XECRET: REMOTE DELETION OF CRITICAL FILE ON STOLEN MOBILE PHONE VIA SMS

AHMAD KAMIL BIN KAMARUDDIN MALIK
AI 160168
INFORMATION SECURITY

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

ABSTRACT

Nowadays, many people lost their phone at public area. This may lead to data disclosure when someone find into the phone information and expose to public. However, there are many remote wiping tools have been developed. But there is issue on connection and wiping methods. In this project, remote wiping is developed to delete file from stolen phone called Xecret application. This project creates an alternative way to remote wiping. Xecret application use Single-Pass Write Zero to make sure the data cannot be retrieved and using SMS (Short Message Service) to connect to stolen phone.

ABSTRAK

Sejak kebelakangan ini, kehilangan telefon bimbit dikalangan orang ramai di tempat terbuka semakin meningkat. Ini akan menyebabkan maklumat peribadi seseorang boleh terdedah kepada orang ramai jika terdapat orang yang tidak bertanggungjawab mengambil data daripada telefon bimbit tersebut. Walau bagaimanapun, terdapat banyak aplikasi pemadaman data secara kawalan jauh telah dibangunkan. Tetapi terdapat beberapa isu terhadap aplikasi tersebut seperti sambungan yang digunakan ke telefon bimbit dan cara pemadaman data yang digunakan. Didalam projek ini, aplikasi pemadaman data secara jauh dibangunkan untuk menghapuskan fail daripada telefon bimbit yang telah dicuri iaitu aplikasi Xecret. Projek ini bertujuan untuk memberi alternatif lain dalam pemadaman data secara jauh. Aplikasi Xecret ini menggunakan cara “Single-Pass Write Zero” dalam pemadaman data untuk memastikan data didalam telefon bimbit yang dicuri itu tidak boleh didapatkan kembali dengan menggunakan Mesej Pesanan Ringkas (SMS) untuk menghubungankan kepada telefon bimbit yang dicuri itu.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, mobile phone is a necessity for everyone regardless of ages. Mobile phone usage has been increasing with the widespread use of social media and online shopping. Some people even have more than one mobile phones, to be used for work and for entertainment. Mobile phone helps people in their daily activities such as making communication and storing of information easier. Furthermore, it allows users to keep pictures and personal information in one place. In short, mobile phone can ease users from bringing book, album and important documents.

Number of mobile devices grow from year to year. Loss of devices is one of the problems faced nowadays. When a mobile device is lost, user will try to locate it by calling the device's phone number. However, it only works if it is within a close distance to the user. A bad person who steals or finds the mobile device may use the information stored in the device for illegal purposes. Lost mobile phones may lead to data privacy disclosure that can affect the owner’s reputation.

Due to the data privacy disclosure, mobile phone users need to be aware about the importance of mobile phone security. User needs to know that mobile phones are vulnerable to be lost or stolen. Due to this, some precaution needs to be taken for instance by installing remote wipe application in the phone. The application can be used to send remote wipe instruction to erase important information in the phone.

There are already some existing applications on the market providing features to solve stolen or lost phone issues. One example of existing application available in the market is ‘Find My Device’ which has been developed by Google on August 2017. Nevertheless, the application requires connection to server via internet connection to operate.

Thus, an application called XECRET application is proposed. XECRET only uses SMS (no server required) via 4G network or internet connection to send remote wiping instruction. It does not require a server like the implementation of ‘Find My Device’. XECRET focuses on secure remote deletion of folder selected by user during installation via proposed SMS instruction. XECRET agent will be installed in a Stolen Phone (the phone that need to be monitored if stolen) and Initiator Phone (the phone that issue the wiping command).

