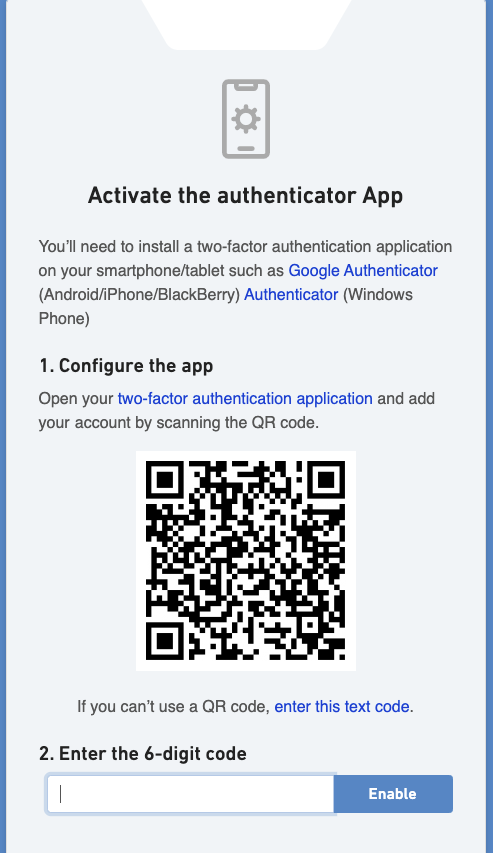
**SOLUTION 1**

**Step 1:**

1. Alice performs registration with personal details and username
2. Password will be sent to Alice’s registered email.

**Step 2:**

1. Alice logs in the application
2. Alice wishes to enable to 2FA authentication.
3. Under security option Alice enable the 2FA authentication.



**Step 3:**

1. During the next login, Alice enters the username and password.
2. Once application verify the username and password is valid, it will be routed to enter 2FA auth code.
3. Alice’s enters the 2FA auth code displayed in QR code scanned mobile.
4. Google auth code is validated and application logs in upon valid auth code

