What is JWT?

- **JWT** (JSON Web Token) is an open standard used for securely transmitting information between two parties (such as a client and a server) in the form of a signed token.

Why is JWT used?

1. **Authentication**: To verify the user's identity after login.
2. **Authorization**: To define the user's roles or permissions.
3. **Data Security**: Ensures data integrity and prevents tampering.

How does JWT work?

1. The server generates a token upon user login and signs it using a secret key.
2. The token is sent to the client.
3. The client includes the token with every subsequent request for validation.

Components of JWT:

1. **Header**: Contains the token type and the signing algorithm.
2. **Payload**: Holds the claims (e.g., user ID, roles).
3. **Signature**: Ensures the token's integrity and authenticity.

Key Advantages of JWT:

1. **Stateless**: The server does not need to store the token.
2. **Secure**: The signature ensures data integrity.
3. **Easily Verifiable**: Tokens can be validated using the secret or public key.

Potential Drawbacks:

1. **Revocation**: Tokens cannot be easily revoked after issuance.
2. **Size**: Tokens can be relatively large compared to cookies.