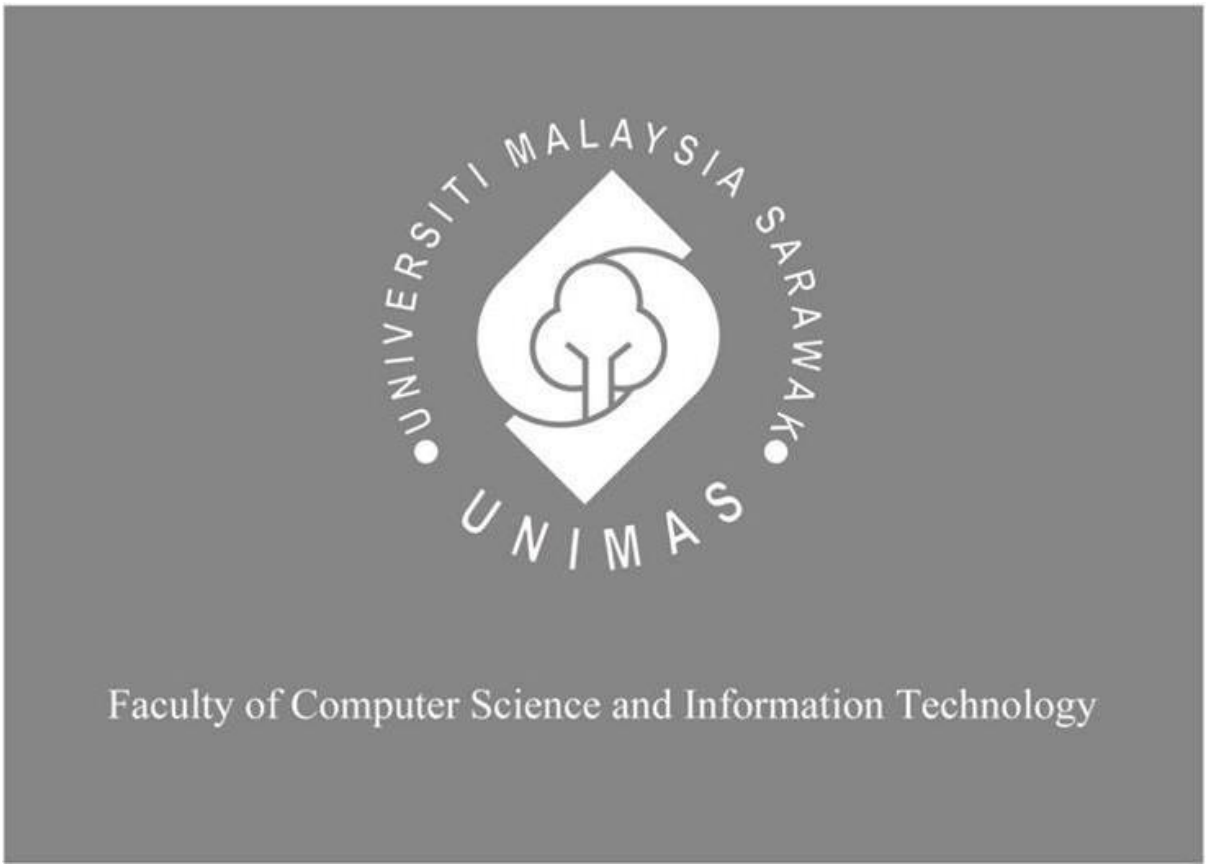


NOTEPAD ANDROID APPLICATION WITH BIOMETRIC FINGERPRINT LOCK (NOTEY)

Emmaryna anak Irie

Bachelor of Computer Science with Honours

(Software Engineering)

2019

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE NOTEPAD ANDROID APPLICATION WITH BIOMETRIC FINGERPRINT LOCK (NOTEY)

ACADEMIC SESSION: 2019/2020

EMMARYNA ANAK IRIE

(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

☐	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
☐	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
☑	UNRESTRICTED	

(AUTHOR'S SIGNATURE)

Permanent Address

NANGA BAN ILI, KM 4
JALAN TANJUNG ASSAM,
95700 BETONG, SARAWAK

Date: 10th AUGUST 2020

Validated by

(SUPERVISOR'S SIGNATURE)

WEE BUI LIN
Senior Lecturer
Software Engineering Programme
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak

Date: 10 / 8 / 2020

Note * Thesis refers to PhD, Master, and Bachelor Degree
** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

ACKNOWLEDGEMENT

Throughout the completion of this final year project 1, there are so many people I want to thank for their direct and indirect contributions to this project.