1.2 Problem Statement

Generally, the user only has remote access to the lost phone. Remote access can be done by installing mobile wiping application or agent that provide wiping of important file via internet. From this point onwards, the mobile wiping application will be called as wiping agent because this application is intended to be hidden or working in the background without the knowledge of the thief. One example of wiping agent is ‘Find My Device’, developed by Google. The purpose of this application is to lock, locate and format mobile phone through internet. Nevertheless, firstly this agent requires internet connection and secondly, formatting the phone will take longer time as compared to wiping of selected folder.

Without Internet connection, the agent cannot lock, locate or format the stolen phone. Therefore, the proposed XECRET agent is developed to improve remote wiping. The advantages of XECRET agent are as follows:

- use SMS for sending wiping instruction, thus no server is required.
- remote wipe folder that user selects during installation which is faster than formatting the whole phone

- XECRET agent in Stolen Phone will send notification to the XECRET agent in Initiator Phone, when subscriber identification module (SIM) card is swapped.

1.3 Objective

Following are the objectives of project that have been identified: -

1. To propose an Android-based Initiator Phone and Stolen Phone agents called XECRET, sending secure wiping instruction via SMS. (Contribution: secure wipe via SMS)
2. To develop XECRET agents for Stolen Phones.
3. To test XECRET functionality.

1.4 Project Scope

The scope for this project is as follows: -

- This project only for Android-based mobile phone.
- This proposed XECRET agent will only work on powered device (turned on) with SIM card attached.
- XECRET agents will be installed in Stolen Phone.
- Wiping instruction is sent via SMS only.

1.5 Expected Outcome

At the end of the project, an Android-based XECRET agents for Stolen Phone will be successfully developed with secure deletion.

1.6 Project Significance

The significance of this project is to develop XECRET agents for Stolen Phone to remotely delete user selected folder via SMS.

1.7 Chapter Summary

In this chapter, 3 objectives have been stated namely proposing XECRET agents for Stolen Phones sending wipe instruction via SMS.

1.8 Chapter Organization

In chapter 1, explain about the project background, problem statement, objectives, scope of the project, expected result and project significance. More explanation on problem of the case study and the proposed tools to solve the problem.

In chapter 2, literature review of the projects will be discussed by covering all study of concept, method or technique through the existed system that has similarity with the system that will be developed. The comparison between proposed system and existed system will be shown to ensure that system will be developed has contribution.

In chapter 3, methodology of the project will be explained in detail. Every phase and process are will be explained in this chapter. In chapter 4, designing of XECRET agent will be done in this chapter by covering all the process of analyzing tools requirement and sketching the system design for implementation.

In chapter 5, implementation of the project will be discussed in this chapter by explaining main code structure of the proposed system and testing process also will be done in this chapter. Finally, in chapter 6 will explain about the conclusion of the project, strength of project and constraints that have been faced while developing the project.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

All the keywords mentioned in the project are discussed. This chapter will explain in detail about the concepts that are being used and the implementation of the remote data deletion in the project. A comparison also has been made between the current remote data wiping application and the proposed application.

There are many ways to recover the deleted files in a mobile phone. When a user deletes a file in a device, the files are not permanently removed from the mobile phone (Olvecky & Gabriska, 2018). There is many professional software on the internet that are capable in recovering back all the deleted files in a device under certain conditions (Manson, 2007). Most of the mobile phone users are unaware about this matter. This situation is unsafe when the device is being stolen or falls into the wrong hands. The files that contain personal information in a device might be accessed by people with bad intentions.

In this project, a remote data wiping operation will be developed when the private information in a device can be deleted remotely using a SMS command. The user needs to install the Xecret agent in the mobile phone and adjusts the settings in the application. Once the phone receives the right command through the SMS from the device's owner, the agent will run the data wiping process in the current mobile phone.

2.2 Operating System

Operating system (OS) is a system software that manages computer hardware and software resources. It provides common services for computer programs. The operating system also provides services to facilitate the efficient execution, management and memory allocations for any additional installed software application programs (Stallings, 2013).

2.2.1 Android

Figure 2.1: Google Play *L*ogo.

