JWT (JSON Web Token)

Mshari Alshammari

JWT (JSON Web Token)

JWT is a secure way to transfer information between two parties, like a digital ID card.

It is composed of three parts:

- Header: Defines the token type and algorithm.
- Payload: Stores user data.
- Signature: Confirms the token is valid and untampered.

How it Works

1. User logs in with credentials.
2. Server validates the input.
3. A JWT is generated with user details.
4. Token is sent back to the user.
5. User attaches token to each request.
6. Server reads token to identify the user.

Advantages

- No need for server storage.
- Lightweight and fast to transmit.
- Works with any programming language.

- Digital signature ensures security.

Limitations

- Tokens can’t be revoked instantly.
- Can grow large if overloaded with data.
- Requires proper handling to stay safe.

Conclusion

JWT provides a modern and efficient way to handle authentication in web and mobile apps.

It is simple, fast, and secure, making it a popular choice despite a few limitations.