First and foremost, I would like to dedicate my special thanks to my supervisor, Miss Vanessa Wee Bui Lin for her professional advice and guidance on this project. I really appreciate the encouragement and useful critiques which have been a great help in my research and thesis writing. As a supervisor, she has done a good job in sharing her knowledge and motivating me.

Next, I wish to acknowledge the help from my fellow peers and colleagues who are taking along the final year project 1 with me in the final year. I am thankful for their willingness to share useful information and essential knowledge about the final year project.

Not to forget my precious family members, mom, dad, and my brother who always be there for me for mental support and encouragement throughout my years of study in UNIMAS. I am so lucky to have such amazing family that always pray for my success in life.

Finally, I am particularly grateful to those who helped me with data collections especially the respondents who have spent their valuable time to participate in every survey conducted. Their co-operation in the data collections were greatly and highly appreciated. This project would have been impossible without their help.

ABSTRACT

This paper is to develop a notepad Android application with biometric fingerprint lock. Biometric lock within applications in mobile devices is the latest security features that operates with the hardware that can scan the biometric of a person in order to access a confidential information. There are some applications that has implemented biometric lock, and among the listed are notepad application. This paper describes the evaluation of security of biometric lock on the notepad application as well as developing a notepad application embedding biometric lock in it.

ABSTRAK

Laporan kajian ini adalah untuk membangunkan aplikasi notepad Android dengan menggunakan kunci cap jari biometrik sebagai keselamatan aplikasi tersebut. Penggunaan kunci cap jari biometrik di dalam aplikasi teknologi mudah alih merupakan ciri keselamatan terkini yang beroperasi dengan perkakasan yang boleh mengimbas biometrik seseorang untuk mengakses maklumat yang sulit. Terdapat beberapa aplikasi yang telah menggunakan kunci biometrik, dan antara yang disenaraikan adalah aplikasi notepad. Makalah ini menerangkan penilaian keselamatan kunci biometrik pada aplikasi notepad serta membangun aplikasi notepad yang memasukkan kunci biometrik di dalamnya.

TABLE OF CONTENTS

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Introduction

Mobile users today like to keep their information online and in their own device, such as pictures, videos, mails, messages, and many more. Most of the time the user will save their login information in the application itself after they log out. Some applications have this kind of features such as Instagram, Facebook, Twitter and many other kinds of application. This feature is beneficial for users as they will only need to go to the application in one tap, but the downside of it is that anyone can access the pre-filled login form and access them without the user's permission. Jotting down the passwords and its correlative emails or usernames on paper can be messy and the risk for it to be lost is high. Typing down the information in notepad application in mobile proved to be easier and eco-friendly, but it also has its own risk of being discovered.

The purpose of this project is to enhance the current notepad application with biometric fingerprint lock along with key-in password, where the user can safely store their information in the application.

1.2 Problem statement

A few problems have been encountered during the research of some similar applications with the security feature. Firstly, the current software application only limited to password on screen, which can be cracked by some users other than the main user of the device. Since the fingerprints leave some prints on the screen regardless of the surface, the other users can track down the password of the device by trial-and-error.

Other than that, the current software only applied a one-time password after unlocking the application on start-up or after viewing one of the notes. After the user enters the password one time, the user will gain full access for the notes inside the application without another

authentication being engaged whenever the user opens one of the notes. This might prove a bit unsafe as the notes are vulnerable being taken by any unauthorised user on the device.

Furthermore, the login information saved in some applications in the device allows anyone to access the pre-filled login form of the application without the permission form the device's owner. To save some log-in time, some social media applications enabled the login form to be pre-filled with the email of the owner, this can be problematic if the other users know the right combination of email and password of the account simply by looking at the email at the login screen.

1.3 Objective

The main objective of this project is to develop a biometric security feature for current notepad application to enhance data protection by reducing unauthorised access to the files. Some other objectives for this project are:

a) To develop an application for recording and securing the notes at the same time in local storage;

b) To evaluate the security features for both biometric and passwords protection added onto the file for this application.