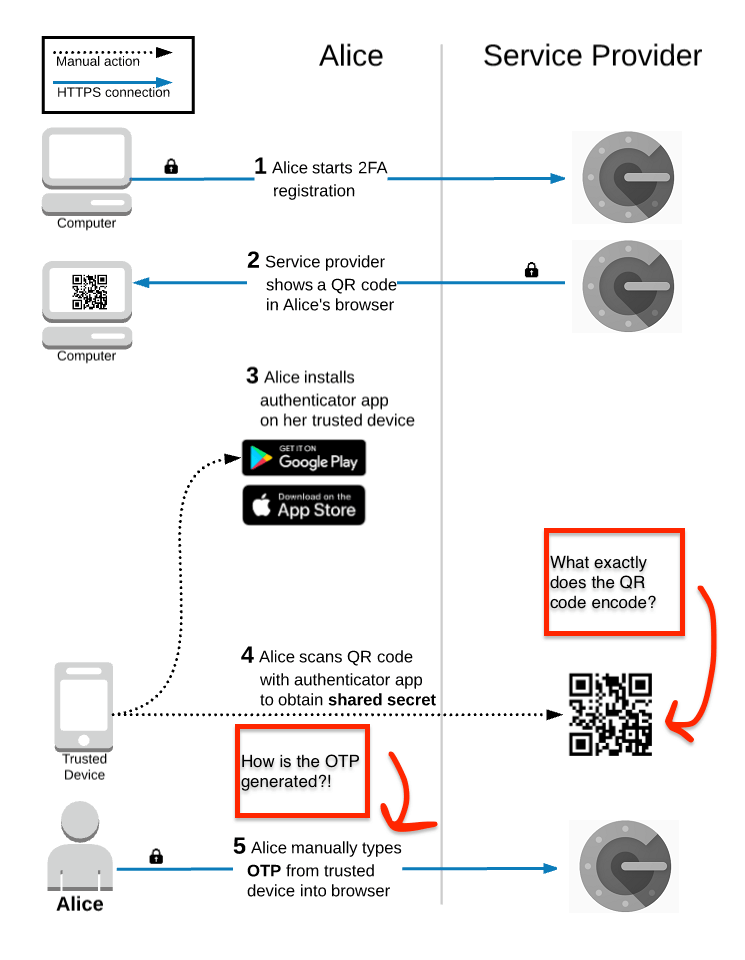
**Step 4:**

1. If in case Alice wants to reset his Google auth code by herself in future
2. Alice’s needs to enable the SMS & Email notification under security setting.
3. Alice’s will receive two different pin numbers, one to her register mobile and another to her registered email.
4. QR code will be displayed for scan
5. Upon scanning the QR code using Google authenticator, new auth code will be generated.
