Token in Authentication

For authentication, a token is a piece of data that represents the user's credentials. It is used to verify the identity of a user or a device trying to access a resource.
Tokens are often used in stateless authentication systems, where the server does not maintain session information about the user between requests.

There are multiple types of tokens - refresh tokens, ID tokens, access tokens etc.

How are they used in the authentication flow?
Step 1: The user provides their credentials (e.g., username and password) to authenticate with the server.

Step 2: Upon successful authentication, the server generates a token and sends it back to the client.

Step 3: The client stores the token, typically in local storage or a cookie.

Step 4: For subsequent requests, the client includes the token in the HTTP headers (usually in the Authorization header) to access protected resources.

Step 5: The server verifies the token to check if the request is authenticated and authorized.

A well known example of this is **JWT** Token (JSON Web Token) : Read More
They are a compact, URL-safe token format that consists of three parts: header, payload, and signature. JWTs are widely used for stateless authentication and are easy to parse and validate.