



UNIVERSITY
OF WOLLONGONG
AUSTRALIA

 SIM GLOBAL
EDUCATION

Bachelor of Computer Science

(Digital System Security)

CSCI321 – Final Year Project

SOFTWARE REQUIREMENT

SPECIFICATION

Project Particulars

Supervisor	Dr Ta Nguyen Binh Duong
Project Group	SS18/1F
Project Title	Two Factor Authentication

Project Team's Particulars

Student Number	Student Name	Email Address
5363536	Koh Hong Wei	hwkoh003@mymail.sim.edu.sg
5710923	Chua Han Ming Adler	hmachua002@mymail.sim.edu.sg
5711356	Ong Wei Hao	whong012@mymail.sim.edu.sg



go2FA

A secure file locking application

Document Control

Title: Project Proposal

Document Name: FYP_ProjectProposal

Distribution List

Name	Title/Role	Where

Record of Revision

Revision Date	Description	Section Affected	Changes Made By	Version after Revision	Notes
16 March	1 st Draft of SRS	All	Team		

Table of Contents

1.	Introduction	8
1.1.	Background.....	8
1.2.	Project Scope	8
1.3	Intended Audience and Reading Suggestions.....	8
2.	Product Overview Description	8
2.1	Product Perspective.....	8
2.2	Product Features.....	8
2.2.1	Locking File	8
2.2.2	Unlocking file	8
2.2.3	Secure OTP generation	8
2.2.4	View File	9
2.2.5	View History.....	9
2.3	User Classes and Characteristics	9
2.3.1	Physical Actors.....	9
2.3.2	System Actors	9
2.4	Operating Environment	9
2.5	Implementation Constraints	9
2.6	User Documentation.....	9
2.7	Assumptions and Dependencies	9
3.	System Features	10
	Main Use Case	10
1.1	Register Account	10
	Use Case	10
	Activity Diagram	11
	Sequence Diagram	12
1.2	Account Recovery	13
	Use Case	13
	Activity Diagram	13
	Sequence Diagram	13
1.3	Login.....	14

Use Case	14
Activity Diagram	15
Sequence Diagram	16
1.4 Change Password.....	17
Use Case	17
Activity Diagram	17
Sequence Diagram	18
1.5 Lock.....	19
Use Case	19
Activity Diagram	19
Sequence Diagram	20
1.6 Unlock	21
Use Case	21
Activity Diagram	21
Sequence Diagram	22
1.7 View File.....	23
Use Case	23
Activity Diagram	23
Sequence Diagram	23
1.8 View History.....	24
Use Case	24
Activity Diagram	24
Sequence Diagram	24
1.9 Change Registered Mobile.....	25
Use Case	25
Activity Diagram	25
Sequence Diagram	25
2.1 Delete User.....	26
Use Case	26
Activity Diagram	26
Sequence Diagram	26
2.2 Account Recovery.....	27
Use Case	27
Activity Diagram	27

Sequence Diagram	27
3.1 Login	28
Use Case	28
Activity Diagram	28
Sequence Diagram	29
3.2 Register Account	31
Use Case	31
Activity Diagram	32
Sequence Diagram	33
3.3 OTP Generation	34
Use Case	34
Activity Diagram	34
Sequence Diagram	35
3.4 Change Password	36
Use Case	36
Activity Diagram	36
Sequence Diagram	37
3.5 Account Recovery.....	38
Use Case	38
Activity Diagram	38
Sequence Diagram	38
3.6 Change Registered Computer	39
Use Case	39
Activity Diagram	39
Sequence Diagram	39
4. External Interface Requirements	40
4.1 Hardware Interfaces.....	40
4.2 Software Interfaces	40
5. Non-functional Requirements	41
5.1 Performance Requirements	41
5.2 Safety Requirements	41
5.3 Security Requirements	41
5.4 Software Quality Attributes	41
References.....	41

Appendix A: Glossary	41
----------------------------	----

1. Introduction

1.1. Background

The purpose of this document is to provide a detailed overview of our software product. This includes the description of our project's target audience, system features, user interface and both hardware and software requirements.

1.2. Project Scope

This project aims to provide users with a way to enhance security on file management on desktop applications. We will be including a two factor authentication mechanism to secure our files from unauthorised usage.

1.3 Intended Audience and Reading Suggestions

2. Product Overview Description

2.1 Product Perspective

Go2FA is an application running on both Windows/ Macintosh (PC) and Mobile(Android) platform written in JAVA. It is intended for providing a secure method of protecting a user's file or folder in their local PC with our Two Factor Authentication. The system uses a secured cryptographic algorithm to identify a user action within the application. This system uses what the user has and what the user knows as a way of identification. User has a username and password which will be created upon installing the application on either PC or mobile. User has mobile phone with them all the time, so we implemented QRCode scanner capability in our application to further add into the security of the application function.

2.2 Product Features

2.2.1 Locking File

The user has the option to lock file located in their local PC with our cryptographic algorithm.

2.2.2 Unlocking file

The user has the option to unlock file located in their local PC with our cryptographic algorithm.

2.2.3 Secure OTP generation

The system provides QRCode upon the locking or unlocking action done by User, which will need the camera functionality of the user's mobile by using the application on the device. The QRCode will then issue an OTP after scanning which can be entered to recognise legitimacy of user.

2.2.4 View File

The user has the option to view files that are locked using our application just by simply entering the date which the file has been locked or the file name.

2.2.5 View History

The user has the option to view past login history and actions that he has done using our application just by simply entering the date he wants to identify.

2.3 User Classes and Characteristics

2.3.1 Physical Actors

Window/Mobile Users: The user who uses the system and make use of the services provided by the application.

2.3.2 System Actors

2.3.2.1 SQL Database

2.4 Operating Environment

This system operates in both Windows/Macintosh and Android Operating System.

2.5 Implementation Constraints

The main constraint of this program is the support for files and folders in local directories and files locked can only be unlocked by the same PC with contains the directory.

2.6 User Documentation

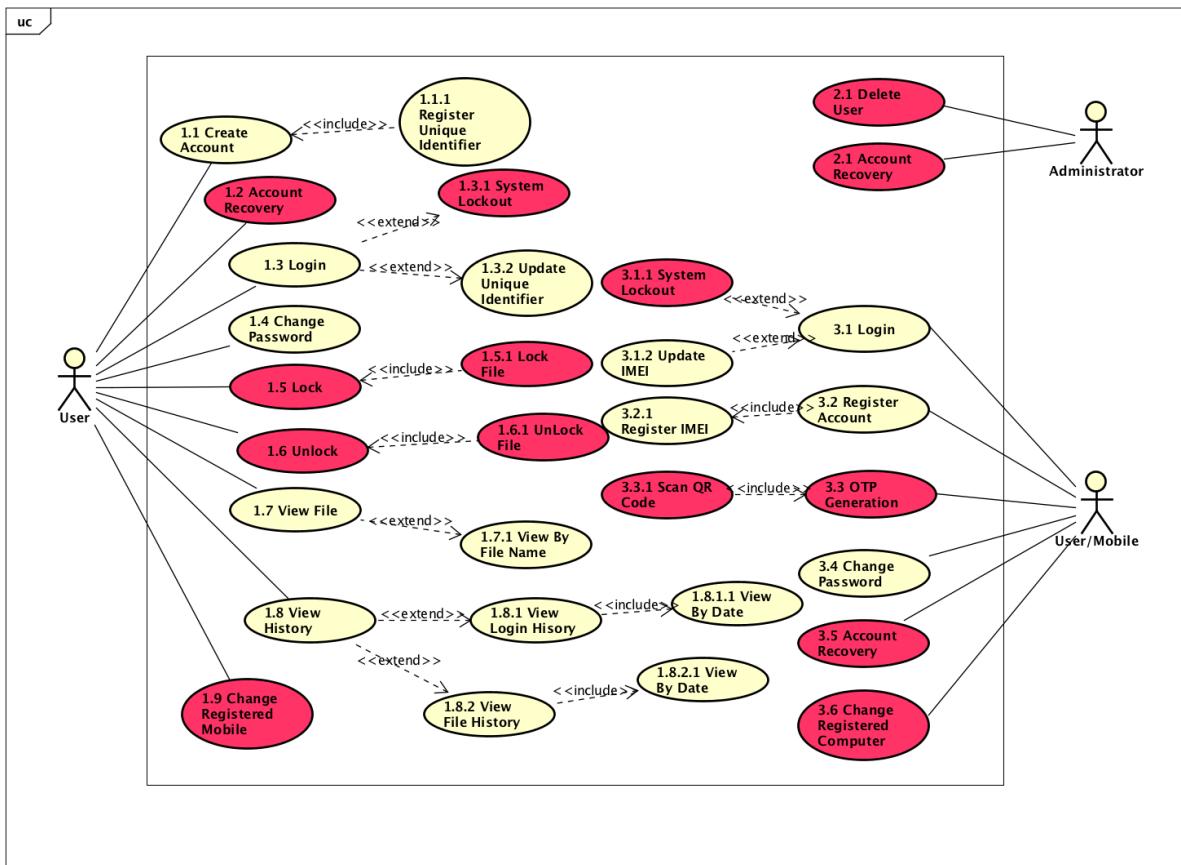
The user can use the User Manual to understand more of the interfaces of the system.

2.7 Assumptions and Dependencies

- The user is liable for keeping his log in credentials secured and confidential.
- The user is liable for the safekeeping of his copies of document outside of our system secured.
- The user is liable for the security and breach of his local PC.