The Android platform is an open source platform that allows any user or developer to modify and develop application based on their ideas. There are more than 2 million applications in Google Play Store website. The Play Store market is an online electronics and digital store for Android applications. The latest version of Android OS is Android Pie version 9.0.

2.2.2 iOS

Figure 2.2: Apple Store logo.

iOS (iPhone OS) is a mobile operating system that was created and developed by Apple Inc. The iOS platform is a closed source platform that disallow users to change the operating system. Based on Apple's App Store website, there are more than 2.1 million

iOS applications that available for Apple devices like iPhone, iPad and iPod. The latest version of iOS in iPhone is iOS 12.

2.2.3 Windows

Figure 2.3: Windows Phone logo.

Windows Phone (WP) is a mobile operating system developed by Microsoft for smartphones as a successor to Windows Mobile and Zune. The Windows Phone is a closed source platform that disallow users or developers to modify the operating system. Application marketplace for Windows Phone is called Windows Phone Store that contains more than 1 million application for users.

2.2.4 KaiOS

Figure 2.4: KaiOS logo.

KaiOS was introduced in 2017 and it was developed by KaiOS Technologies. KaiOS is a Linux-based mobile operating system and an open source successor to Firefox OS and has been discontinued by Mozilla in 2016. The operating system is incredibly light when it runs in hardware resources. It is also able to run in devices with just 256 MB of memory. Application marketplace for KaiOS is called KaiStore that allows users to download applications from it.

2.2.5 Comparison of Operating System for Mobile Phone.

Table 2.1: Comparison of various operating system platform

OS / Info	Android	iOS	Windows	KaiOS
Worldwide Smartphone Market Share Source: GS. StateCounter (October 2018)	74.69%	22.34%	0.36%	0.93%
Smartphone Company	Samsung, Huawei, Xiaomi, Sony, LG	Apple	HTC, Dell, Nokia	JioPhone, Alcatel, Nokia, Maxcom
Operating System Source	Open Source	Proprietary	Proprietary	Open Source (Linux)
Application Market	Google Playstore	Apple App Store	Windows Phone Store	KaiStore

Table 2.1 shows four different platforms for mobile phones were compared to determine which platform is best suited for the proposed application. Android platform dominated the mobile market with a share of 74.69 percent, followed by iOS (22.34 percent), Windows (0.36 percent) and KaiOS (0.93 percent). In conclusion, the Android operating system platform was chosen by most of the users.

2.3 Data Wiping

Data wiping means erasing the files content after overwriting the files content with some characters like null character or randomized character. After wiping process, it becomes impossible to recover the previous existing data because it deletes the links to memory blocks and replace the files content with some new character value (Olvecky & Gabriska, 2018).

2.3.1 Technique of Data Wiping

Data wiping is one way to delete a file in computer securely. Perfect process of wiping data can make retrieve of data become impossible. There are two type of data wiping techniques that already available on the internet can be shown below: -

Table 2.2: Description of Data Wiping Techniques

Data Wiping Technique	Description
Degaussing	Deletion of data by using magnetic field on hard disk to corrupt the entire disk.
Overwritten	Overwrite the existing data on hard disk using existing method with multiple round to make sure the data are irretrievable.

Refer to the table 2.2, overwritten data wiping techniques have several methods already developed. All the existing methods can be categorized in multiple ways. Every method will be explained below: -

2.3.1.1 Random Data

The Random Data method is a software-based data sanitization method used in some file shredder and data destruction programs to overwrite existing data on a hard drive or other storage devices.

The deletion of a hard drive using the Random Data Sanitization method will prevent all software file recovery methods from finding drive information and may also prevent most hardware recovery methods from extracting data (Castiglione, 2011).

2.3.1.2 Single Pass Write Zero

Write Zero is generally referred to as the single overwrite method. Many data wiping tools support Write Zero technique for overwriting existing storage data. The Write Zero data sanitization method can still be obtained by using hardware recovery methods to extract at least some of the deleted data, but it can almost prevent software file recovery methods from obtaining data from the deleted disk.

