Date : 20/08/2020
JWT - Session-1
Mr. RAGHU

Client-Server Authentication:-
a. Stateful Authentication:

It will create one HTTP Session at server side when client is successfully authenticated
One Session-Id is provided and same is sent to client using Response as one Cookie
Client Machine, for next request onwards, submits Cookie to server,then server
verifies and provides service, until logout.

On click logout session will be invalidated.

b. *** Stateless Authentication:-
It will never create any Memory at server side.
For a client Authentication one unique number is generated ie called TOEKN.

Token can be created using SecretKey and even
Generated Token can be read using SecretKey.

This generated token is sent to client machine using Response.
Client has to send token using Request for 2nd request onwards..
Token is valid only for a period of time.

** State means - Data of Client stored at Server

-----Stateless Authentication used at----------
a. Webservices Authentication (server - server)
b. Horizontal Scaling (Microservices)
c. Resource Grant (Open Authorization/OAuth)
Register/Login + Login with Google, Facebook

Benifits:
*) Stateless concept, never allocates any memory at server.
*) It is good for Distributed Applications

Limitations:
*) Token must be validate on every request
*) If Token is shared with others then they can access client data/services.

==========

JWT (JSON Web Token)

JWT is a opensource service (API) that supports generating Token based on client
details and secretKey.