3. System Features

Main Use Case



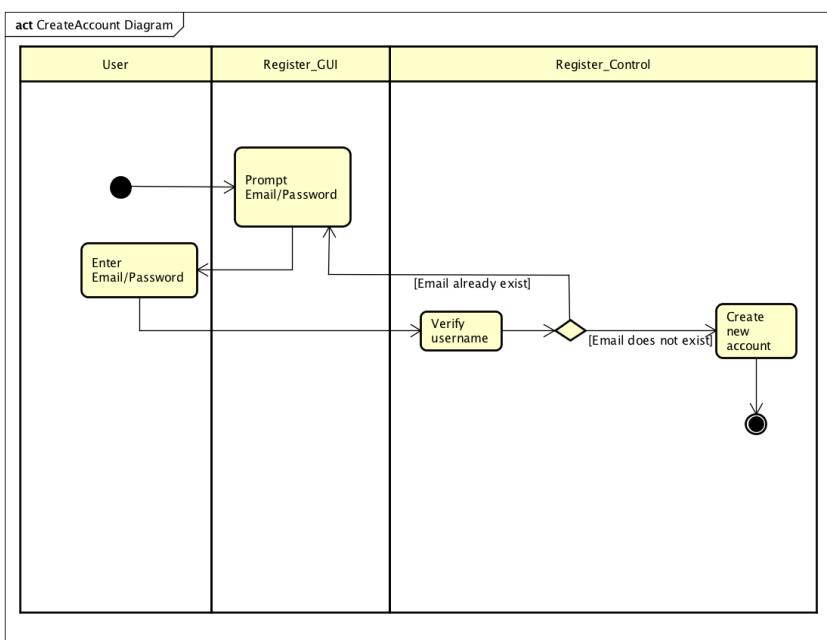
1.1 Register Account

Use Case

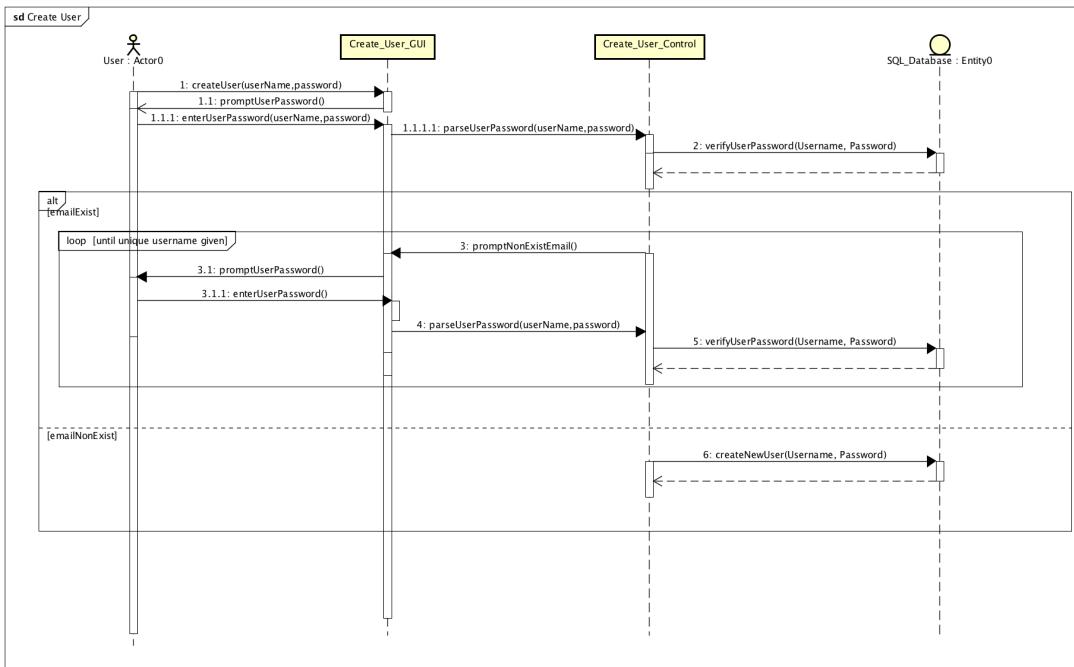
Use Case Textual Description	
UC-ID	1.1
Name	Register Account
Description	To allow user to register new account after he download the application for the first time
Actor(s)	User
Precondition	A user has installed the application and wish to create a new account
Main Scenario	<p>Step 1: System display a User Interface with fields to ask for user email address and desired password</p> <p>Step 2: User submits form and system does validation</p> <p>Step 2(alternate): If data is invalid, an error message will be displayed, and user is sent back to form for re-entry of right credentials</p> <p>Step 3: User password will be hashed</p> <p>Step 4: System captures MAC address <u>via U/C 1.1.1 Register Unique Identifier</u></p> <p>Step 5: System updates the SQL Database</p> <p>Step 6: User is redirected to log in screen</p>

Use Case Textual Description	
UC-ID	1.1.1
Name	Register Unique Identifier
Description	To allow system to register a unique identifier of user for log in
Actor(s)	User
Precondition	The user is registering an account and system will need to capture user's unique identifier (MAC Address)
Main Scenario	Step 1: After user has created account, system will automatically capture the MAC Address of the user's computer.

Activity Diagram



Sequence Diagram



1.2 Account Recovery

Use Case

Use Case Textual Description	
UC-ID	1.2
Name	Account Recovery
Description	To allow user to recover their lost or forgotten account
Actor(s)	User
Precondition	The user has a registered account and forgotten password
Main Scenario	Step 1: User selects account recovery on Log in screen Step 2: System prints out a form to prompt for User account email Step 3: User fills up the email and system do validation Step 3(alternate): If email is invalid, an error message will be displayed, and user is sent back to form for re-entry of right credentials Step 4: System will generate new password Step 5: System will send an email with new generated password to the register email address

Activity Diagram

Sequence Diagram

1.3 Login

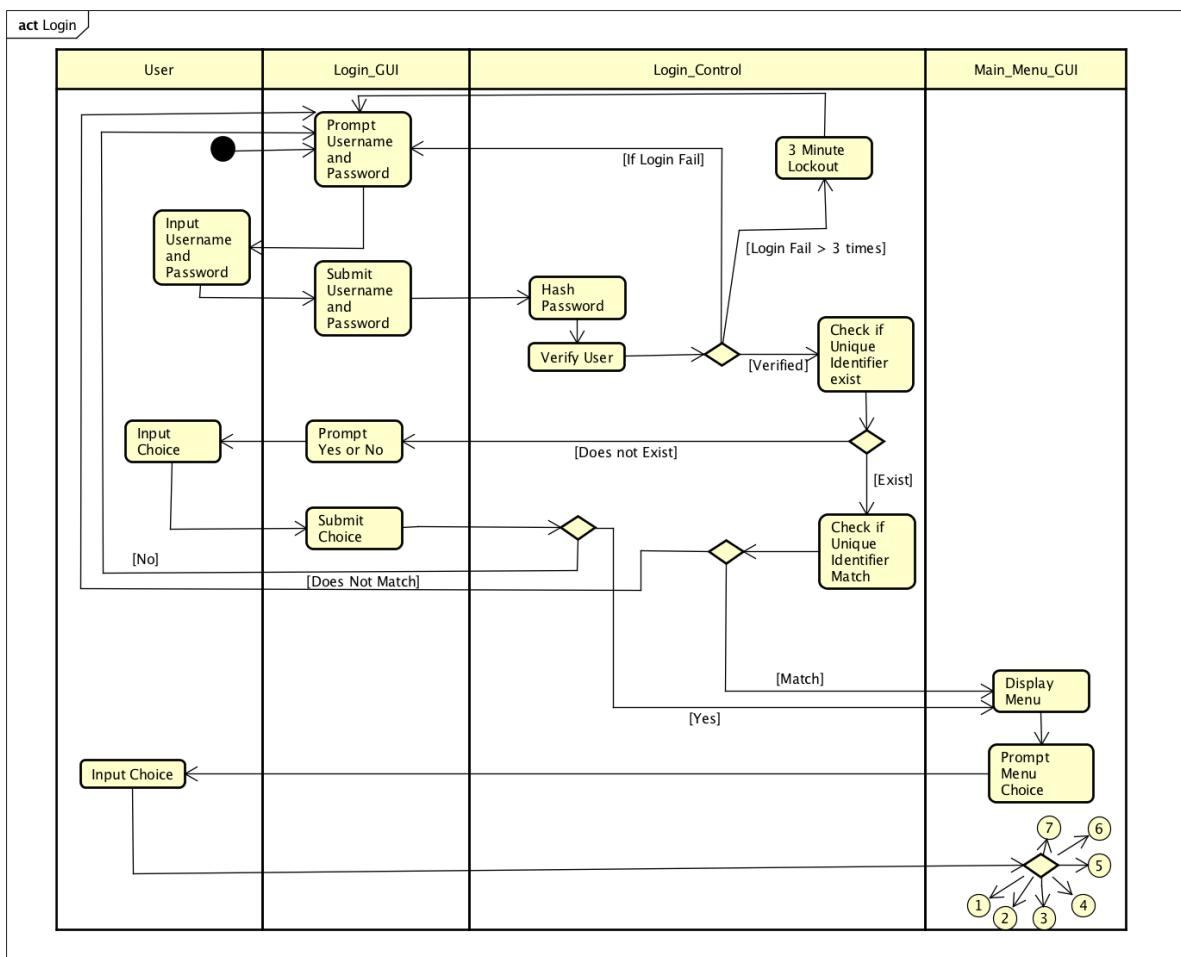
Use Case

Use Case Textual Description	
UC-ID	1.3
Name	Login
Description	To allow User to log in to the system
Actor(s)	User
Precondition	The user has a registered account
Main Scenario	<p>Step 1: User enters their log in credentials in the log in screen</p> <p>Step 2: System hash the User password and validates with SQL Database</p> <p>Step 2(alternate): If log in credentials are wrong, an error message will display, and User will be prompt to enter credentials again</p> <p>Step 2(alternate): If log in credentials is wrong for 3 times, system will be lock from User for 3 minutes <u>via U/C 1.3.1 System Lockout</u></p> <p>Step 2(alternate): If account is created via Mobile app, upon first login on the computer, user will be prompt to capture MAC address of the computer via <u>U/C 1.3.2 Update Unique Identifier.</u></p> <p>Step 3: System will display Main Menu</p>

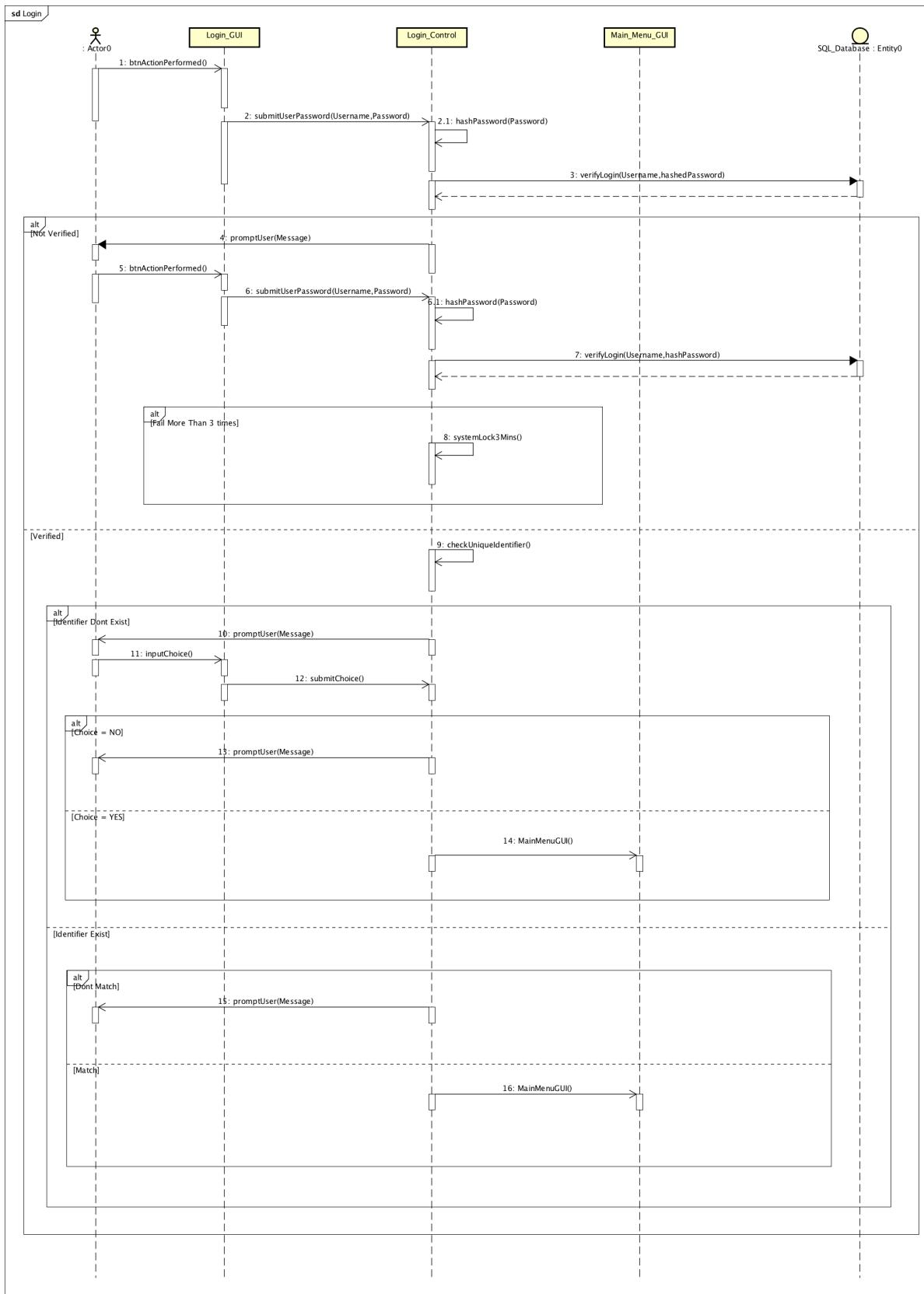
Use Case Textual Description	
UC-ID	1.3.1
Name	System Lockout
Description	Lock User out after several failed log in attempts
Actor(s)	User
Precondition	The user has 3 failed log in attempts
Main Scenario	<p>Step 1: System will lock the user out of the system</p> <p>Step 2: User will be required to restore account via <u>U/C 1.2 Account Recovery</u></p>

