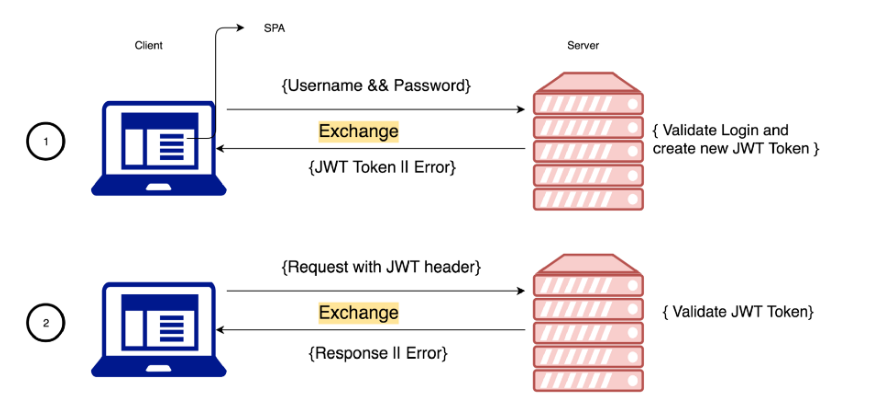
# What is JWT(JSON Web Tokens)? How it works?

. JWT is a type of token-based authentication. For every single request from a client to the server, a token is passed for authentication. It supports the stateless API calls.

JWT authentication is becoming very popular these days. The traditional authentication uses cookies and sessions. With the advent of Single Page Applications(SPA) and microservices, there is a need to look beyond the sessions. Any token based authentication serves that purpose

It is used for Securing Node.js RESTful APIs with JSON Web Tokens.



Let’s say a user wants to sign in to their account. They send a request with the required credentials such as email and password to the server. The server checks to see if the credentials are valid. If they are, the server creates a token using the desired payload and a secret key. This string of characters that results from the encryption is called a token. Then the server sends it back to the client. The client, in turn, saves the token to use it in every other request the user will send. The practice of adding a token to the request headers is as way of authorizing the user to access resources.

**authentication** is the act of logging a user in. **Authorization** is the act of verifying the access rights of a user to interact with a resource.

**Middleware** functions are used as bridges between some pieces of code. When used in the function chain of an endpoint they can be incredibly useful in authorization and error handling.