6. Alice needs to enter the newly generated auth code and save the setting.

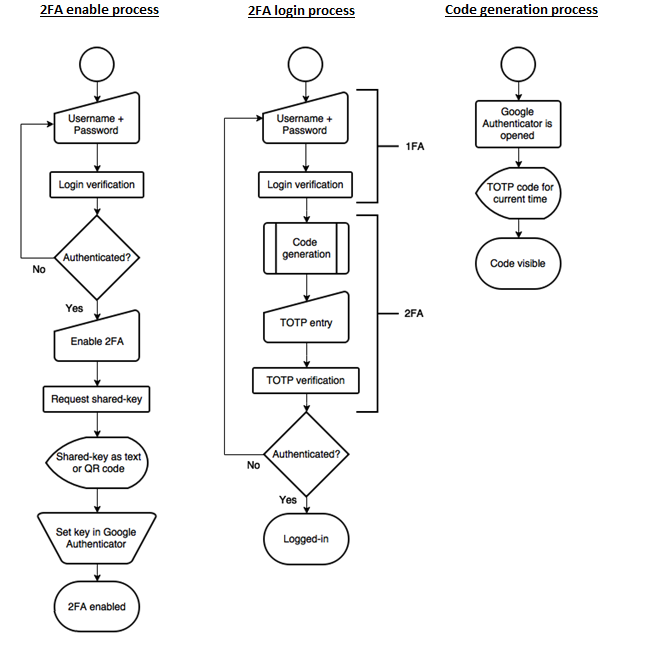
**Step 4.1:**

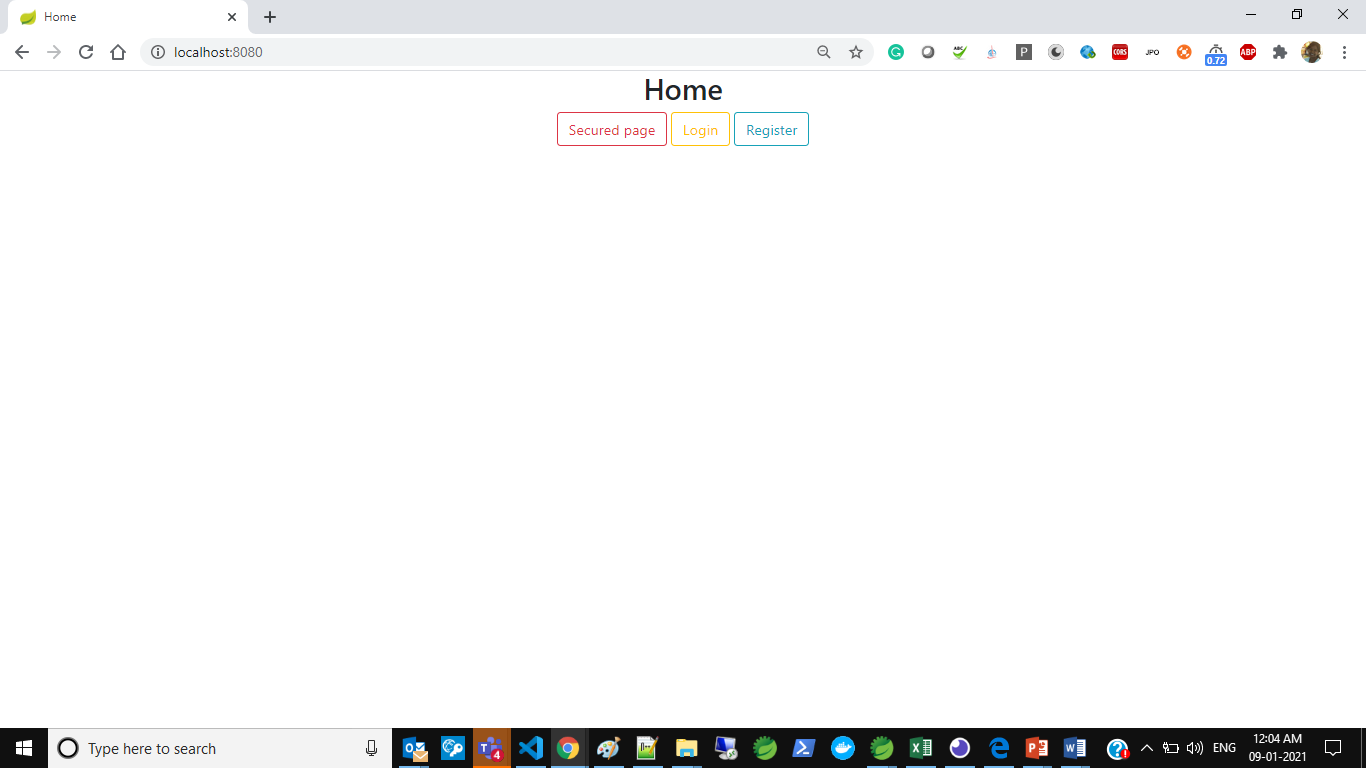
1. If in case, Alice does not register her mobile & email and she wants to reset her Google auth code, as her mobile is lost.
2. Alice should contact administrator or branch user for assistance.