Use Case Textual Description	
UC-ID	1.3.2
Name	Update Unique Identifier
Description	To allow system to capture the missing identifier from user (MAC Address)
Actor(s)	User
Precondition	The user has created an account with his mobile and log in to his computer for the first time.
Main Scenario	Step 1: After user has logged in, the system will automatically capture the missing unique identifier and update in the database.

Activity Diagram



Sequence Diagram

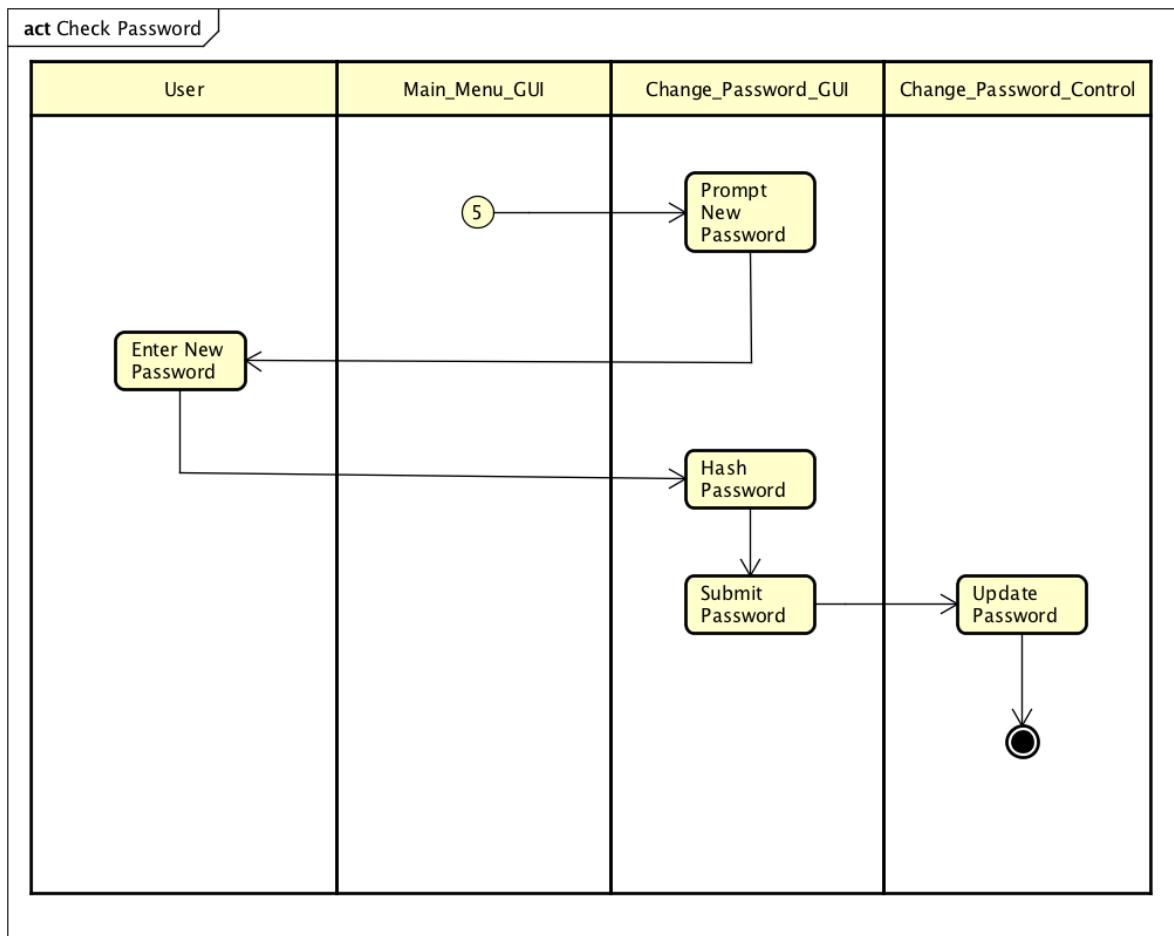


1.4 Change Password

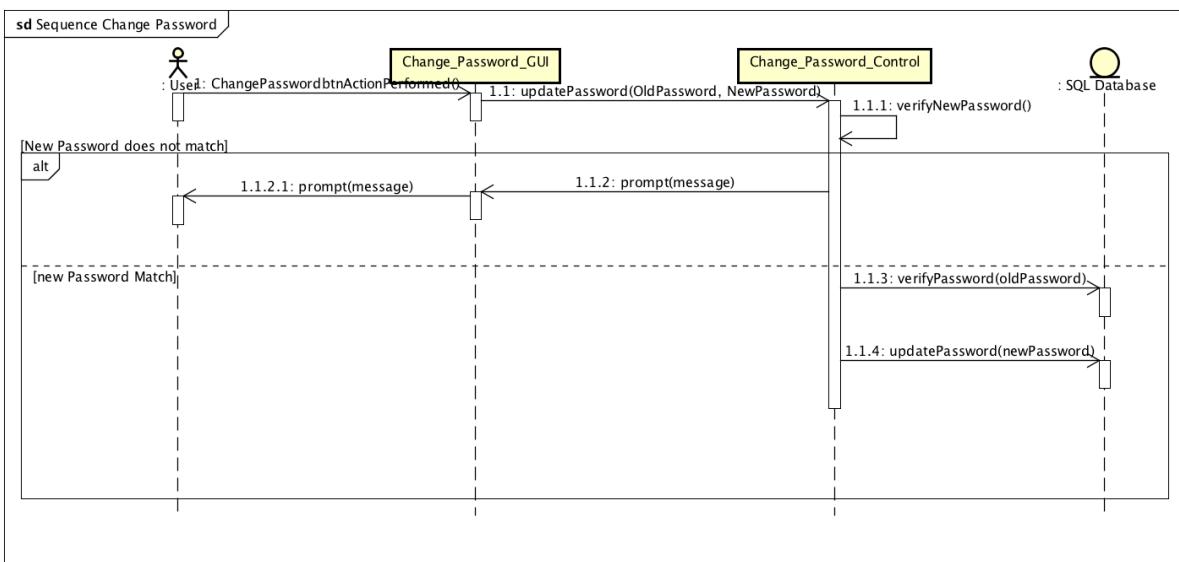
Use Case

Use Case Textual Description	
UC-ID	1.4
Name	Change Password
Description	To allow User to change their password
Actor(s)	User
Precondition	The user has a registered account and wish to update the current password
Main Scenario	<p>Step 1: User enters username and password at Log in screen</p> <p>Step 2: User selects change password at the main menu</p> <p>Step 3: System displays a form for user to fill up the new password they desire</p> <p>Step 4: User enters the new desired password and system do validation</p> <p>Step 5: System will update the SQL Database with the new password</p>