Implementation of the writing zero technique includes verification after the first zero overwriting. In addition, Write Zero used character or number other than zero to overwrite the process. Most recovery software cannot use this method to obtain information from a disk that has already been deleted using this technique (Reardon, 2016).

2.3.1.3 DoD 5220.22-M

The DoD 5220.22-M sanitization method was originally defined in the National Industrial Security Program Operating Manual (NISPOM) as one of the most common sanitization methods used in data destruction software by the US National Industrial Security Program (NISP). Process of DoD 5220.22-M sanitization method show at below: -

Table 2.3: Description of DoD 5220.22-M process.

Deletion Method	Description Process
DoD 5220.22-M	Round 1: Overwrites with random single value Round 2: Overwrites with complement of that Round Step 3: Repeats step 1-2 seven times

Table 2.3 shows DoD 5220.22-M is a process of data sanitization used in various file shredder and data wiping tools to overwrite existing data on a hard drive or other storage device type. Deleting a hard drive using this method can prevent software-based file recovery from obtaining hard drive information (Lee, 2011).

2.3.1.4 Schneier

This method is based on the algorithm of Bruce Schneider. It is based on a cryptographically secure random number generator that is deleted with random data. A file is overwritten 7 times. It is very secure and should be used for private files (Schneier, 2015).

Table 2.4: Description of Schneier process.

Deletion Method	Description Process
Schneier	Round 1: Writes a one Round 2: Writes a zero Round 3: Writes a stream of random characters Round 4: Writes a stream of random characters

Table 2.4 (Continued)

Deletion Method	Description Process
Schneier	Round 5: Writes a stream of random characters Round 6: Writes a stream of random characters Round 7: Writes a stream of random characters

The table 2.4 shows the process undertaken using the Schneier data deletion method. In order to finish a deletion using the Schneier method, 7 round overwriting must be completed before completion.

2.3.1.5 Gutmann

The Gutmann method is an algorithm that securely erases the contents in computer hard disk drives, such as files. The method was introduced by Peter Gutmann and Colin Plumb. It involves the writing about a series of 35 patterns over the region to be erased (Wright & Kleiman, 2008)

Most of the patterns in the Gutmann method were designed for older MFM/RLL (Modified Frequency Modulation and Run-length limited) encoded disks. Gutmann had mentioned that more modern drives are no longer using these older encoding techniques, making parts of the method irrelevant.

An overwrite session consists of a lead-in of four random write patterns, each of patterns 5 to 31 were designed with a specific magnetic media encoding scheme in mind, which each pattern targets. The drive is written for all the passes even though the table below only shows bits of patterns for the passes that are specifically targeted at each encoding scheme.

2.4 Remote Wiping

Remote deletion allows owners of the stolen phone to delete their private data at other places. This process is useful for mobile phones or laptops that are vulnerable to be stolen. In case a mobile phone is stolen, the owner may not want their private information to fall into the wrong hands. When this thing happens (the laptop has been stolen), the owner can issue a remote wiping to avoid the leakage of private information to other people.

2.4.1 Socket Programming for Personal Computer

Socket programming is a way to connect two nodes to each other on the network. One socket (node) listens to an IP on a specific port, while another socket reaches the other to form a link. The server forms the listener socket to reach the server (Xue & Zhu, 2009).

Server is middleware that allow remote deletion to be succeed. The server will handle all the request and forwarding process. Process of remote deletion is one computer must be a Initiator Phone and the other become Stolen Phone. The Initiator Phone will create a command and send a request to the server, then the server authenticate the request and forward the request to the Stolen Phone in order to perform a deletion.

2.4.2 SMS command for Mobile Phone

SMS is a service component of most telephone, Internet and mobile device systems. This text messaging service is part of the Global System for Mobile Communications (GSM) standards and it has standardized phone protocols. The protocols enabled users to send and receive messages from and to GSM mobiles with up to 160 alpha numeric characters.

The implementation of remote deletion via SMS is possible to be done by develop an agent that can read incoming SMS. The agent must have default command for deletion that will be compared with incoming SMS. If the comparison between default command and the SMS is true, the agent will be trigger deletion process.

2.5 Development Tool for Android Application

There are several tools being used in developing Xecret agent which are Java, Android Software Development (SDK), Android Development Tools (ADT), SQLite Database and Android Studio. Explanation about these tools are stated below:

2.5.1 Java

Java is a computer language that can be found in various types of devices from mobile phones to computer mainframes. Java programming becomes a choice for developers to develop an Android application because it can be used for classes, object-oriented and specifically designed to minimize the implementation dependency.

2.5.2 Android Software Development (SDK)

A Software Development Kit (SDK or Devkit) is a set of software development tool that can be used to create applications for a software package, framework, hardware platform, computer system, video game console, operating system, or similar development platform. The development of an Android application in Java platform requires a Java Development Kit (Burd, 2015).

2.5.4 SQLite Database

SQLite is being used in Android platform to implement and manage the database concept. SQLite is also an open source database that provides a fast response in requesting information. It only requires a small amount of disk space and suits perfectly on most of the Android devices.

2.5.5 Android Studio

Android Studio is used to develop applications, mostly in Java code or C support with Kotlin. It contains all the basic development environments for Android applications such as the basic workshop and an extensible plug-in system to adapt to the application's environment.

2.6 Existing Remote Deletion Application for Mobile Phone

There are several applications have same function with the proposed application. Several applications function in the same way as the proposed application. In this section, a comparison between the current application and the proposed application was created. The following will explain all existing applications feature: -

2.6.1 Find My Device

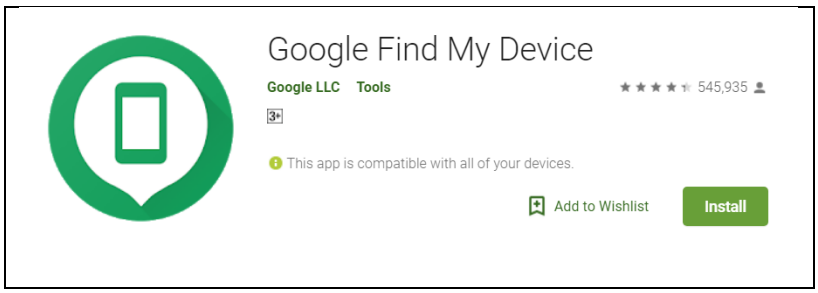

Figure 2.5: Google Find My Device Application

Figure 2.5 shows the Find My Device application icon. Find My Device to remotely track, lock and delete lost or stolen phone data easily. It also allows users to see the remaining battery life on the phone and the connected Wi-Fi network. It's the easiest way to track a lost Android phone, although other ways are also available. All operations on this application need connected to the Internet. User can get the application by download it at Google Play Store and it is free application for Android's phone.

2.6.2 Find My iPhone

Figure 2.6: Apple Find My iPhone Application

Figure 2.6 shows the Find My iPhone application icon. Find My iPhone app that allows users to see the location of the stolen or lost device on the map. Apple devices such as iPhone, iPad or iPod touch will also mark their location when their battery is critically low to help users find it even when power is out. The application provides remote format user personal data and restore iPhone to its factory settings. All operations on this application need connected to the Internet. User can get the application by download it at Apple App Store and it is free application for Apple's phone.

