Secure2FA

P. Teja Swaroop (17MIS1003)
Sandeep Kumar

Modules of proposed system :

1. **API (Application Program Interface)** : API is the way of communicating with the Secure2FA server. When any website wants to implement secure2fa, they can make requests to the API and get corresponding responses.

2. **Encryption** : The OTP generated by the server is encrypted with the Public key of the Secure2FA client device.

3. **Sender** : A sender program on the server will send the generated OTP to the corresponding Secure2FA device.

4. **Receiver** : A receiver program on the Secure2FA client device receives the data from the sender program (running on server)

5. **Fingerprint Scanner** : A fingerprint scanner sensor will scan the fingerprint data from the user's finger and forwards this to the authentication module

6. **Authenticator** : The authentication module authenticates the fingerprint data inputed by the user and makes sure that the user is allowed to access the device.

7. **Decryption** : The decryption module decrypts the received data by using the private key. The decrypted data is nothing but the received OTP.

8. **Display/Screen** : This module is responsible for displaying the decrypted OTP on the screen of the Secure2FA device.

9. **Clear/Reset** : This module is responsible for clearing the screen and deleting the OTP from the memory of the device.

Protocol Used : CoAP(Constrained Application Protocol)