Activity Diagram



Sequence Diagram

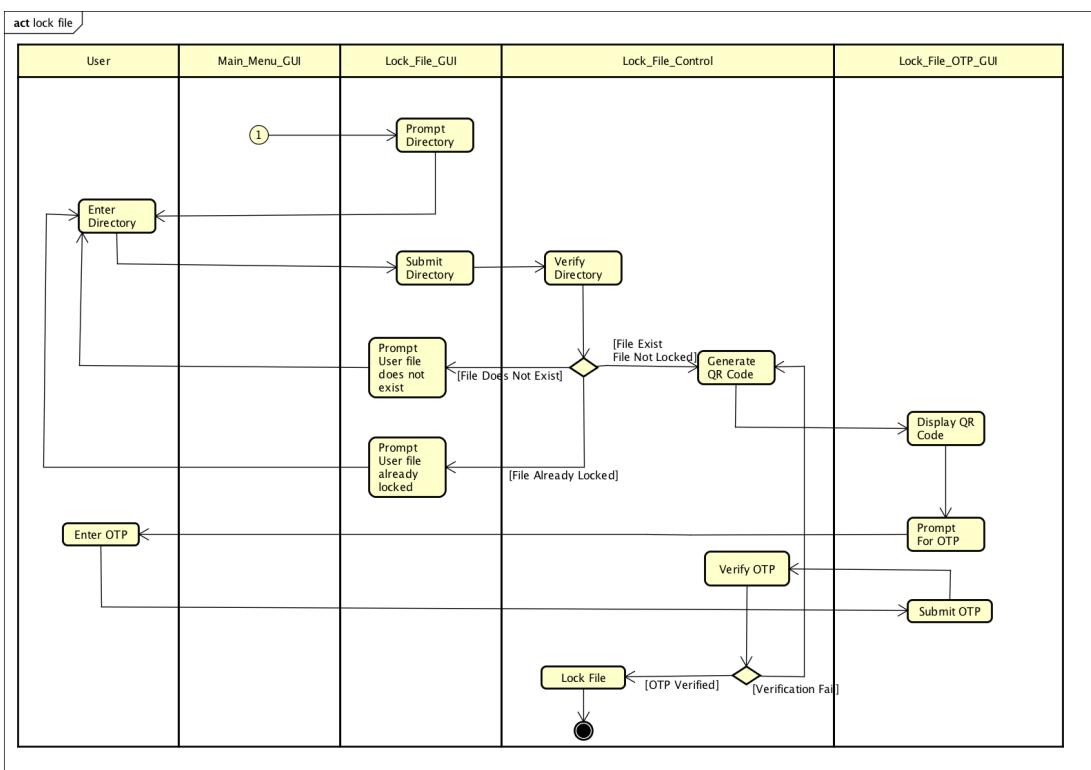


1.5 Lock

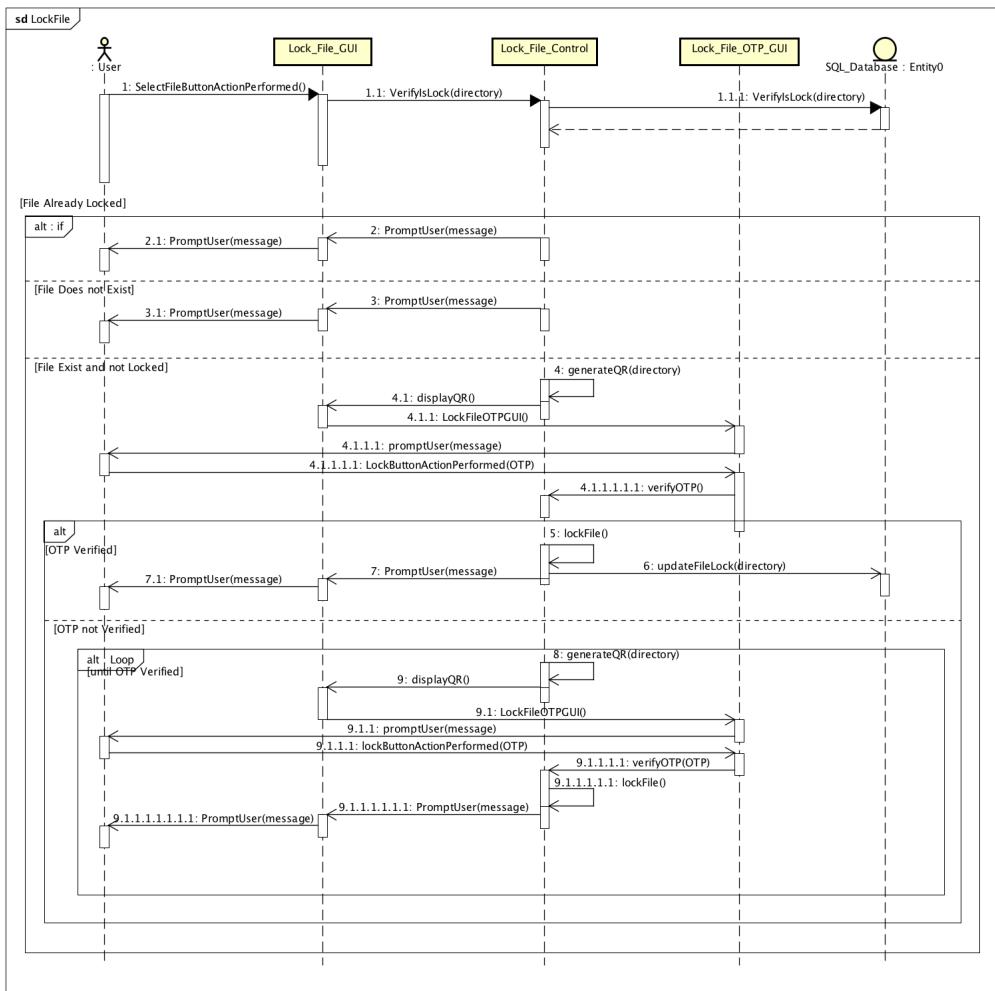
Use Case

Use Case Textual Description	
UC-ID	1.5
Name	Lock
Description	To allow user to lock their files using in the system
Actor(s)	User
Precondition	The user has a registered account and has file that they want to lock
Main Scenario	<p>Step 1: User selects Lock file option in the Main Menu.</p> <p>Step 2: System displays a form to fill up the directory</p> <p>Step 3: User enters the directory and system validates</p> <p>Step 3(alternate): If directory is invalid, an error message will display, and User will be redirected to form to fill up directory.</p> <p>Step 3(alternate): If the file in directory is already locked, an error message will display, and User will be redirected to form to fill up the correct directory</p> <p>Step 4: The system locks the file via via U/C 1.5.1 Lock File</p>

Activity Diagram



Sequence Diagram

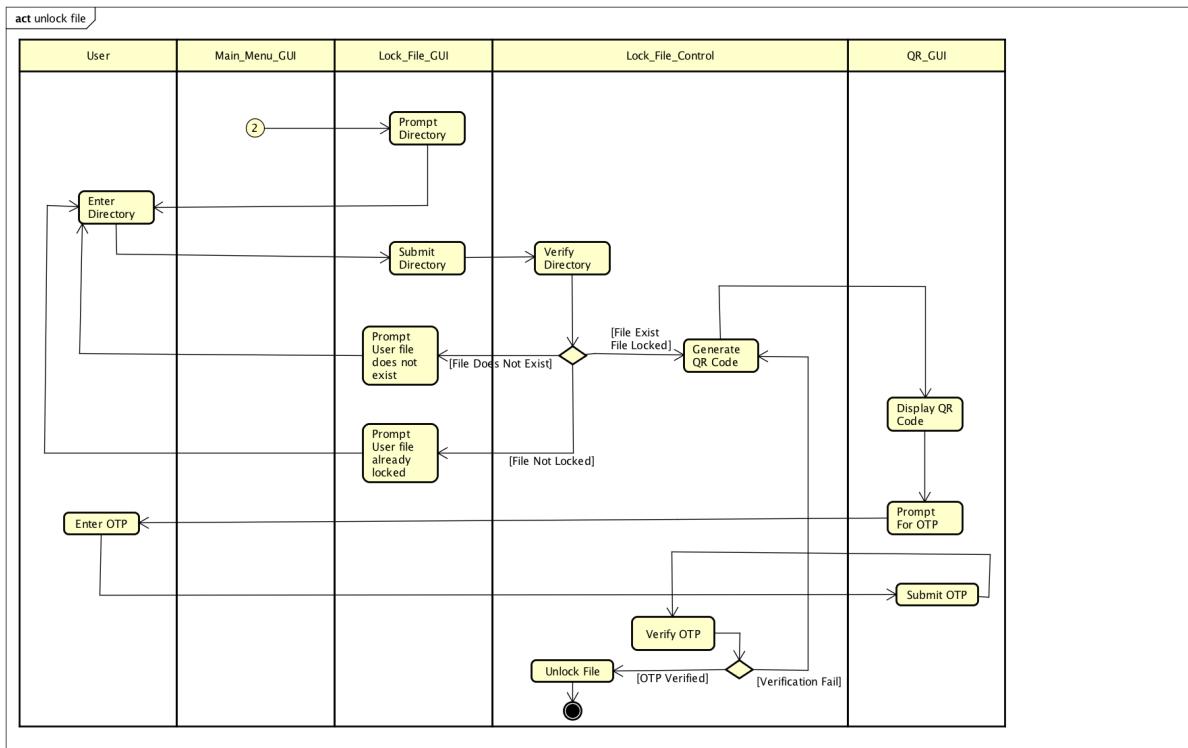


1.6 Unlock

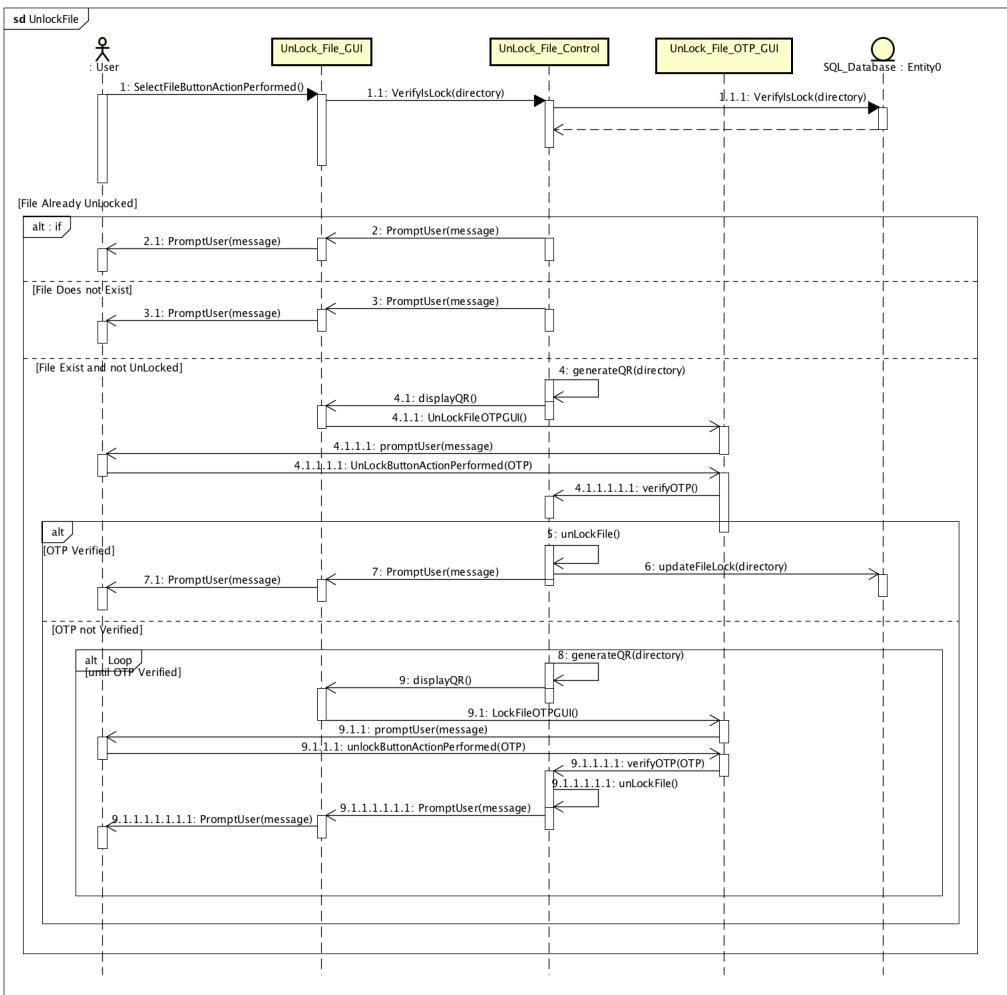
Use Case

Use Case Textual Description	
UC-ID	1.6
Name	Unlock
Description	To allow user to unlock their folders or files using system cryptography feature
Actor(s)	User
Precondition	The user has a registered account and logged into the system
Main Scenario	<p>Step 1: User selects Unlock file option in the Main Menu.</p> <p>Step 2: System displays a form to fill up the directory</p> <p>Step 3: User enters the directory and system validates</p> <p>Step 3(alternate): If directory is invalid, an error message will display, and User will be redirected to form to fill up directory.</p> <p>Step 3(alternate): If the file in directory is not locked, an error message will display, and User will be redirected to form to fill up the correct directory</p> <p>Step 4: The system unlocks the file <u>via U/C 1.6.1 UnlockFile</u></p>

