

JWT:

JSON Web Token (JWT) is an open standard used to exchange data securely between parties. It consists of three parts: Header, Payload, and Signature.

How it Works

1. The server generates a JWT after verifying the user's identity.
2. The token is sent to the client for storage.
3. The token is included in each request to verify permissions.

This token has all the info the server needs to identify the user. Every time you make a request, you show the token instead of logging in again.

Components

Header: Contains the token type and the encryption algorithm.

Payload: User data or claims.

Signature: Ensures data integrity and verification.

Advantages

Secure: Based on encryption.

Lightweight: Transferred in the request header.

Stateless: Does not require the server to store session data.

Name: Bayan Sameer Basrana.