University of Venda
Creating Future Leaders

SOFTWARE IMPROVEMENT PROJECT

SURNAME & INITIALS	STUDENT NUMBER
Simane L	23002063
Manyua I	23013317
Mathelemusa M	23002610
Netshabumu V	23004051
Nemakonde E	21012784
Manganyi KC	21013999
Magoro MP	23027275
Baloyi N	21012267
Mbanyele AS	21003230
Masiphephethu E	22012522

Software Selection

CAPITEC MOBILE APPLICATION

The application chosen is the Capitec Mobile App. To clear out the confusion, Capitec is a retail bank, and it offers a wide range of banking services. Capitec also offers mobile banking services which we are putting our focus on. Here are some of challenges and challenges it currently facing.

- Customers are facing the problem of their funds being accessed without their concerns and does not require proper verification that is the rightful person doing such transactions. Funds can be accessed by just providing the card's details and it is very easy to lose your banking card.
- The Capitec's security software that is been used currently does not provide clarification on how customers can create a complex and a strong password/pin for the Mobile app. In that case, customers tend to create fewer complex password/pins which makes it easier for intruders to access their mobile app.
- The Mobile app itself it's not up to date, some of cancelled services such as debit orders that may have been cancelled still deduct funds not approved.
- The Mobile app is not well maintained, the application can crash for more than 4 hours and can be affecting customers who use this bank for business purposes. It becomes impossible for them to make urgent transactions.
- The application does not have proper software to capture information on who used the application, time and location.

Requirement Analysis

Existing Functionalities

- The application requires a pin or fingerprint to log in, so the intended user can access it.
- It uses data encryption to protect all data in transit, so even if the data is intercepted, it cannot be read.
- The application uses two factor authentication for certain transactions, like money transfers to make sure only the intended recipient receives the funds.
- Customers can pay bills for utilities, credit cards, loans, and other services directly from their Mobile app.
- Customers can activate, deactivate, or report lost/stolen cards directly from the Mobile app, as well as manage card limits and preferences.

Short Comings

- The app is not completely immune phishing or other types of attacks where a malicious actor tricks the user into revealing sensitive information.
- The application does not require a secure password/pin for login, so customers who create weak pin combination could be at risk of having their account compromised.
- Some customers are not well educated about the risks of using the public Wi-Fi networks when accessing the application, which could make them vulnerable to attacks.
- The application can take a long time(hours) going through service breakdown, where the Mobile app is not functioning.

Area Of Improvement

- The application should implement an advanced authenticator for proper verification of every transaction that happens on the app.
- A password/pin strength dictator must be implemented, to ensure that customers create a complex combination.
- There must be a software that ensure that the application is up to date, to avoid unnecessary clashes with the customers.
- The application must use software like JENKINS for maintenance purposes, Jenkins will make sure that maintenance is regularly scheduled. It will also run tests for deploying new versions of the application.
- They can implement a system of facial recognizer to record the person in use of the application in that moment, which will help when doing investigations of how funds were accumulated.

Solution Proposal

- The application should provide information to the customers while creating the profile on how they should create complex and strong password/ pin combinations. This will prevent customers from creating weak combinations like the year of birth which is easy to crack.
- The application must have the password dictator implemented, when customers reach the step of creating password/pin while registering a profile, the dictator must not allow them to continue with following step if the password created is not strong enough.

- There must be extra layers of security that must be implemented on the application. Face recognition technology such as Open Face tool must be used for capturing the facial expressions of the person who is in use of the application, this will help with evidence when the are funds missing or transactions that are unknown.
- Beside the traditional pin-based authentication, advanced authentication such a biometric factor (fingerprint recognition) must be used as an extra layer of authentication.
- To add to layers of security used, the application must provide the user with a one-time password/pin to verify if the person in use of the application is the right person. The one-time password/pin to verify must be sent to the mobile device that the customer registered a profile with.
- The managers or owners of the application should hire more tech employees who will be responsible for making sure that the application is up to date and is well maintained. This will help that the application will not experience service breakdown regularly since it will be well maintained.
- The application should also provide information to customers on how they can be able recognize malicious attacks. Also educate on how they cab be able to avoid such tricks for the safety of their funds.