Activity Diagram



Sequence Diagram

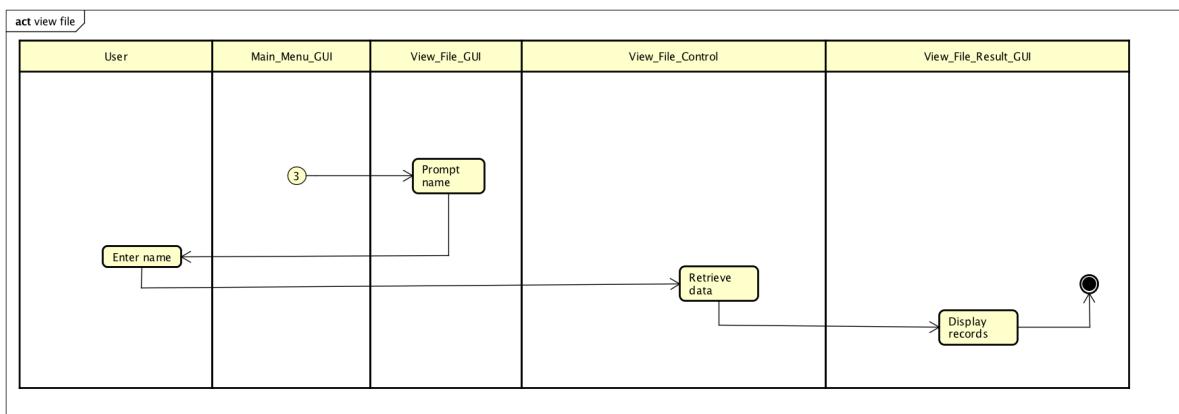


1.7 View File

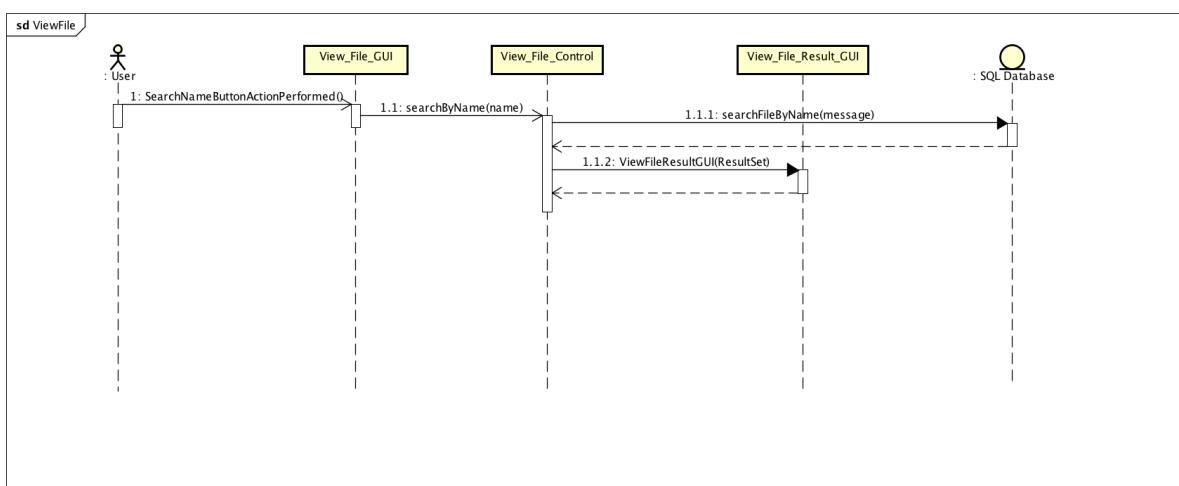
Use Case

Use Case Textual Description	
UC-ID	1.7
Name	View File
Description	To allow user to view the locked files in the system
Actor(s)	User
Precondition	The user has a registered account and logged into the system
Main Scenario	<p>Step 1: User selects View File option in the Main Menu</p> <p>Step 2: System will display a prompt to User to choose viewbyname option</p> <p>Step 3(viewbyname): User enters a date from where he locked a file and system validates via U/C 1.7.1 View File By File Name</p> <p>Step 3(alternate): if the name the User entered does not contain any locked file, the system will display an error message and prompt the User to enter a valid name.</p> <p>Step 4: When name is validated, system will retrieve the data and display the data of the file in its current status</p>

Activity Diagram



Sequence Diagram

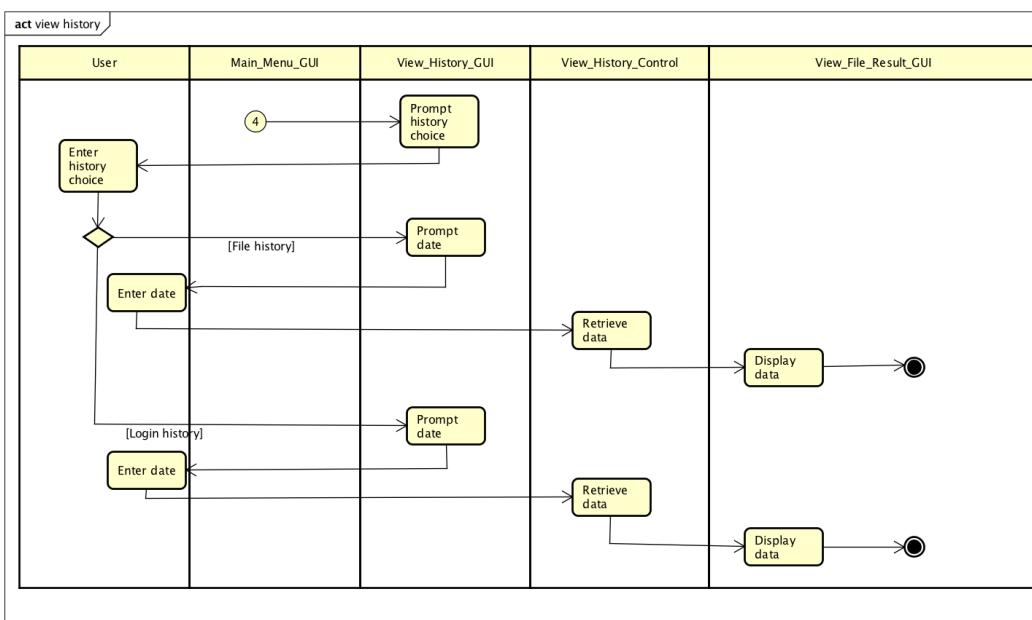


1.8 View History

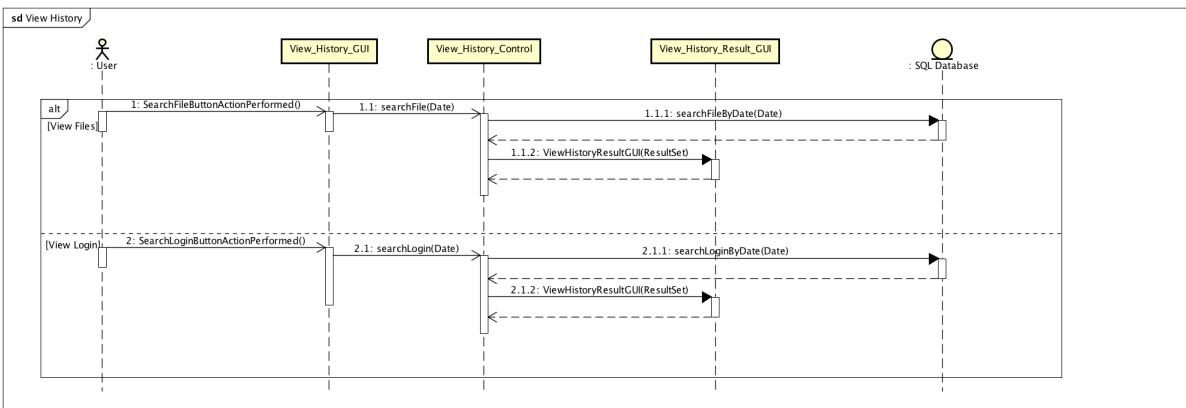
Use Case

Use Case Textual Description	
UC-ID	1.8
Name	View History
Description	To allow user to view history of log in and file
Actor(s)	User
Precondition	The user has a registered account and logged into the system
Main Scenario	<p>Step 1: User selects View History option in the Main Menu</p> <p>Step 2: User selects a choice in the view history menu</p> <p>Step 3: System will display a prompt to User to choose from View File History or View Login History</p> <p>Step 4(viewfilehistory): User enters a date via U/C 1.8.2 View File History</p> <p>Step 4(viewloginhistory): User enters a date via U/C 1.8.1 View Login History</p> <p>Step 5: System will retrieve the data and display the data to the User from the date User input consisting of past actions done by user regardless of current file status.</p>

Activity Diagram



Sequence Diagram



1.9 Change Registered Mobile

Use Case

Use Case Textual Description	
UC-ID	1.9
Name	Change Registered Mobile
Description	To allow user to change their registered mobile
Actor(s)	User
Precondition	The user has a registered account and lost or misplaced phone
Main Scenario	Step 1: User selects Change Registered Mobile at Main Menu Step 2: System prompts user to confirm the change of registered mobile Step 3: Once confirmed, the IMEI of the user mobile will be reset, and user will need to log in with new mobile to register the unique identifier.

Activity Diagram

Sequence Diagram

2.1 Delete User

Use Case

Use Case Textual Description	
UC-ID	2.1
Name	Delete User
Description	To allow the administrator to delete users from database
Actor(s)	Administrator
Precondition	The administrator wishes to delete off unused accounts
Main Scenario	Step 1: Administrator selects delete user on Main Menu Step 2: System prompts to enter username of the account that is to be deleted Step 3: Administrator fills up form and system validate Step 3(alternate): If username is invalid, an error message will be displayed, and Administrator is sent back to form for re-entry of right credentials Step 4: System will prompt to confirm username Step 5: Administrator re-enter username of the account to be deleted Step 6: System validates Step 7: System deletes username from database

Activity Diagram

Sequence Diagram

2.2 Account Recovery

Use Case

Use Case Textual Description	
UC-ID	2.2
Name	Account Recovery
Description	To allow Administrator to recover their lost or forgotten account
Actor(s)	User
Precondition	The Administrator has registered account and forgotten password
Main Scenario	Step 1: Administrator selects account recovery on Log in screen Step 2: System prints out a form to prompt for Administrator account email Step 3: Administrator fills up the email and system do validation Step 3(alternate): If email is invalid, an error message will be displayed, and Administrator is sent back to form for re-entry of right credentials Step 4: System will generate new password Step 5: Email with new generated password will be sent to Administrator email address.

