Spring Boot Security Documentation

There are several types of spring security features those are shown below which we can implement in our web application among them Spring Boot JWT Authentication and Authorization is one of them. We can implement JWT details below like this

Spring Security Features:

1.LDAP (Lightweight Directory Access Protocol)

2.Single sign-on

3.JAAS (Java Authentication and Authorization Service)

4.LoginModule

5.Basic Access Authentication

6.Digest Access Authentication

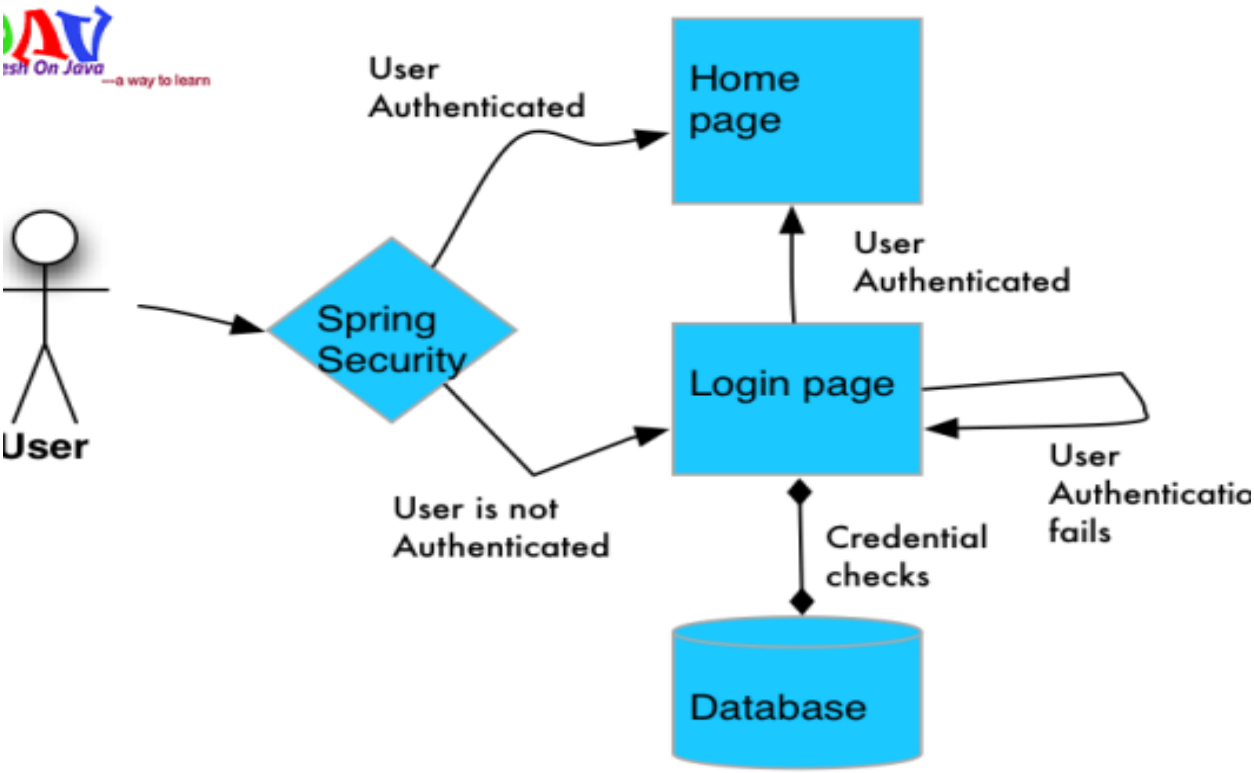
7.Web Form Authentication

8.Authorization

9.Software Localization

10.HTTP Authorization

Spring Security Flow:



Spring Boot JWT Authentication and Authorization :

JWT, or JSON Web Tokens is a standard that is mostly used for securing REST APIs. Despite being a relatively new technology, it is gaining rapid popularity.

In the JWT auth process, the front end (client) firstly sends some credentials to authenticate itself (username and password in our case, since we're working on a web application).

The server (the Spring app in our case) then checks those credentials, and if they are valid, it generates a JWT and returns it.

After this step client has to provide this token in the request's Authorization header in the "Bearer TOKEN" form. The back end will check the validity of this token and authorize or reject requests. The token may also store user roles and authorize the requests based on the given authorities.

JWT Authentication and Authorization flow Diagram: