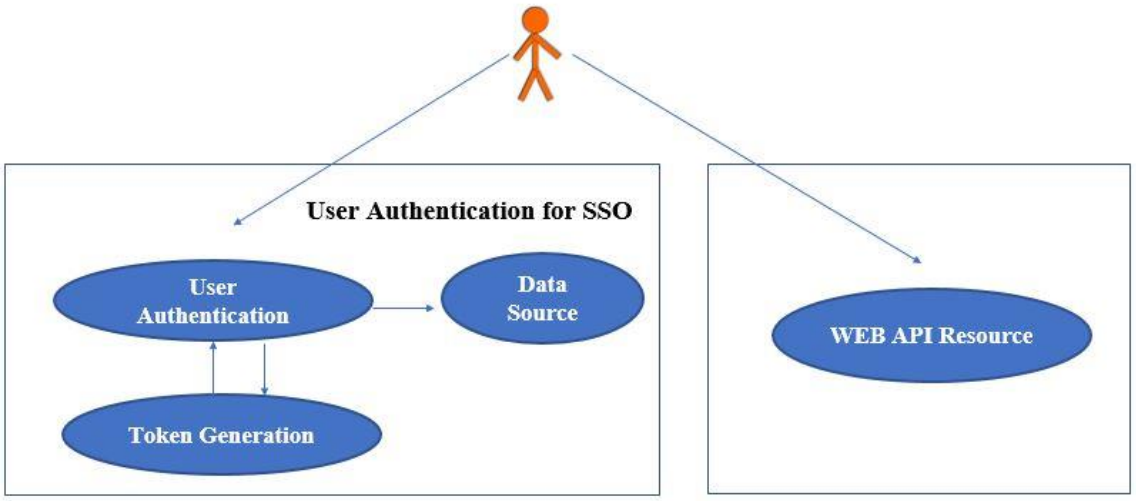

ALTIMETRIK

Use Case High-Level Description

- ✓ Develop a REST based web service with a dummy API (details at the end) and implement a token authentication system for the service (APIs) with the following specifications.
- ✓ User should be able to generate a unique token by providing his/her Username and Password.
- ✓ Once the token is generated then the application should be able to recognize the user if the token is set in the Authorization request header on any REST API calls, the user makes.
- ✓ The generated token should expire in 5 minutes and this expiration time should be configurable.
- ✓ Once the token is expired, the user should be provided with the 'Token Expired' message on the subsequent calls the user makes with the token.
- ✓ Before the expiry time, the user should be able to refresh the token that is the user should be able to generate a fresh token leading to the old token to expire before the actual expiry time.
- ✓ The token generation and verification logic can either be implemented from scratch or a library (like JWT) can be used.

ALTIMETRIK

- ✓ Implement standard Encryption Algorithm like (AES etc).
- ✓ One dummy REST API should be developed, which should return some dummy JSON data for verification of the token authentication developed. This dummy API should be accessed only by providing the active token in the header and return the respective expired message, if the token is expired as mentioned above.