Activity Diagram

Sequence Diagram

3.1 Login

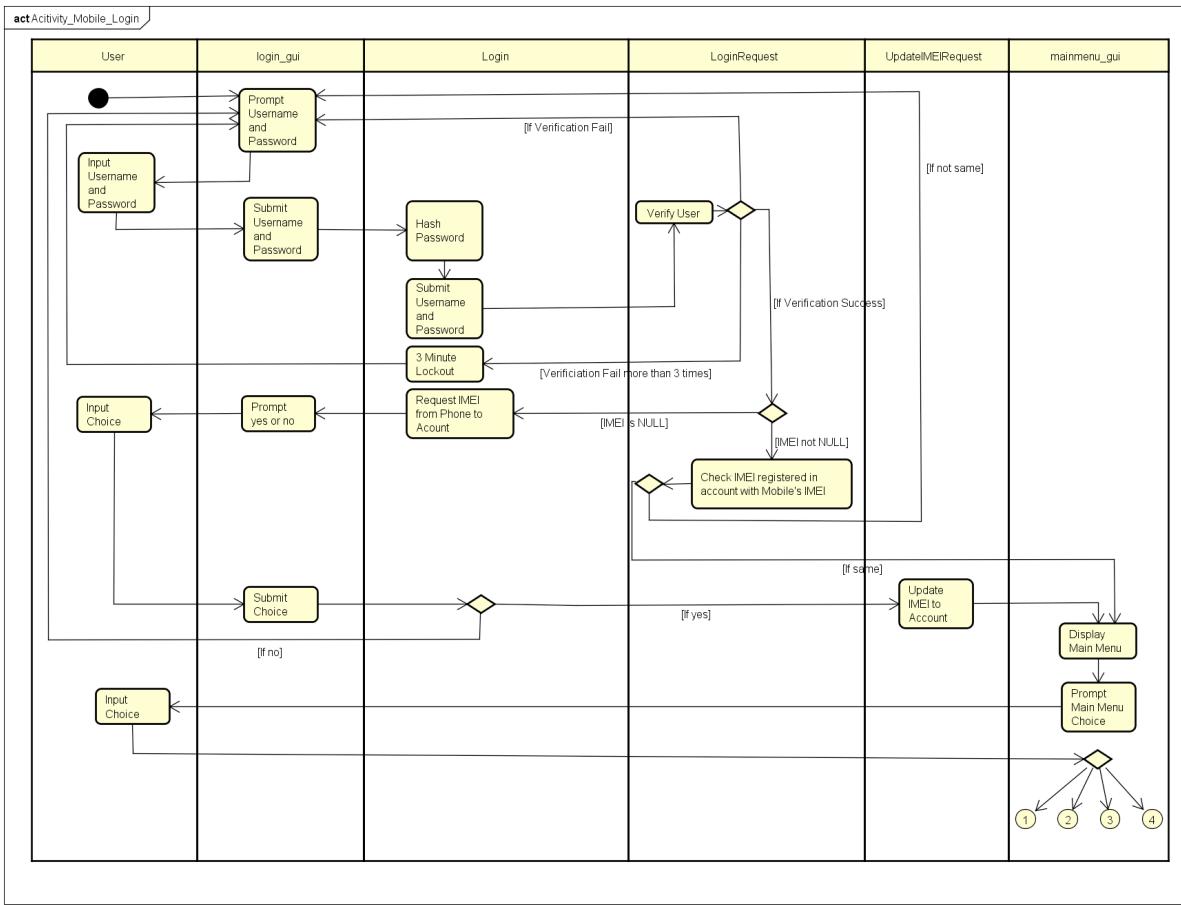
Use Case

Use Case Textual Description	
UC-ID	3.1
Name	Login
Description	To allow User to log in to the system
Actor(s)	User
Precondition	User wants to use the system
Main Scenario	<p>Step 1: User enters their log in credentials in the log in screen</p> <p>Step 2: System hash the User password and validates with SQL Database</p> <p>Step 2(alternate): If invalid log in credentials, an error message will display, and User will be prompt to enter credentials again</p> <p>Step 2(alternate): If log in credentials is wrong for 3 times, system will be lock from User for 3 minutes <u>via U/C 3.1.1 System Lockout</u></p> <p>Step 3: System will display Main Menu</p>

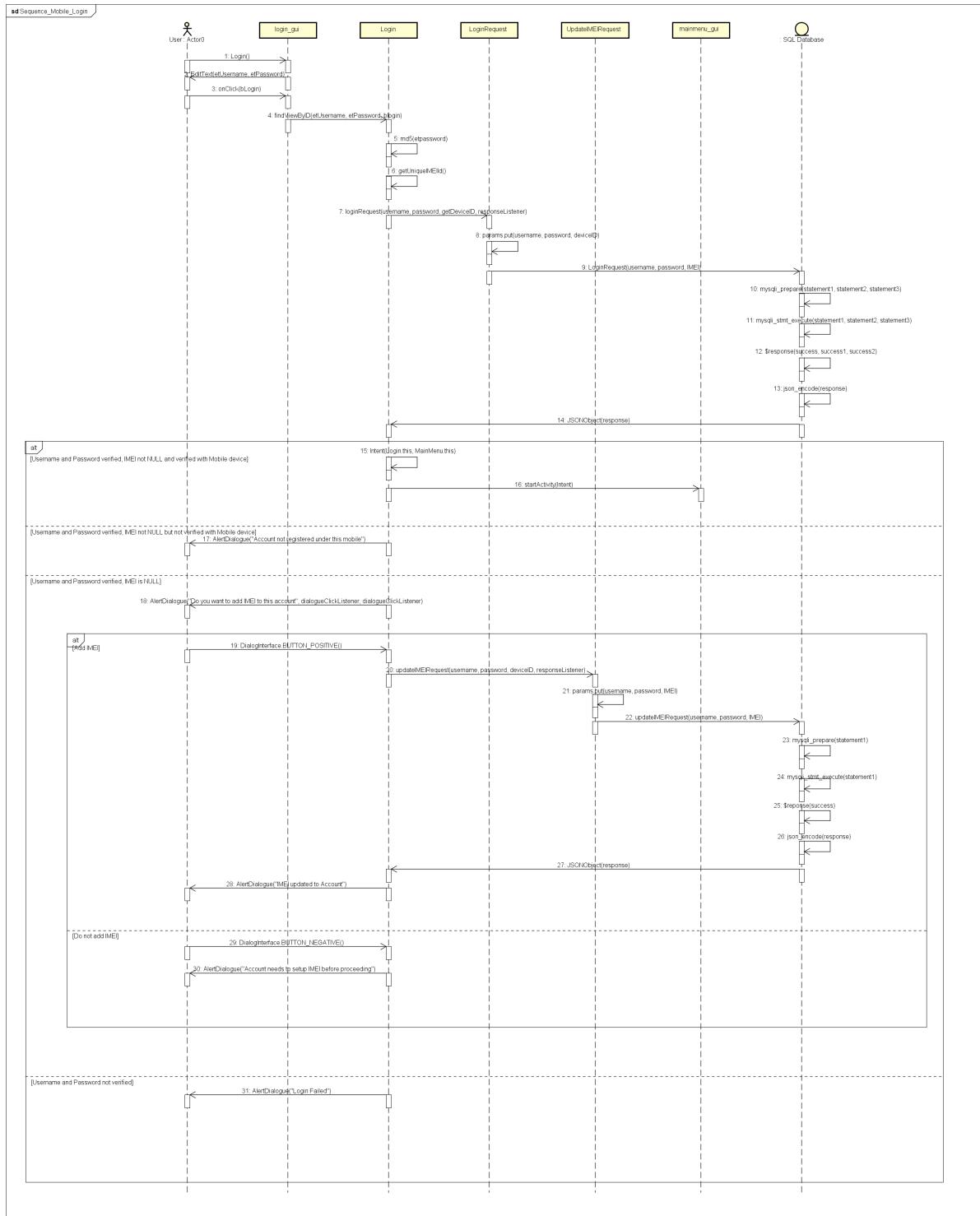
Use Case Textual Description	
UC-ID	3.1.1
Name	System Lockout
Description	Lock User out after several failed log in attempts
Actor(s)	User
Precondition	The user has 3 failed log in attempts
Main Scenario	<p>Step 1: System will lock the user out of the system for 3 minutes</p> <p>Step 2: System will resume after 3 minutes.</p>

Use Case Textual Description	
UC-ID	3.1.2
Name	Update IMEI
Description	Updates to IMEI of user mobile to database record for unique identifier
Actor(s)	User
Precondition	The user has created an account on computer and first time log in on mobile
Main Scenario	<p>Step 1: After user has logged in, the system will prompt user for choice to register mobile with the account.</p> <p>Step 2(alternate): User selects yes and system will automatically capture the IMEI number of the mobile.</p> <p>Step 2(alternate) User selects no and the system will return to login page.</p>

