**4. Spring Security**

**Token-Based Authentication (JWT):**

• **Theory:**

**1.Introduction to token-based authentication using JSON Web Tokens (JWT):-** JWT (JSON Web Token) is a secure way to authenticate users without storing session data on the server. Instead, a token is issued after login and sent with each request to verify the user.

**2.Explanation of the authentication process: token generation, validation, and secure access to protected resources:-**

**Authentication Process Using JWT**

1️.User Logs In

* Sends username & password to the server.

2️.oken Generation

* If credentials are valid, the server creates a JWT (JSON Web Token) containing user details and expiration time.
* The token is sent back to the user.

3️.Token Storage

* The user stores the JWT (usually in localStorage or HTTP cookies).

4️.Accessing Protected Resources

* For each request, the JWT is sent in the Authorization header (Bearer Token).

Authorization: Bearer <JWT\_TOKEN>

5️.Token Validation

* The server verifies the token’s signature & expiration before granting access.

6️.Secure Access to Resources

* If the token is valid, the request is allowed; otherwise, the server returns 401 Unauthorized.