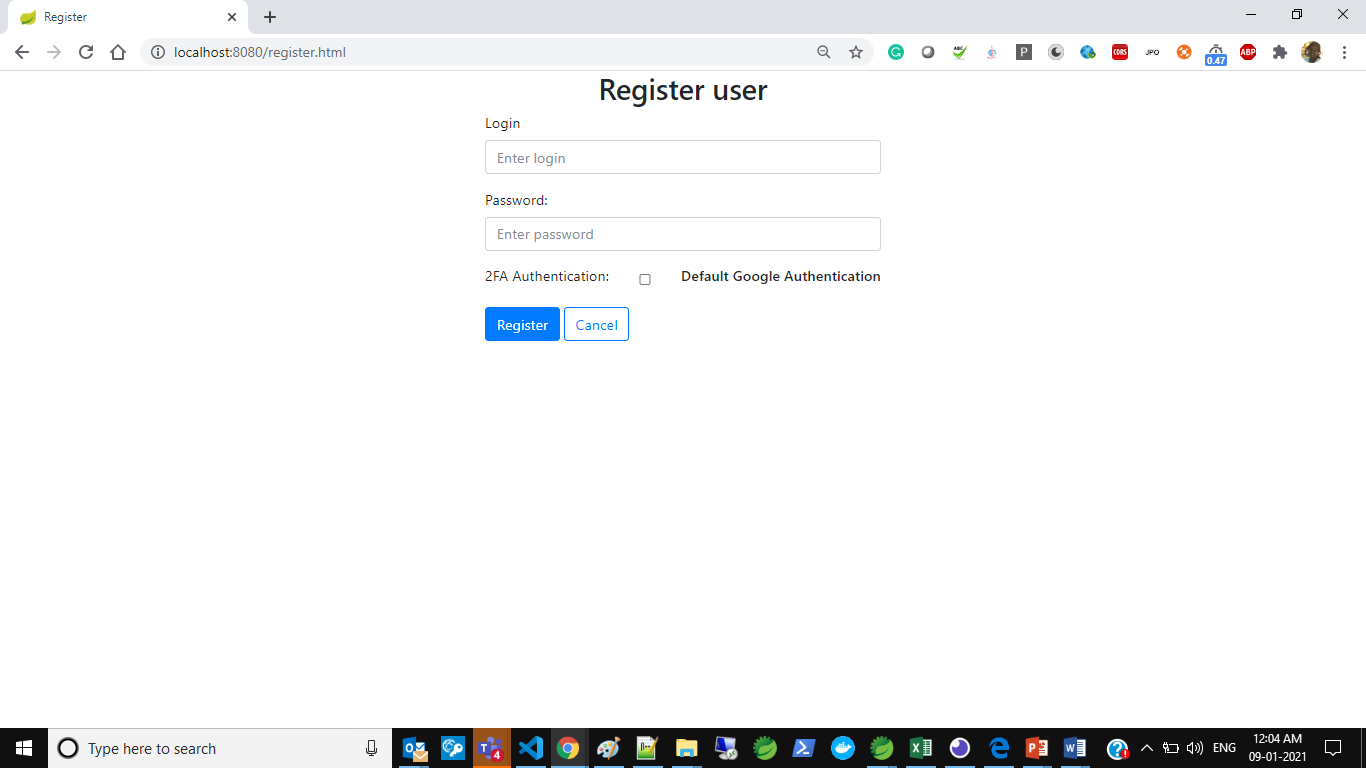
**Technical process**



**Functional process**

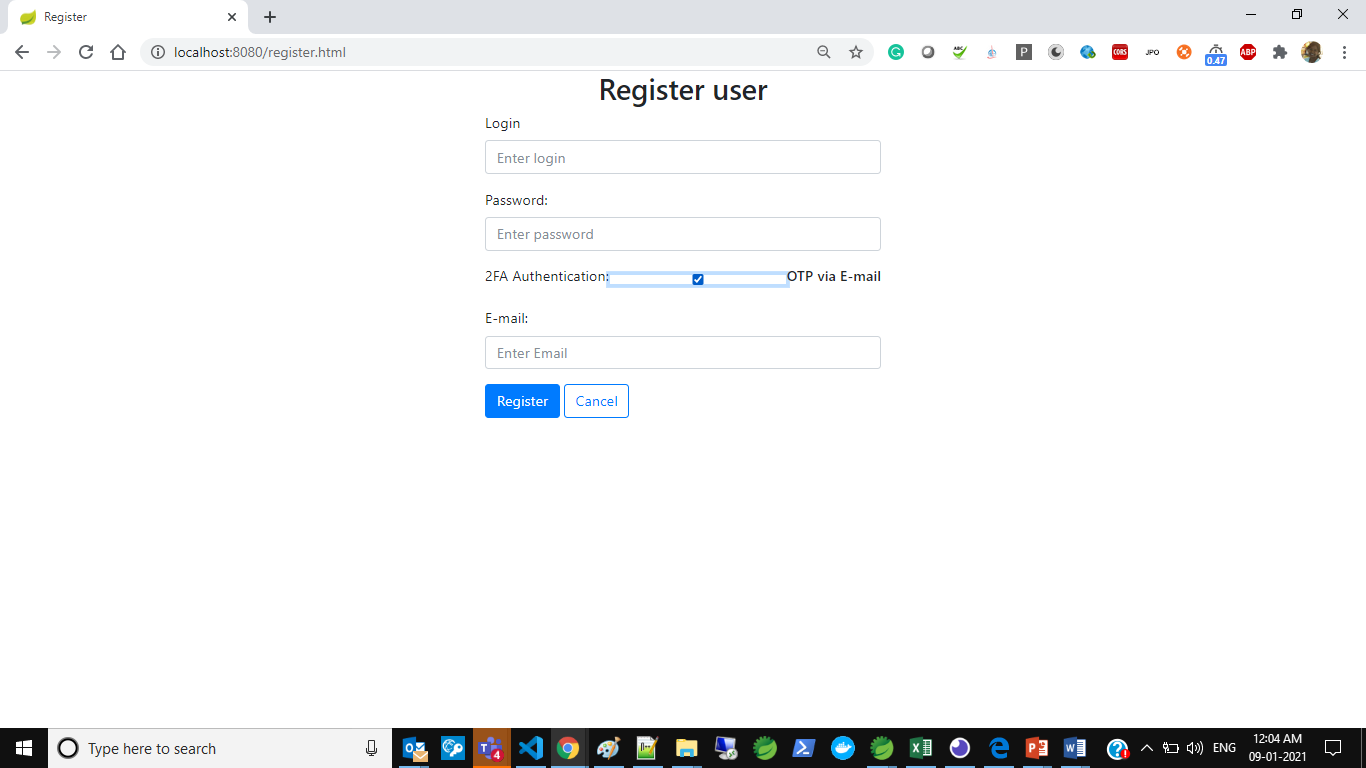




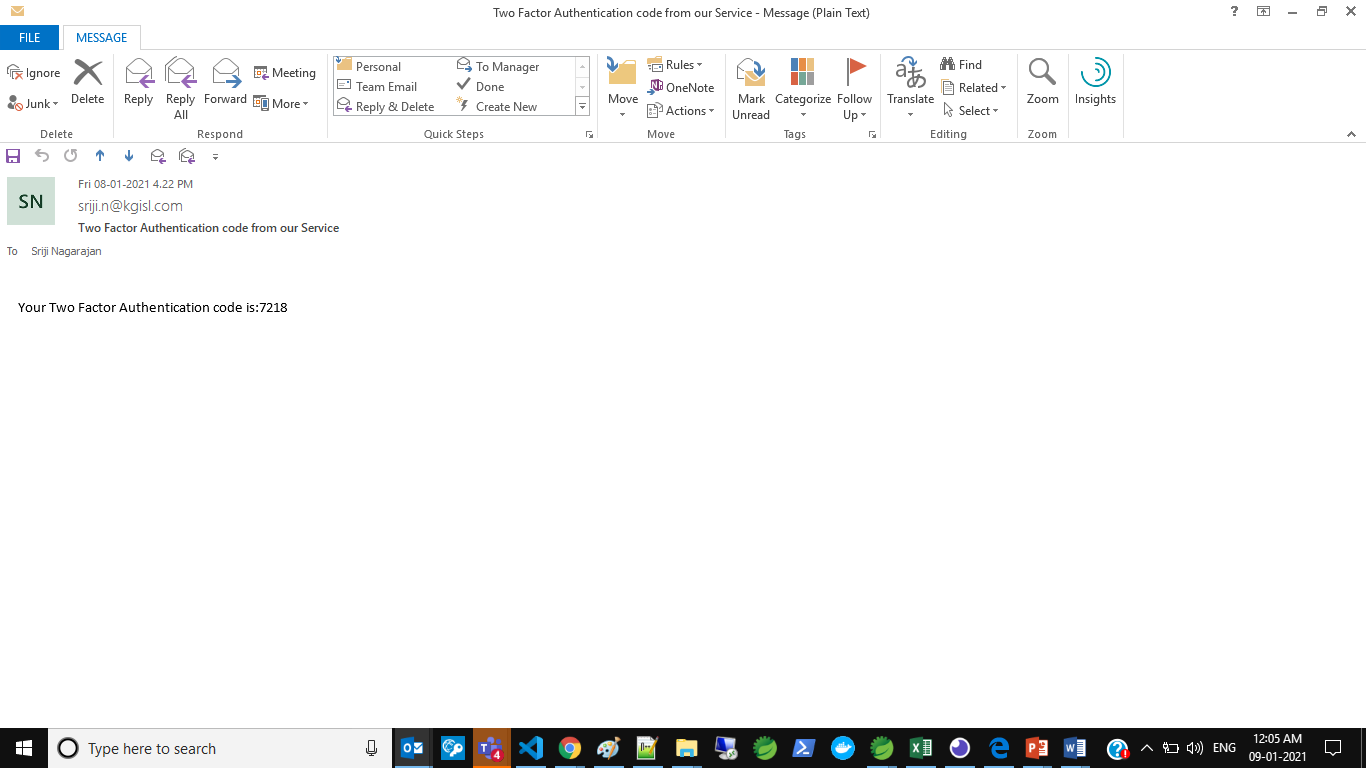


**SOLUTION 2**

* Whenever a user cannot access their mobile device for authentication, they can use their verified email to complete authentication.
* Implementation is added in the project by enabling 2FA



**Sample Email**



**SOLUTION 3**

* Any phone capable of receiving SMS text messages can be used to receive one-time codes.
* Implementation are available service provider need to be added. Sample project we have used Twilio
* 