Activity Diagram



Sequence Diagram



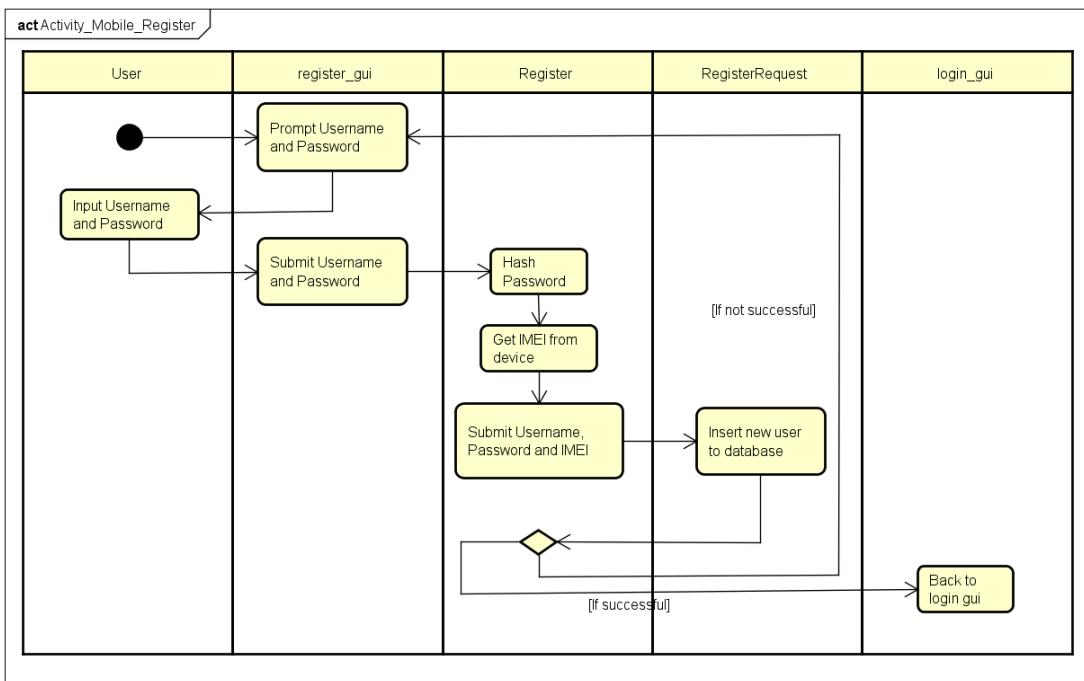
3.2 Register Account

Use Case

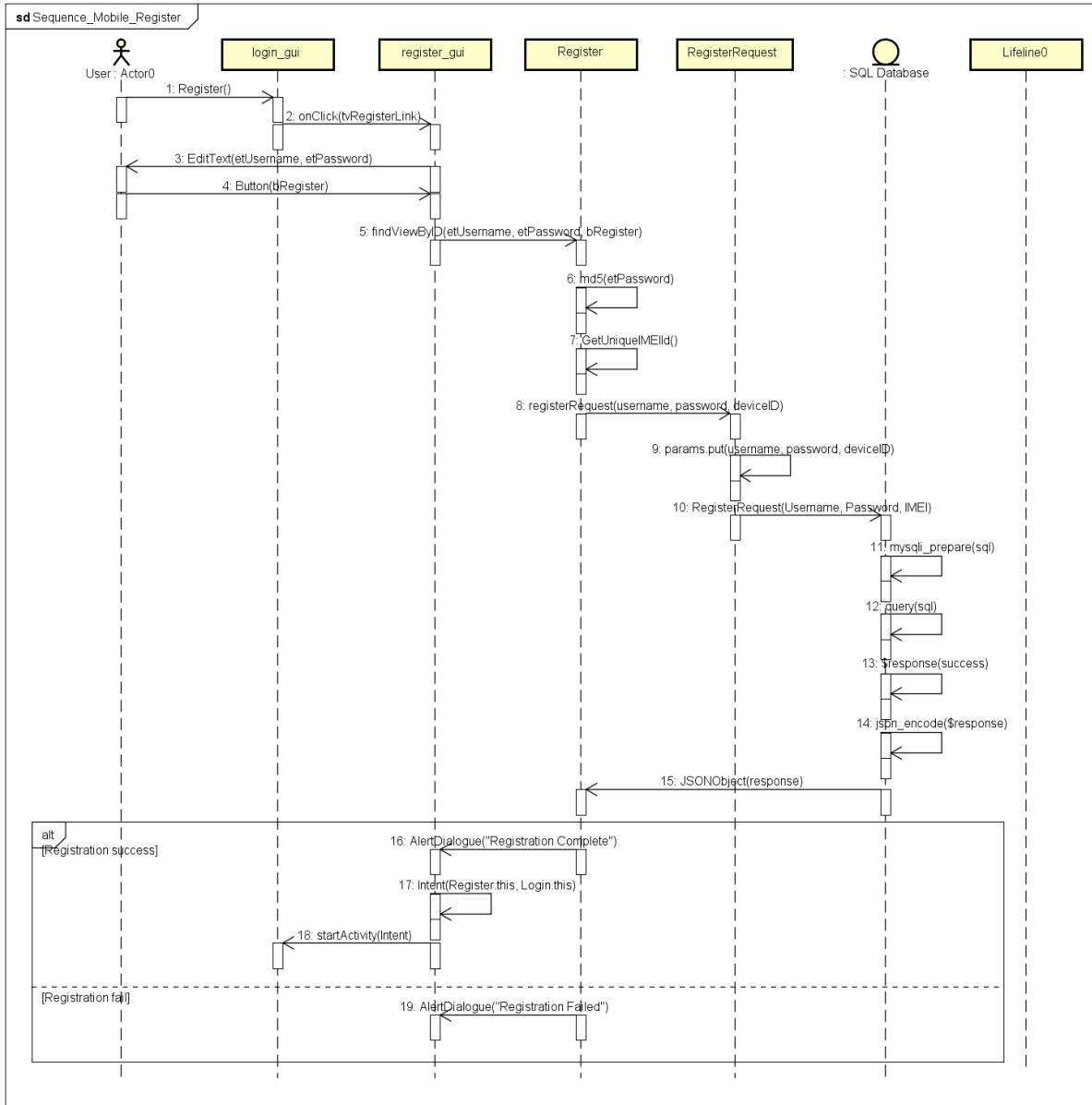
Use Case Textual Description	
UC-ID	3.2
Name	Register Account
Description	To allow user to register new account after he download the application for the first time
Actor(s)	User
Precondition	A user has installed the application and wish to create a new account
Main Scenario	<p>Step 1: System display a User Interface with fields to ask for user email address and desired password</p> <p>Step 2: User submits form and system does validation</p> <p>Step 2(alternate): If data is invalid, an error message will be displayed, and user is sent back to form for re-entry of right credentials</p> <p>Step 3: User password will be hashed</p> <p>Step 4: System captures IMEI via U/C 3.2.1 Register IMEI</p> <p>Step 5: System updates the SQL Database</p> <p>Step 6: User is redirected to log in screen</p>

Use Case Textual Description	
UC-ID	3.2.1
Name	Register Unique Identifier
Description	To allow system to register a unique identifier of user for log in
Actor(s)	User
Precondition	The user has registered an account and system will need to capture user's unique identifier (IMEI number)
Main Scenario	Step 1: After user has created account, system will automatically capture the IMEI number of user mobile

Activity Diagram



Sequence Diagram

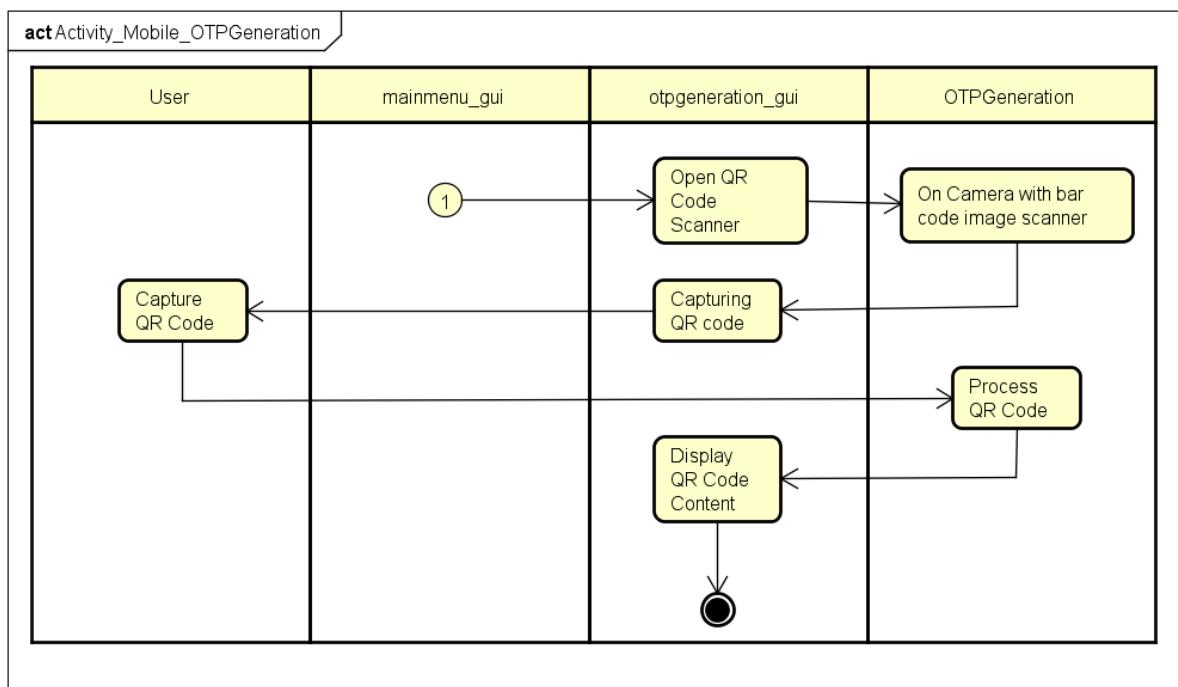


3.3 OTP Generation

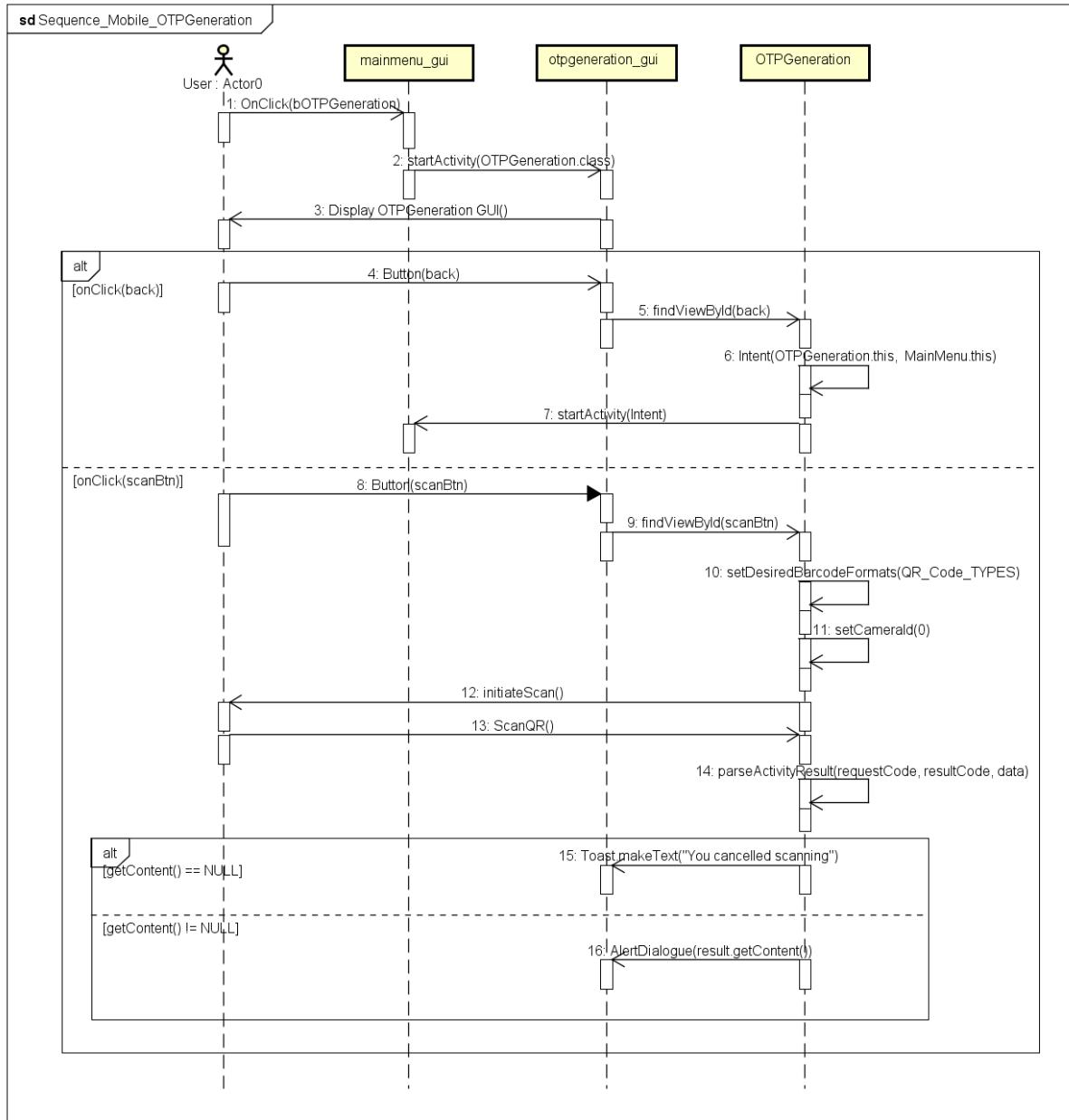
Use Case

Use Case Textual Description	
UC-ID	3.3
Name	OTP Generation
Description	Generate OTP from QRCode upon scanning
Actor(s)	User
Precondition	The user wants to lock or unlock a file and has to key in the OTP on computer
Main Scenario	<p>Step 1: When the user chooses to lock or unlock a file on his computer, a QRCode will be generated</p> <p>Step 2: User will then use his mobile application function to generate the OTP from the QRCode generated via U/C 3.3.1 Scan QR Code</p>

