JSON web tokens- open standard to pass data between client and server.
JSON web tokens enable you to transmit data back and forth b/w server and consumer in a secure manner.
JWT is represented as a combination of three base64URL encoded parts concatenated with period(.) characters.
Header, payload, signature

Header- provides metadata about type of data and algorithm to be used to encrypt data that is to be transferred. Header comprises 2 sections- Type of token, encryption algorithm.
{ “type”: “jwt”, “alg”: “HS256” }
Payload- represents actual info in JSON format that is to be transferred. Payload contains claims, identity info of user, allowed permission. {“userid”: “.. ”, “issuer”: “... “,
“Sub” “....”, “exp”: “..”}
Signature- used to verify integrity of data transferred over wire.

JWT Flow -
1- user logs in using credentials
2- When a user is authenticated, a jwt is created and returned to the user.
3- when a user wants to access a protected resource, the client application sends JWT, typically in the HTTP authorization header.
4- JWT is used by application servers, to identify the user and allow access to resources.

Advantages- JWT are lightweight and easy to use by client applications.
Built in expiry mechanism