JSON Web Tokens (JWT)

A JSON Web Token (JWT) is a JSON object which is used to securely transfer information over the web (between two parties). It can be used for an authentication system and can also be used for information exchange.

It is composed of three parts:

- A header
- A payload
- A signature

A header typically contains the type of the token, and the signing algorithm used.

The payload contains the data being transmitted, such as the user's ID or email address.

The signature is created by hashing the header and payload using a secret key, which can be used to verify the authenticity of the token.

Cookies

Cookies in simpler terms means just the textual information about some website.

They are commonly used to store user preferences, shopping cart items and session data. Cookies can also be used for authentication and authorization.

Cookies can be either session cookies or persistent cookies. Session cookies are stored in memory and are deleted when the user closes their browser.

Persistent cookies are stored on the users computer and are not deleted when the user closes their browser.

Authentication

Authentication is a term that refers to the process of proving the identity of the computer system is genuine.

Authorization

Authorization is the function of specifying access right to resources, which is related to general information security and computer security, and to access control in particular.

NOTE: Mostly, above concepts are based on implementation.