1.4 Brief methodology

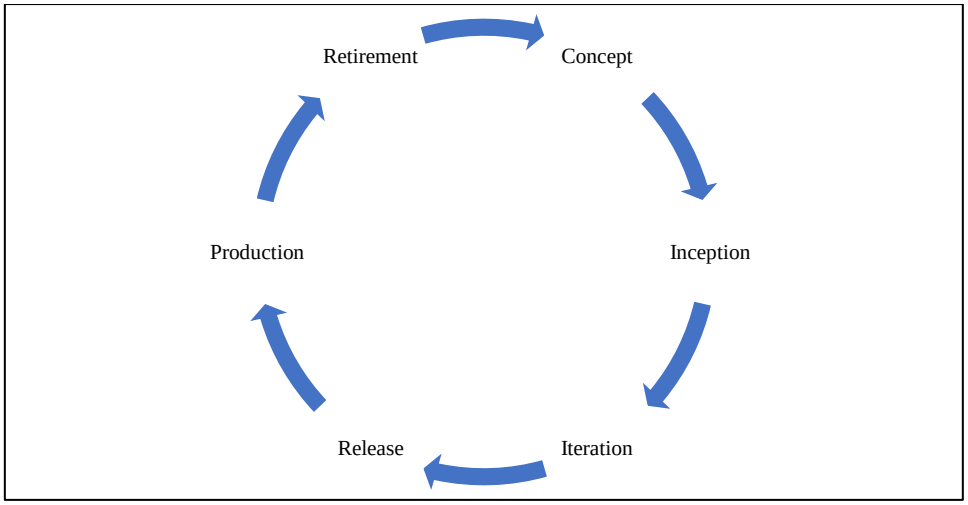


Figure 1.0: Agile methodology phases

The methodology used for this project is agile methodology. Agile methodology is a practice that promotes continuous iteration of development and testing of the project (Guru99, 2019). Referring to Figure 1.0, there are six (6) phases of agile development:

1. Concept

   The concept phase will carry out the activities such as identify problems, understanding the environment of the project and research about the current solution of the project as well as the limitations of the solutions. Requirements gathering and analysis are also being carried out during this phase via questionnaire.

2. Inception

   The inception phase will carry out the designing activities such as planning the draft for the report and proposal as well as estimating the tasks for each activity to be carried out throughout the project. The task estimation will be drafted and included into the project schedule of this project.

3. Iteration

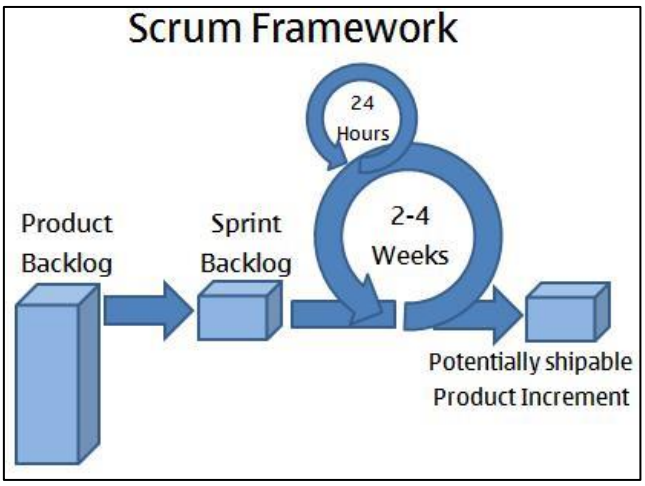


Figure 2.0 The Scrum process

The iteration phase will implement the Scrum iteration, as shown in figure 2.0 where daily meeting and sprints will be carried out. During this phase, designing the report, testing or checking for suitability of the documentation of the report and

implementation will be carried out. The sprint backlog will be the chapter submissions and the potential product of the sprint will be delivered at the end of the sprint, which is the chapters' documentation. Each sprint will be conducted in the range of one to two (1-2) weeks.

4. Release

   During this phase, the potential product will be reviewed and be given feedback based on the suitability of the chapter's content. The product will be finalised and will be released after the review is approved.

5. Production

   The production phase will carry out the submission of the chapters' documentation to the system to be reviewed and tracked by the admin and the examiner of the project. The feedbacks given by the examiner will be considered and will begin another iteration phase until the end of FYP 1. This phase will end after the retirement phase being scheduled.

6. Retirement

   In this phase, the retirement of the documentation is the final submission of the FYP 1 report to the system.

1.5 Scope

The scope of this system is limited to the device that has been embedded with fingerprint pad. Other than that, the project focus at the users that records and saves their notes in written text form, such as password records, email names, bank account numbers or any other confidential information deemed by the user into the note and to secure it properly. Other than that, this project will focus on enhancing the security features of the notepad application.

1.6 Significance of project

The significance of this project is to help the users to secure and protect their important notes that has been entered inside the notepad application. This can safely protect the confidential information from any inside and outside threat of the application by embedding an additional security measure. The application can only be unlocked by the owner of the device since the device has the record of the owner's fingerprint. Information such as passwords, emails, bank accounts or other confidential information can be securely kept in the application. This project can always be accessible to the owner of the device without worry too much about forgetting the written password.

1.7 Project schedule

Figure 3.0 and figure 4.0 below shows the project schedule of Final Year Project for semester 2 2019/2020.

ID	Task Mode	Task Name	Duration	Start	Finish
1		Final Year Project	237 days	Fri 20/9/19	Sat 15/8/20
2		Prepare full proposal	21 days	Sun 22/9/19	Fri 18/10/19
3		Milestone project proposal complete	0 days	Sat 19/10/19	Sat 19/10/19
4		Prepare Chapter 1	6 days	Sun 20/10/19	Fri 25/10/19
5		Milestone Chapter 1 Introduction submission	0 days	Sat 26/10/19	Sat 26/10/19
6		Requirement analysis and iteration	39 days	Mon 21/10/19	Thu 12/12/19
7		Sprint 1			
8		Gather and analyse requirements by questionnaire	6 days		
9		Prepare Chapter 2	16 days		
10		Milestone Chapter 2 Literature Review submission	0 days	Sat 16/11/19	Sat 16/11/19
11		Sprint 2	17 days	Wed 13/11/19	Thu 5/12/19
12		Prepare Chapter 3	16 days		
13		Milestone Chapter 3 Requirement Analysis and Design submission	0 days	Thu 5/12/19	Thu 5/12/19
14		Sprint 3	5 days	Fri 6/12/19	Thu 12/12/19
15		Compile Chapter 1, Chapter 2 and Chapter 3	5 days		
16		Milestone FYP1 report submission	0 days	Thu 12/12/19	Thu 12/12/19
17		Development and Testing	172 days	Fri 20/12/19	Sat 15/8/20
18		Unforseen emergency	69 days	Mon 16/3/20	Thu 18/6/20

