
NORTH INDIA CYBER SECURITY HACKATHON

KEYRING



TEAM MEMBERS

- Sanyam jain
- Shivani sharma
- Raju gautam

- UPES Dehradun uttrakhand

PROBLEM STATEMENT

Currently we use 2 FA authentication. We have USER details and OTP generated over Mobile. But we can make it secure more than that. Anyhow attackers can fetch your OTP if they have your email account or something like “pushbullet” like services.

OUR SOLUTION

Here, the main motive behind is to make more and more secure to Mobile/E-transactions, so we will proceed accordingly.

Here is the workflow for the same

firstly the user will enter a data , data will pass through 4 stages

User Details : Here user will enter its details the details will be stored. But not yet transferred

OUR SOLUTION

OTP : user will get a SMS otp to validate further.

Facial Recognition : The images from the user will be stored in server and when user proceeds to gateway, the facial recognition window pops up and scans face and authorize it (This can be one of the option after OTP)

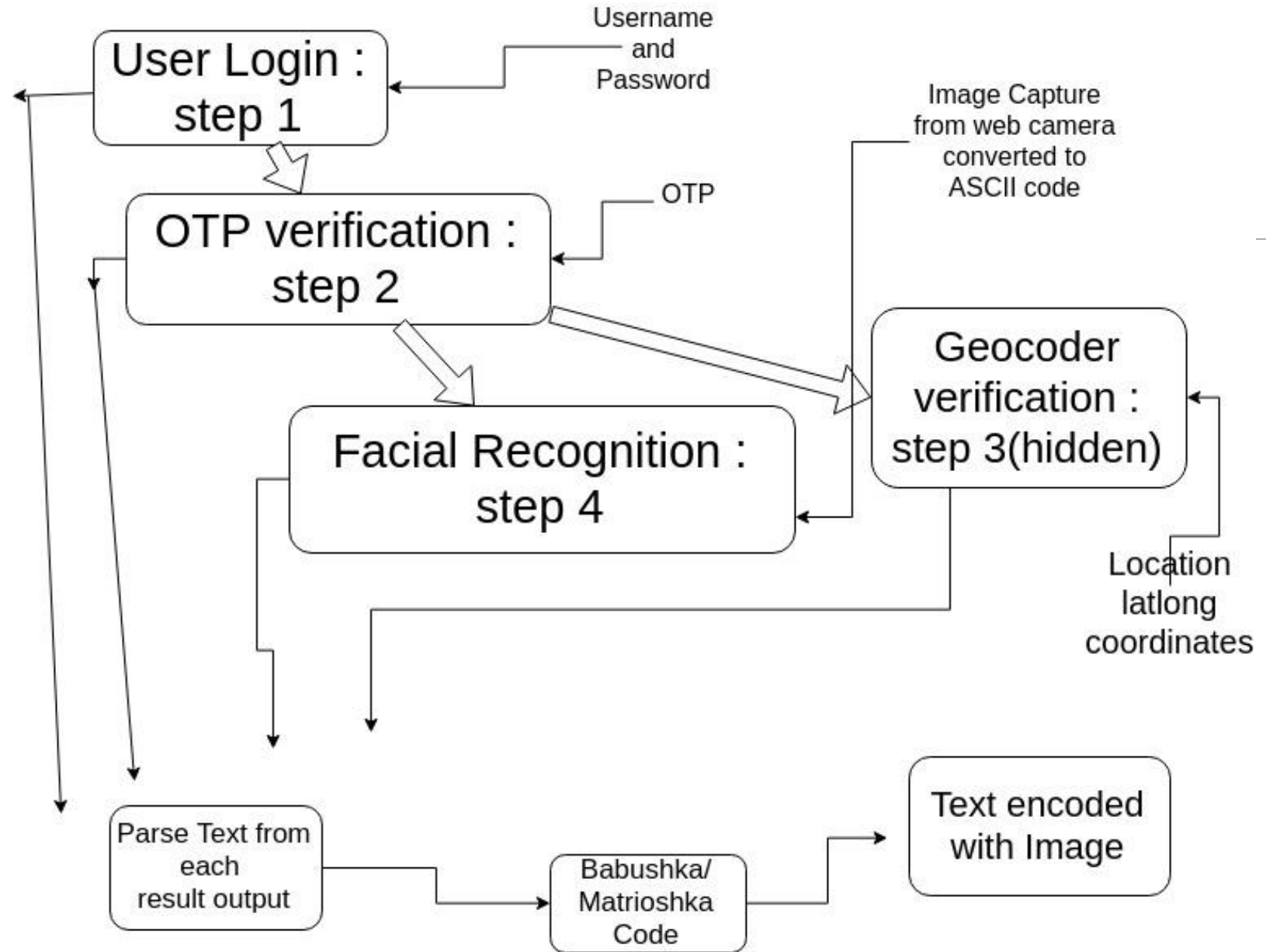
Geo-Location match : The users mobile location as well as the client system location is matched for the integrity.(optional security measure for client),user will update the location each time he travels using our team developed firebase android app – Location tracker by UPESACM and updated information will be shown on Dashboard of – fireapp.upesacm.org

OUR SOLUTION

Location tracker app for android will be used as a secondary resource to update the location of the client . The user will submit the location and the data will be sent to Firebase server.

Primary resource will be the point of transaction and the location will be fetched by application server which will be running on python . Both locations will be matched. If the locations are matched with both resources, User will get authenticated to proceed .

ROADMAP



Location tracker app for android will be used as a secondary resource to update the location of the client . The user will submit the location and the data will be sent to Firebase server.

Primary resource will be the point of transaction and the location will be fetched by application server which will be running on python . Both locations will be matched. If the locations are matched with both resources, User will get authenticated to proceed .

SECURITY ASPECT

- USER ACCOUNT DETAILS
- OTP
- FACIAL RECOGNITION (By front camera)
- GEO LOCATION