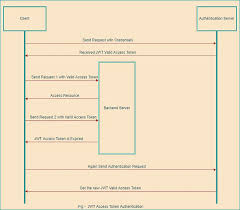
JWT authentication:



Instead of storing user credentials information somewhere on the server that can easily be accessed by attackers over the internet, we use JWT. When we use that, we maintain user secrets with different cryptographic algorithms and encode that to authenticate users.

* First, the user sends a request to the authentication server with credentials like the user name and password.
* Then, the authentication server will validate that information, and whatever information is provided by the user will be correct and successfully authenticated so the auth server can issue the JWT Valid Access Token to the user.
* Next, the user sends the first request to the backend server with a valid JWT Access Token, and the server will provide the requested resource to the user.