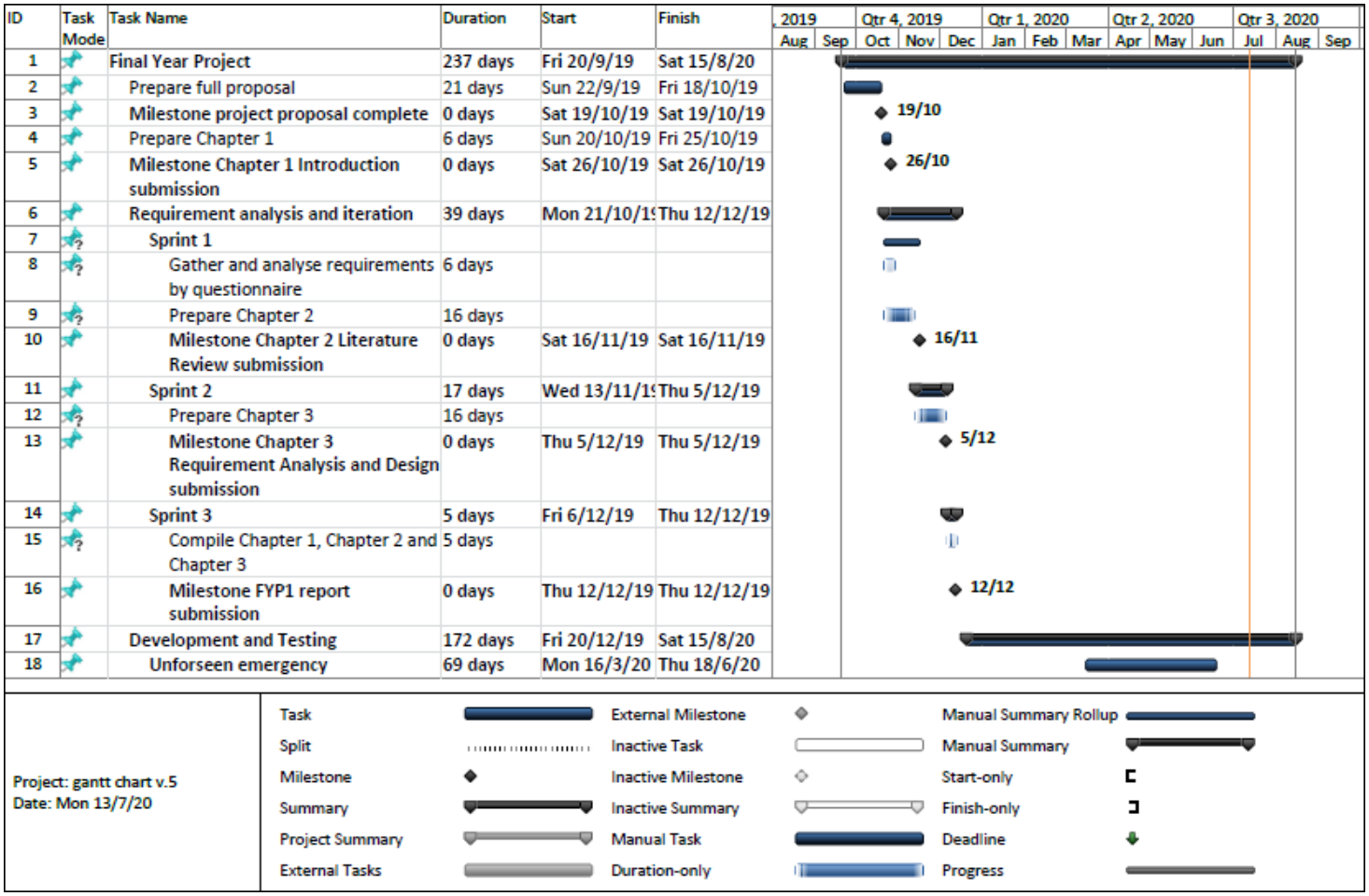
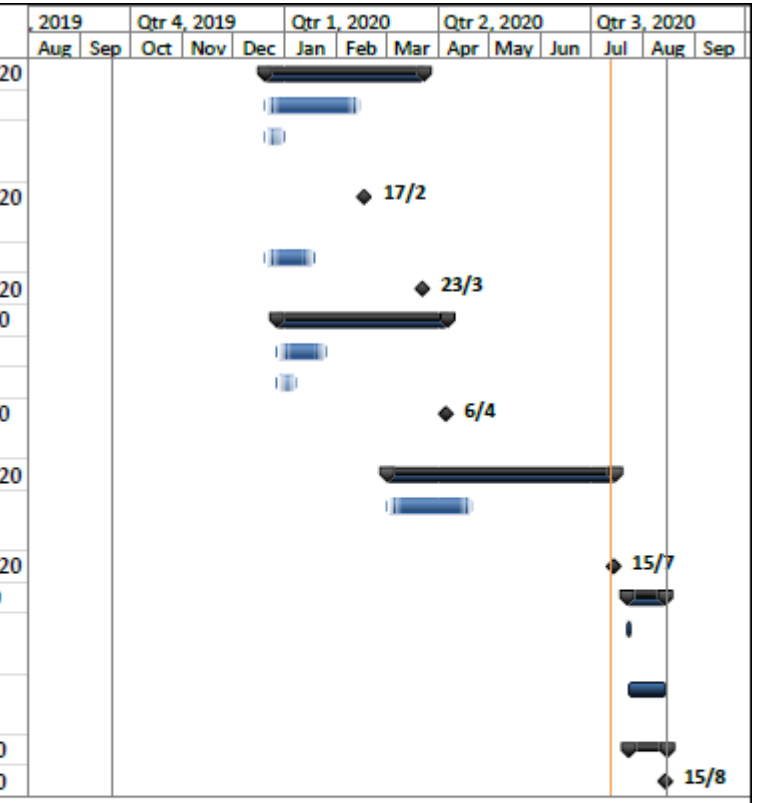