2.6.3 Eradoo

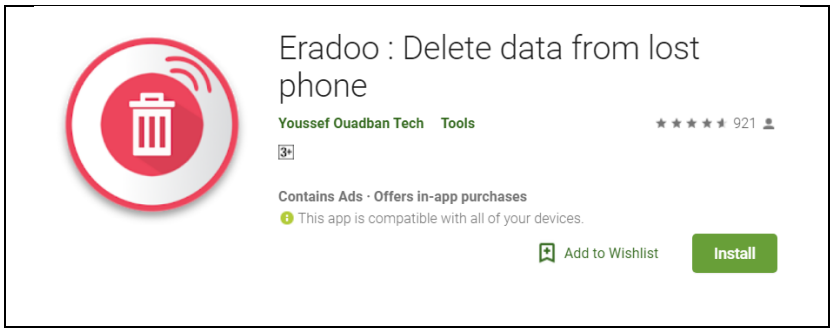

Figure 2.7: Eradoo Application

Figure 2.7 shows the Eradoo application icon. Eradoo application allow user remotely erase data. However, this application is paid application to get the pro version and the free version provide very limited features. Users can get the application by downloading it from the Google Play Store and paying the app for the Android phone price RM5.99.

2.6.4 Xecret (Proposed Application)

Xecret focuses on destroying data and protect privacy from stranger or a thief can access to user's personal information and private document. Xecret is a lightweight application, therefore it does not consume any resources on your phone and it does not drain battery. The process of deletion still can be done without connected to the internet because the application use SMS as a command to trigger the agent to perform deletion process.

2.6.7 Comparison of Existing Application

Table 2.5: Comparison of Existing Application

Mobile Apps / Features	Find My Device	Find My iPhone	Eradoo (Pro Version)	Xecret (Proposed Application)
Platform	Android	iOS	Android	Android
Cost	Free	Free	RM 5.99	Free
SIM card swapped notification	✗	✗	✔ (Via SMS)	✔ (Via SMS)
Remote delete call log and contact	✗	✗	✔ (Via SMS)	✔ (Via SMS)
Selective files with secure deletion.	✗	✗	✗	✔ (Using Single Pass Write Zero's Technique)

Table 2.5 shows the comparison review between similar remote deletion mobile application with the proposed application. The available remote deletion application is using internet connection to trigger the deletion process. Xecret's feature focuses on secure deletion method and using SMS command to trigger the deletion process to be perform.

2.7 Justification of Project Criteria

Xecret application should be able to remotely delete all the selected private files in mobile phones that has been set by the user. The application is beneficial especially when a user loses their mobile phone that may contain private information and can be easily accessed by unwanted people.

To remotely delete the private information from the lost or stolen phone, the owner of the mobile phone needs to install Xecret agent in their mobile phone and adjust the application's settings such as emergency contact, select private files and other configurations.

When the mobile phone is stolen or lost, the owner needs to send a command to the stolen device via SMS. Xecret agent will read all the incoming SMS and compared with the existing command. If the command matches, the Xecret agent will run the wiping process in background to delete the private information that has been selected by the owner of the mobile phone.

2.8 Chapter Summary

There are several mobile phone operating systems that have been reviewed in this chapter such as Android, iOS, Windows and KaiOS. Comparison between all operating system for mobile phone also has been made. In conclusion, Android operating system has the greatest number of users in the world based on the percentage of their market share.

Next, the development tools required for the development of this project such as Java, Android Software Development (SDK), Android Development Tools (ADT), SQLite Database and Android Studio were listed, and their functions were explained. Each tool that is used for the development of this project has its own role and task.

Finally, the existing remote deletion application which are Find My Device (Google), Find My iPhone (Apple), Eradoo and Xecret agent (proposed application) were reviewed and a comparison has been made to determine its capabilities and characteristics.

CHAPTER 3

METHODOLOGY

3.1 Introduction

In this chapter, the methodology for development of Xecret application is discussed. Methodology refers to the application development method, rules, standards and techniques. The methodology allows people to examine whether the project meet their requirements or not (Yeh & Tanik, 1989).

Prototype software development method is chosen in developing the Xecret application. Prototype is the first product example that needs to be developed. So that, people can test it while it's still in developing process.