ALGORITHM DESIGN

ALGORITHM

Step 1: Start.
Step 2: User opens the app using a registered mobile device.
Step 3: Immediately allow the app to access the camera using OpenFace tool.
Step 4: If the camera of an OpenFace tool is not accessed or activated, deny the access.
Step 5: Allow the access to use the app if the OpenFace tool is activated for face recognition.
Step 6: Display the fingerprint menu to the user.
Step 7: Prompt the user to use fingerprint recognition.
Step 8: If the fingerprint pattern does not match prompt the user to try again.
Step 9: If the user exceeds the attempts maintained by the app, display no more attempts, try again later.
Step 10: If the user's fingerprints match, allow the access to the user.
Step 11: Show code verification menu to the user.
Step 12: Prompt the user to enter the verification code that have been sent via SMS to the registered cellphone number.
Step 13: If the user entered the verification code which is incorrect, display code invalid.
Step 14: If the user continues to enter invalid verification code and exceeds the limit, display no more attempts, try again later.
Step 15: If the codes are correct, grant the user an access to the app and display Welcome message to the user.
Step 16: Stop

PSEUDOCODE

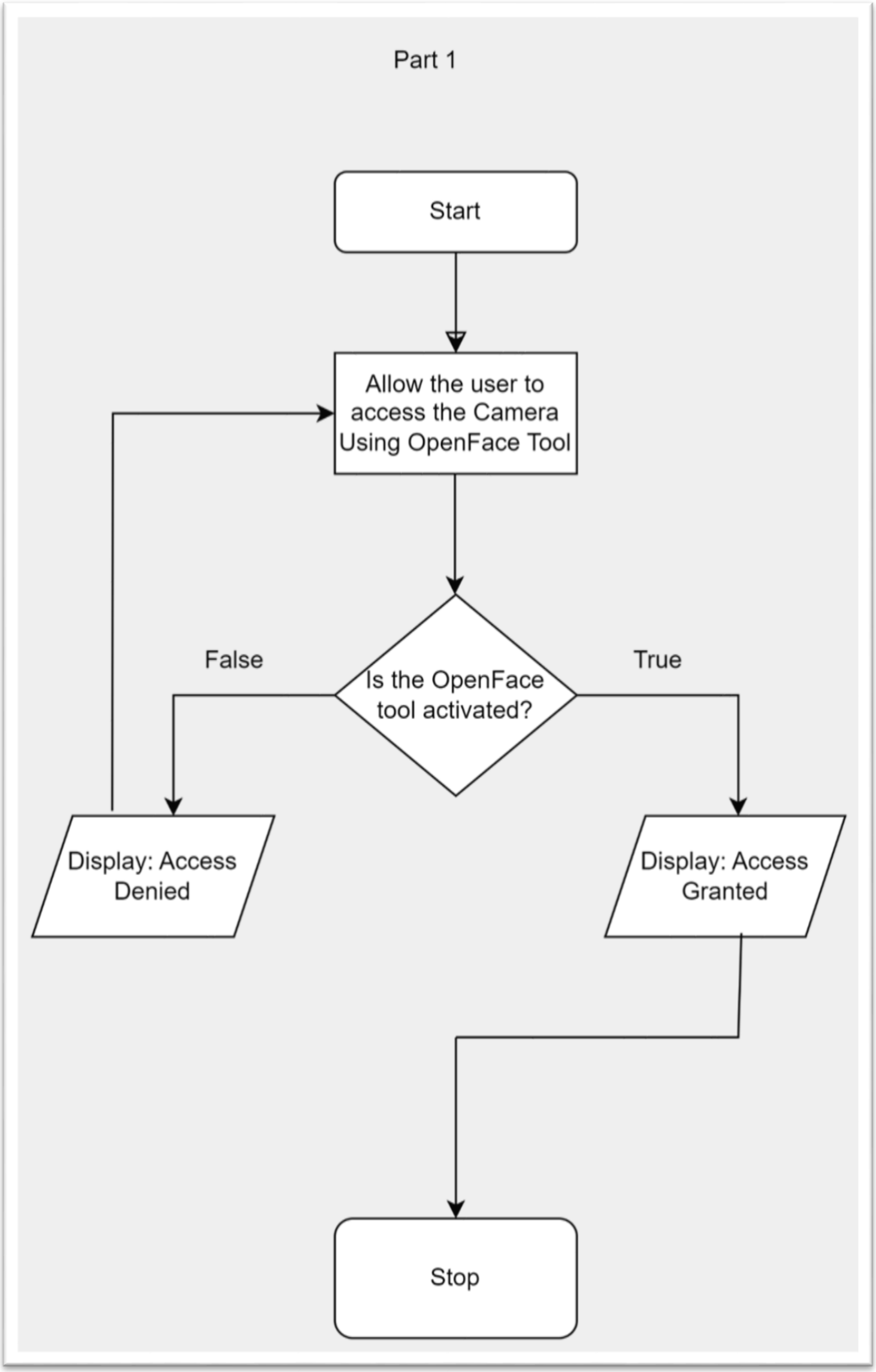
```
1. Start.
   -User opens the app using a registered mobile.
2. Input
   -Allow the app to access the camera using Open Face tool.
   -Prompt the user to use fingerprint recognition.
   -prompt the user to enter verification code that has been sent via SMS to the registered cellphone number
3. Process
   -If the camera of an Open face tool is not accessed or activated, deny the access.
   -Allow access to use the app if the Open Face tool is activated for face recognition
   -If the fingerprint pattern does not match then, prompt user to try again. If the user exceeds the number of attempts, tell the user to try again.
   -If the user's fingerprints match, allow access to the user.
   -If user entered verification code which is incorrect, deny access
   -If codes are correct, grant access to the app.
4. Output
   -Display welcome message and allow user to continue with his/her transactions.
5. End
```

