating secure web applications and services, and the use of HTTPS is an integral part of this process.