Activity Diagram



Sequence Diagram

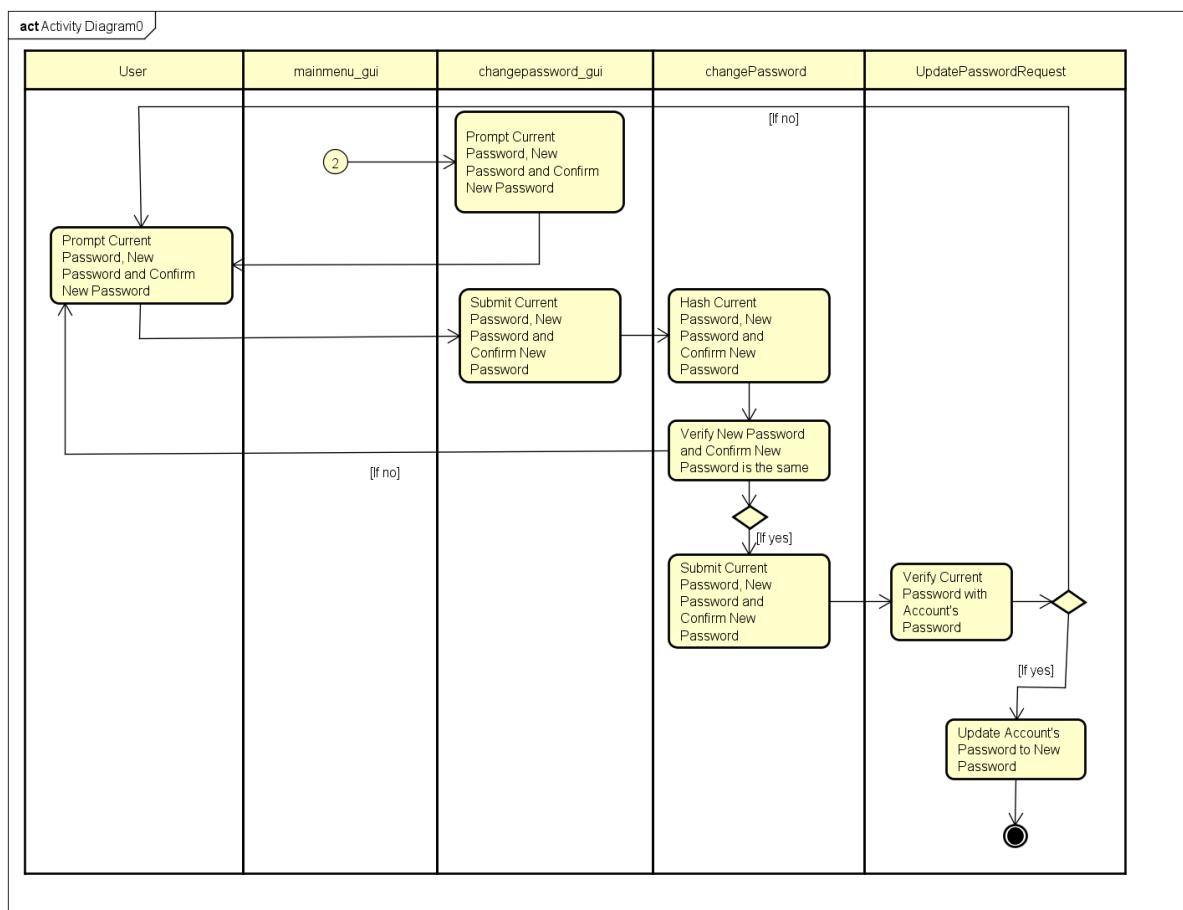


3.4 Change Password

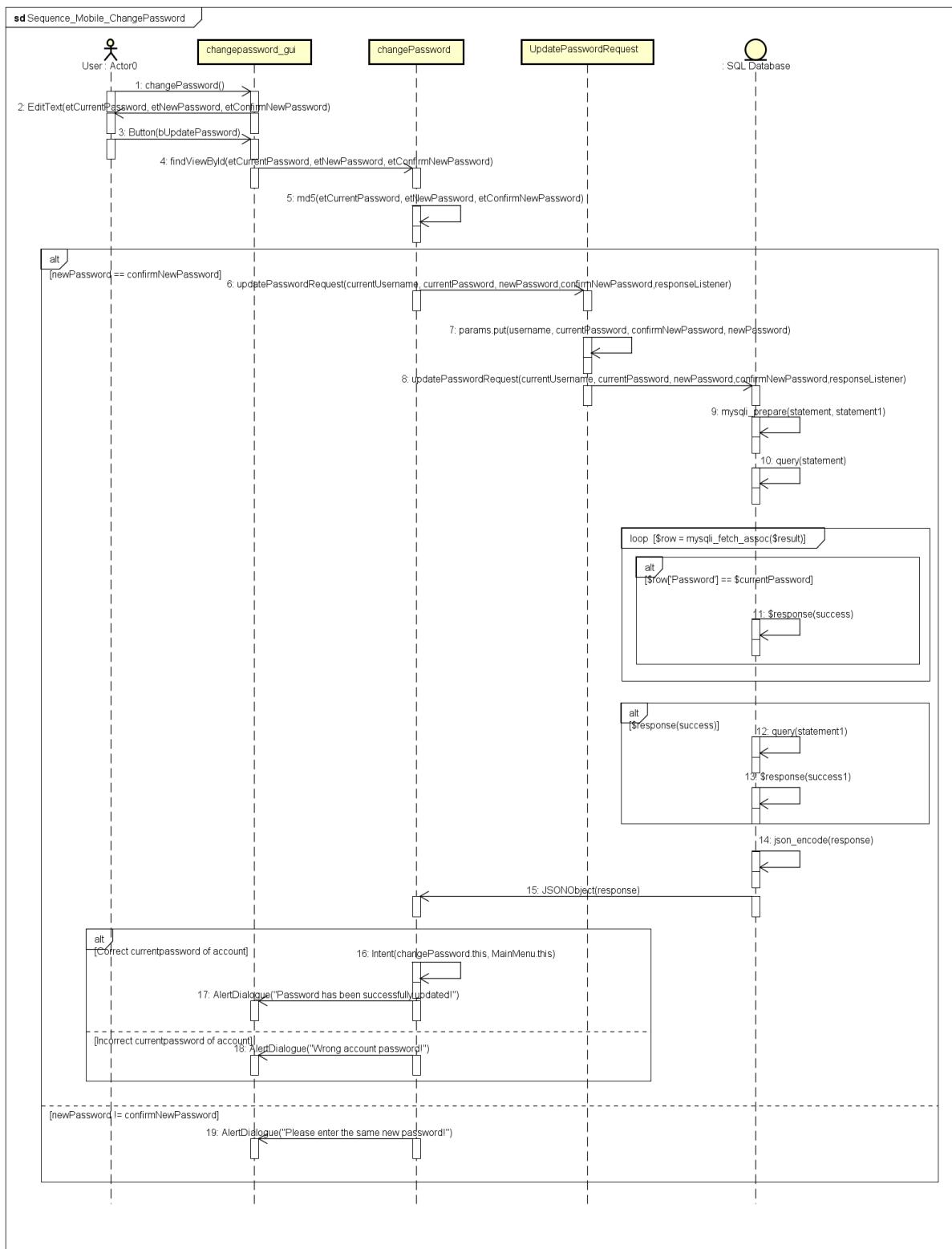
Use Case

Use Case Textual Description	
UC-ID	3.4
Name	Change Password
Description	To allow User to change their password
Actor(s)	User
Precondition	User wants to change existing password to a new one
Main Scenario	<p>Step 1: User enters username and password at Log in screen</p> <p>Step 2: User selects change password at the main menu</p> <p>Step 3: System displays a form for user to fill up the new password they desire</p> <p>Step 4: User enters the new desired password and system do validation</p> <p>Step 5: System will update the SQL Database with the new password</p>

Activity Diagram



Sequence Diagram



3.5 Account Recovery

Use Case

Use Case Textual Description	
UC-ID	3.5
Name	Account Recovery
Description	To allow user to recover their lost or forgotten account
Actor(s)	User
Precondition	The user has a registered account and forgotten password
Main Scenario	<p>Step 1: User selects account recovery on Log in screen</p> <p>Step 2: System prints out a form to prompt for User account email</p> <p>Step 3: User fills up the email and system do validation</p> <p>Step 3(alternate): If email is invalid, an error message will be displayed, and user is sent back to form for re-entry of right credentials</p> <p>Step 4: System will generate new password</p> <p>Step 5: System will send an email with new generated password to the register email address</p>

Activity Diagram

Sequence Diagram

3.6 Change Registered Computer

Use Case

Use Case Textual Description	
UC-ID	3.6
Name	Change Registered Computer
Description	To allow user to change their registered computer
Actor(s)	User
Precondition	The user has a registered account and lost or misplaced computer
Main Scenario	Step 1: User selects Change Registered Mobile at Main Menu Step 2: System prompts user to confirm the change of registered mobile Step 3: Once confirmed, the MAC Address of the user computer will be reset, and user will need to log in with new mobile to register the unique identifier.

Activity Diagram

Sequence Diagram

4. External Interface Requirements

4.1 Hardware Interfaces

The hardware mainly consists of the PC which the user use to lock and unlock their files and a mobile phone with android operating system. Mobile phone must be equipped with a working camera.

4.2 Software Interfaces

The user will install the application on their mobile device from Android Play Store and PC application will be installed from the website of go2FA.

Recommended System Requirements		
	Windows	Macintosh
Connectivity	Wi-Fi 802.11 a/b/g/n/ac)	Wi-Fi 802.11 a/b/g/n/ac)
Operating System	Windows OS (e.g. Windows XP, Windows Vista, Windows 7, Windows 10)	• Mac OS (e.g. Mac OS X or above)
RAM	1GB	1GB

Recommended System Requirements	
	Android
Connectivity	Wi-Fi 802.11 a/b/g/n/ac), Internet Connection(3G/4G)
Operating System	Android Version 6.0 (Marshmallow) and above
RAM	1GB

5. Non-functional Requirements

5.1 Performance Requirements

Upon log in, user credentials will be stored locally to minimise communication overhead with the central database.

5.2 Safety Requirements

Changing Password

The user can change the password by providing the current password and the new password will be updated to the central database.

Password Recovery

If the user forgets his password, the system will generate a new password upon request, and send via email to the user

Multiple Logins

When a user is log in, other instances of logging in with the same username will not be able to successfully log in.

5.3 Security Requirements

5.4 Software Quality Attributes

References

Appendix A: Glossary