Figure 3.0: Gantt chart part 1

ID	Task Mode	Task Name	Duration	Start	Finish
19		Sprint 1	67 days	Fri 20/12/19	Mon 23/3/20
20		Initial development of project	40 days		
21		Modification of project's Gantt Chart	7 days		
22		Milestone revised structure and updated Gantt Chart	0 days	Mon 17/2/20	Mon 17/2/20
23		Prepare Chapter 4	21 days		
24		Milestone Chapter 4	0 days	Mon 23/3/20	Mon 23/3/20
25		Sprint 2	72 days	Fri 27/12/19	Mon 6/4/20
26		Prepare Chapter 5	21 days		
27		Prepare abstract for paper	7 days		
28		Milestone Chapter 5 and abstract for paper	0 days	Mon 6/4/20	Mon 6/4/20
29		Sprint 3	98 days	Mon 2/3/20	Wed 15/7/20
30		Prepare final report, user manual, paper for assessment	36 days		
31		Milestone Final report (draft)	0 days	Wed 15/7/20	Wed 15/7/20
32		Sprint 4	17 days	Thu 23/7/20	Fri 14/8/20
33		Presentation of project's prototype	2 days	Thu 23/7/20	Fri 24/7/20
34		Amendment and modification for final report	16 days	Fri 24/7/20	Fri 14/8/20
35		Sprint 5	17 days	Fri 24/7/20	Sat 15/8/20
36		Milestone of final report	0 days	Sat 15/8/20	Sat 15/8/20



Project: gantt chart v.5
Date: Mon 13/7/20

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	

Figure 4.0 Gantt chart part 2

1.8 Expected outcome

Few results are to be expected from the system. Firstly, the notepad application developed with the biometric lock enhancement will be able to function normally in the device that has been embedded with fingerprint pad. Next, the application will be able to protect the confidential information in the notepad application with the proposed feature. The application is user-friendly to the user, hence there is no need of training to use it. Finally, the system will be expected to have a higher level of security than the current note application.

1.9 Project outline

Chapter 1 covers the introduction of the proposed system, Notepad Application with Biometric Fingerprint Lock. The first phase of agile methodology, and requirement analysis takes place in this chapter. This chapter basically provides the overview of the whole project including the introduction of the current note application, problems that trigger the development of the proposed system, the objectives to be achieved upon the completion of the project, methodology used to assist the development processes, scope or limitations of the proposed system and the significance of the project to user.

Chapter 2 describes the literature review done on existing systems which are similar to the proposed system. This chapter is done by reviewing articles, journals and other research papers. These reference papers are used to gather the information about the background of the current system such as the implementation of biometric into hardware devices.

Chapter 3 explains more about how requirements analysis and design are done for the system development. In this project, several diagrams are used to represent the user diagrams and the flow of process of the application.

Chapter 4 shows a full description of the proposed system. The structure of the system is illustrated using screenshots from the actual application run and the configuration of the interface.

Chapter 5 is where the system testing is conducted. The features of the system will be evaluated to enhance the performance. Testing is done to measure the system's effectiveness, performance and debugging any errors in the system.

Chapter 6 concludes the plan as a whole and discusses the future works of the system. Recommendations and suggestions for possible improvements in the future will be given based on the test results in the previous chapter.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In a literature review, similar existing system to the proposed system will be reviewed as well as the tools and technology for the proposed system. There are a few existing systems that are similar to proposed system in terms of its functionality and the features within the system have been selected to be reviewed in detail. A comparison table for the existing systems and the proposed system is created to easily understand the differences between the systems. A brief background of study will be explained further regarding the biometric authentication on handheld devices such as mobile phone. Other than that, a discussion on choosing the right tools and technology for the proposed system is also included.

2.2 Background of study

The background of study of this project will explain further about biometric authentication system and how it works on devices.

