(JWT) Json Web Tokens

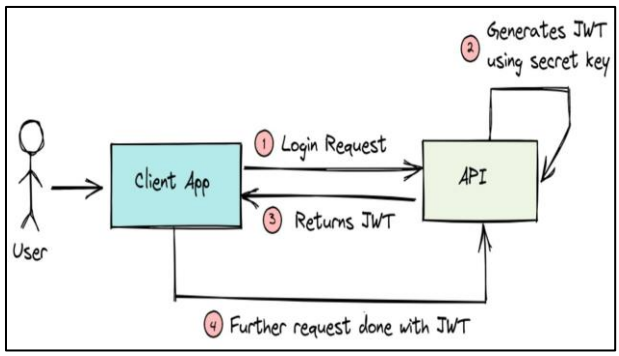
What is JWT?

JWT (JSON Web Token) is an open standard, used to securely share data between a client and server without storing sessions on the server.

A JWT has three Base64-encoded parts separated by dots:

1. Header: Contains the token type (JWT) and signing algorithm (e.g., RS256).
2. Payload: Contains user information like user ID and roles.
3. Signature: Ensures data integrity, created using the Header, Payload, and a secret key.

How JWT Works?



Advantages of JWT:

1. Stateless: No need to store session data on the server.
2. High Performance: No database lookup for session validation.
3. Compact and Portable: Suitable for modern applications like REST APIs.
4. Scalable: Ideal for distributed systems (e.g., Microservices).

Disadvantages of JWT:

1. Not Encrypted: Token data can be read if intercepted, so sensitive data should not be included.
2. Difficult to Revoke: Tokens cannot be invalidated after issuance without additional mechanisms.
3. Security Risks: If stolen, the token can be used until expiration.

Comparison Between JWT and HTTP Basic Authentication:

Feature	JWT	HTTP Basic Authentication
State Management	Stateless; no server-side storage needed.	(stateful) Server stores session data.
Data Transmission	Sends the token only.	Sends username/password with every request.
Security	Uses digital signatures for integrity.	Relies heavily on HTTPS.
Features	Supports expiration, roles, and permissions.	Simple authentication.
Performance	Lightweight and faster.	Session lookup is required.
Scalability	Excellent scalability for distributed systems.	Limited scalability due to session storage.