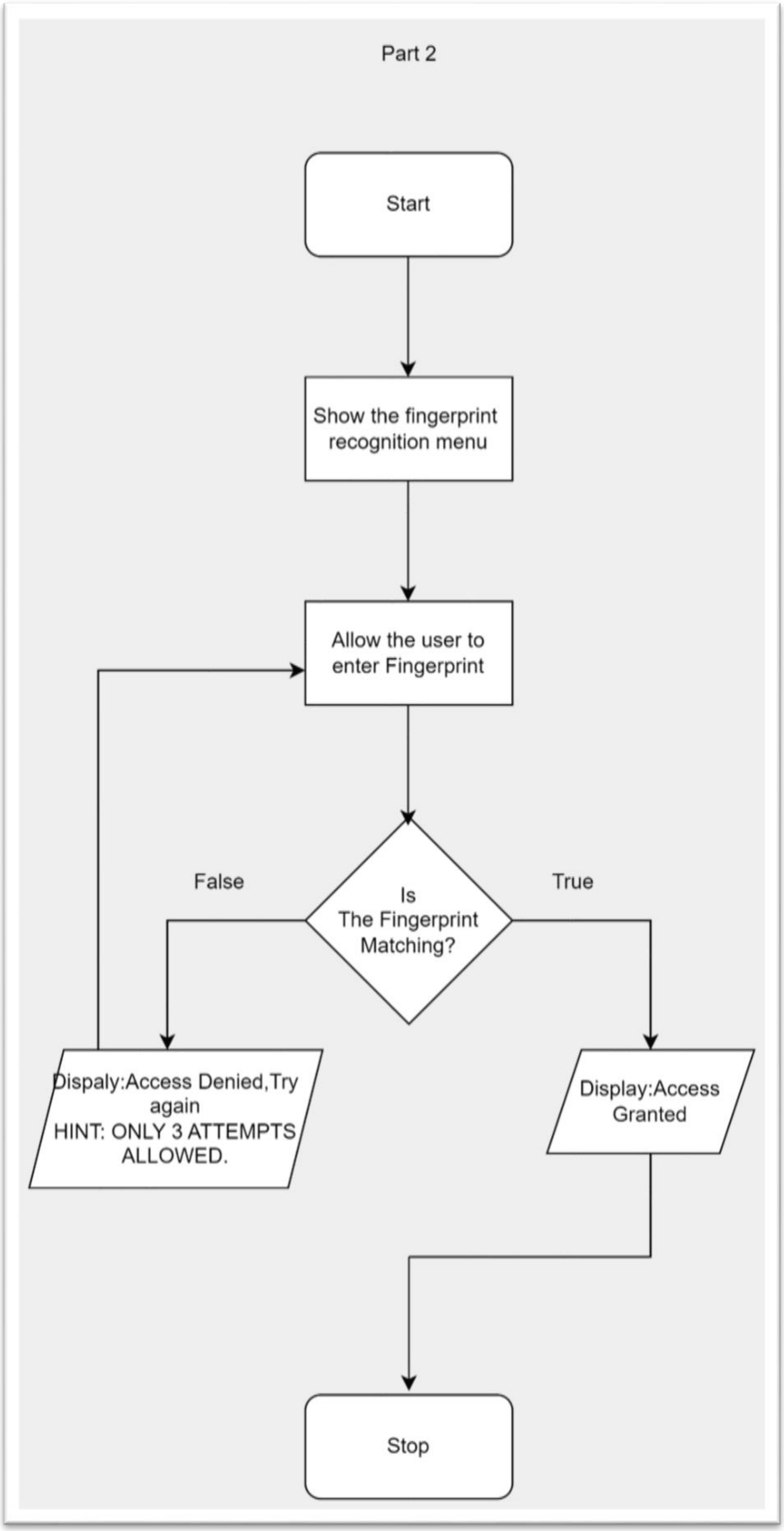
Visualization using Draw.io

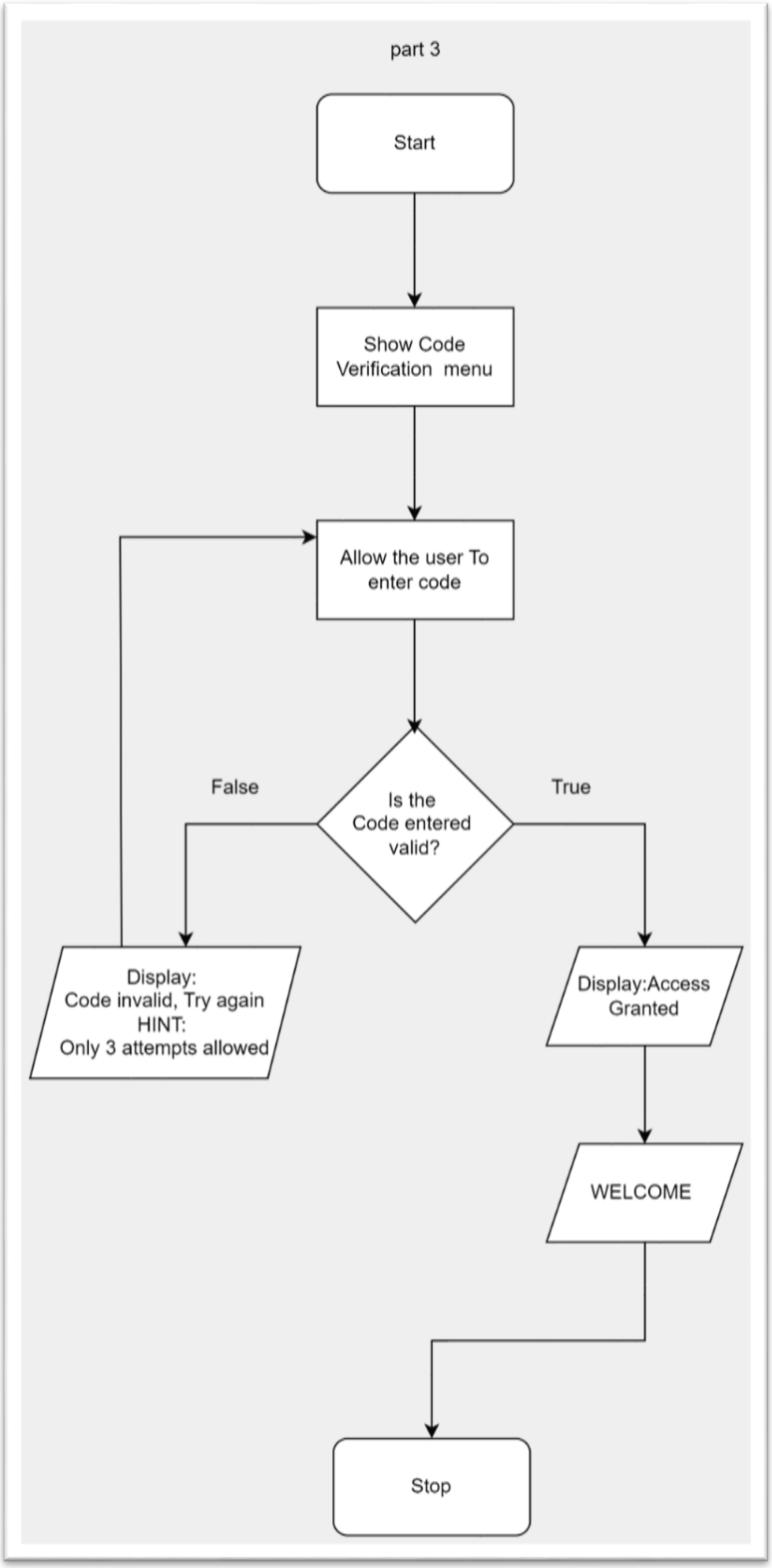
PART 1: Flowchart of OpenFace tool.

PART2: Flowchart of Fingerprint Recognition.

PART 3: Flowchart of Code Verification.


Part 1
Start
Allow the user to access the Camera Using OpenFace Tool
Is the OpenFace tool activated?
False
True
Display: Access Denied
Display: Access Granted
Stop


Part 2
Start
Show the fingerprint recognition menu
Allow the user to enter Fingerprint
Is The Fingerprint Matching?
False
True
Dispaly:Access Denied,Try again
HINT: ONLY 3 ATTEMPTS ALLOWED.
Display:Access Granted
Stop


part 3
Start
Show Code Verification menu
Allow the user To enter code
Is the Code entered valid?
False
True
Display: Code invalid, Try again HINT: Only 3 attempts allowed
Display:Access Granted
WELCOME
Stop