2.2.1 Biometric authentication system

Biometric authentication system or locking system uses only a part of the human body to be scanned on the scanner hardware. It is useful in terms of security measures as each biometric record can identify a specific person's access to the certain device embedded with the scanner, as every person has a different pattern of biometric of their body. Biometric authentication system is developed to lower the risk of individual's identity (Jain & Nandakumar, 2012). There are many types of biometric authentication on the human body, such as fingerprints, irises, face, the human DNA (Deoxyribonucleic Acid), ear patterns, hand and fingers geometry, retinal scanning, signature verification and voice recognition (Kumar & Ryu, 2009). Among all of these, fingerprint authentication is the most used authentication as it is easily accessible and easy to capture on the scanning hardware.

The biometric fingerprint authentication works in these steps (Kumar & Ryu, 2009):

1. A person's fingerprint will be scanned on the scanner hardware, scanning the ridges and the furrows of the user's fingers.
2. After a series of scanning the records will be stored in the database provided as the fingerprint of that person.
3. When in use of the system, the authentication might enter two modes, known as the verification mode or identification mode.
    a. Verification mode works on comparing the captured fingerprint that has been scanned with the one stored in the database. If the matching is successful, the authentication is open for that user. This mode emphasises with the question "Is this belong to this person?".
    b. Identification mode works where the system recognises the person by comparing their biometrics with the existing template in the database for a match. This mode emphasises with the question "Whose biometric data is this?".

To summarise, the verification mode uses positive recognition (to prevent multiple people using the same identity) while identification mode uses negative recognition (prevent a single person using multiple identity).

There are some pros and cons of biometric fingerprint authentication. One of the pros is that the fingerprint of a person is hard to fake (Verma, 2017). Since each person has their own unique set of fingerprint patterns, it is hard to copy the exact pattern as the original, thus the security is preserved. Other than that, fingerprint records requires very less database memory (Verma, 2017) as it only records the pattern bits of the ridges and furrows of the fingerprint. Another advantage of using fingerprint as biometric authentication is that it requires low implementation cost and easy to use and setup on devices such as mobile devices (Thakkar,

2019). According to Shoemaker (2018), biometric fingerprint authentication provides two-factor authentication, where the user have two kinds of passwords (fingerprint lock and onscreen password) set up on the device. One of the password will be the backup to another.

The cons of using biometric fingerprint authentication is having the risk of privacy infiltration, according to Shoemaker (2018). Once the hacker or any unauthorised user retrieves the fingerprint record, there is no saving the confidential records unless the administrator delete the database as to protect the privacy of the stolen user's fingerprints. The next on the list is the identification problem with old people's fingerprints or the fingerprint is not in an optimal condition for scanning (Thakkar, 2019). Other than that, the problem of user acceptance towards the biometric fingerprint authentication is still there (Verma, 2017). According to Verma (2017), the authentication method has high cost of maintenance when in the cast of the authentication has been jeopardised.

2.3 Reviews on similar existing systems

This section will review and explain about similar existing system as the proposed system. The review will cover some applications such as SecNotes, Safe Notes and Private Notes.

2.3.1 SecNotes notepad app (Skipser, 2013)

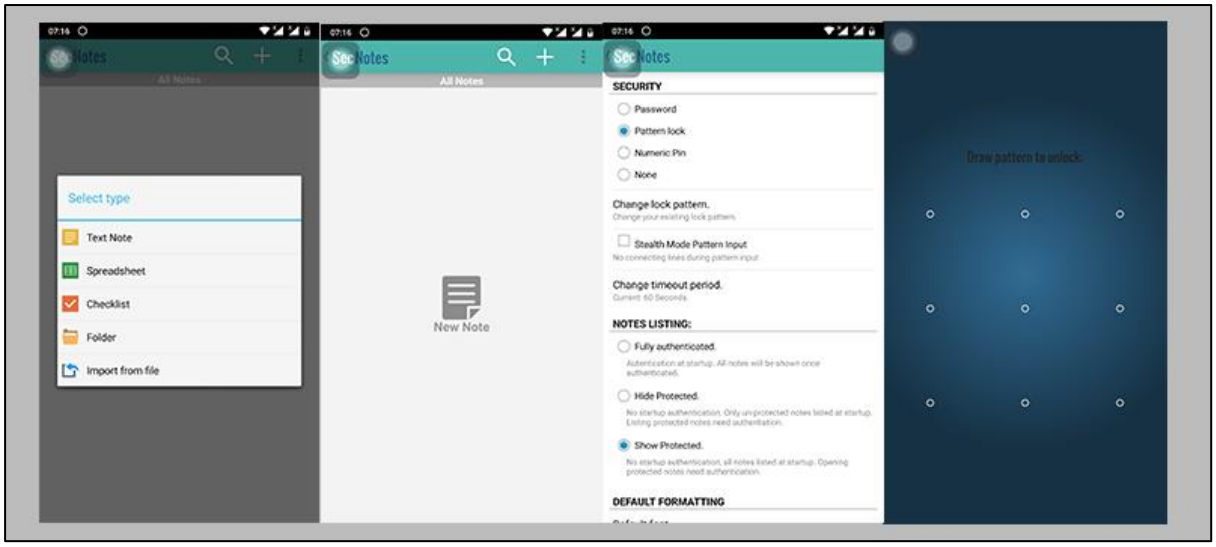


Figure 4.0: Snapshot of SecNotes' application

SecNotes notepad app was developed by Skipser to protect the notes in the application with a range of password type to be used by the user. It is a simple notepad app with passwords that has been encrypted with AES-128 security. The user can create three types of notes inside the application, such as excel files, checklist, and the normal text notes, as shown in figure 4.0.

There are limitations of this application. One of them is the random occurrence of forgotten password. From the reviews of this application, one of the users pointed out that the application is not completely applied AES key for the password protection. Other than that, users are mostly not satisfied with the user interface of the application. There is no tech support for this application so if anything goes wrong, the user has no choice but to uninstall the application. There is also an issue where the user attached medias in the application for their notes but when the same media is being deleted in the main gallery, the media in the application is being deleted as well, because the media attached is not back up into the application.

2.3.2 Safe Notes (YouGoSoft.com, 2016)

Figure 5.0: Snapshot of Safe Notes' password type

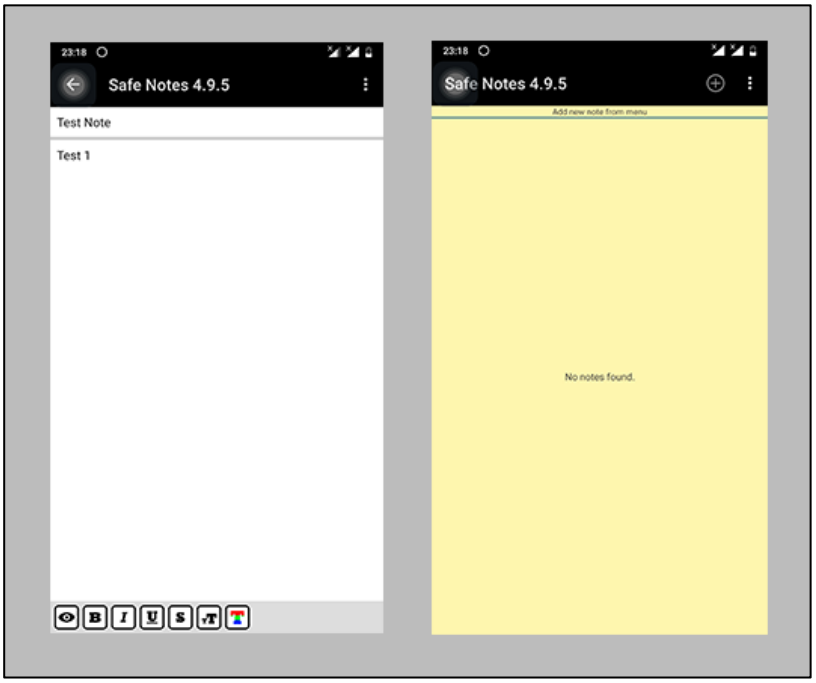


Figure 6.0: The contents of the notes

Safe Notes application is another password-protected application on mobile device that uses 128bit encryption level on the passwords. This application was developed by YouGoSoft.com that aims to protect the confidential notes inputted by the user of the application. User can only lock the application using pin number, and in case of forgot password, the user will be prompted a secret question where the main user knows the answer