3.2 Prototype Software Development Methodology

The prototype software development methodology is a system development method (SDM) in which a prototype is built, tested and modified as necessary until an acceptable prototype is finally reached from which the entire application now be developed. This model works best in situations where not everything works (Jones et al., 1992). Prototype software development can be separated into few types, which are throwaway prototyping, evolutionary prototyping and incremental prototyping.

3.2.1 Throwaway Prototyping

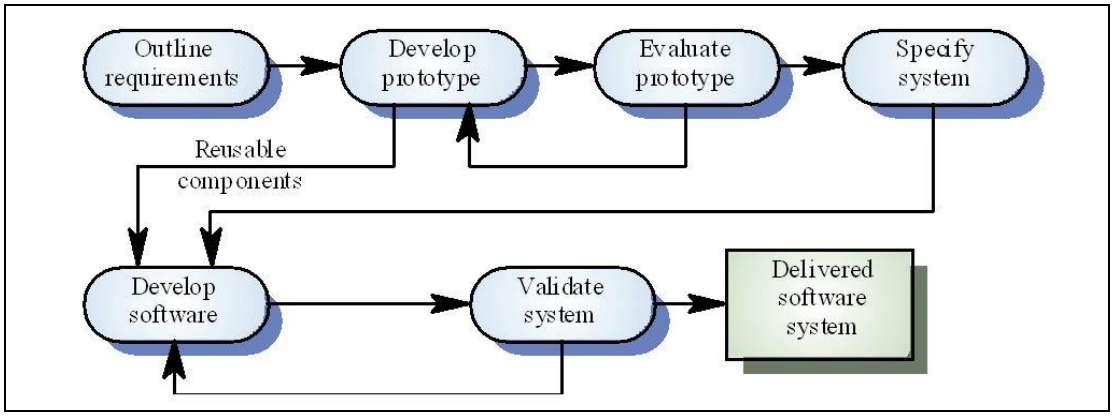

Figure 3.1: Throwaway Prototyping Process (Pressman, 2010).

Based on Figure 3.1, there are processes that need to be followed while using throwaway prototyping method. The reason for using throwaway prototyping is that it is fast. If user can quickly receive feedback on their needs, they can refine them early in the development of the software. Any changes at early development stage is costly, nothing can be done at that point.

3.2.2 Evolutionary Prototyping

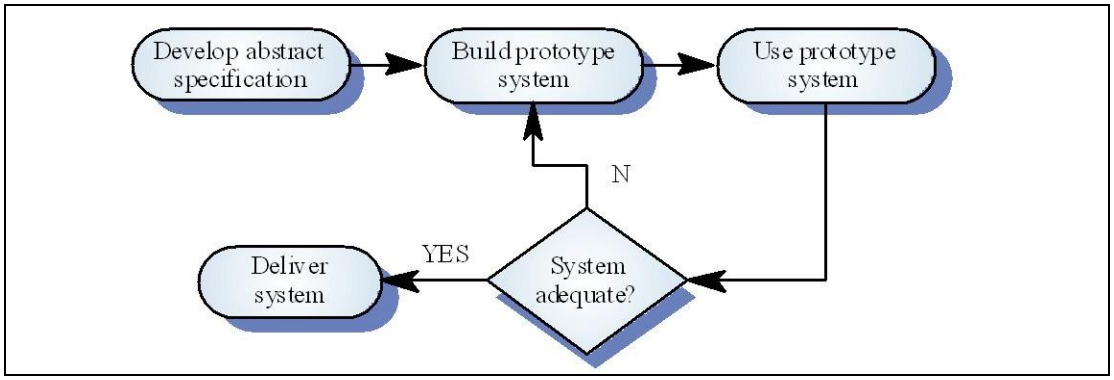

Figure 3.2: Evolutionary Prototyping Process (Pressman, 2010).

Refer to Figure 3.2, there are the processes that need to be followed while using evolutionary prototyping method. The main objective of using evolutionary prototyping is to functionally build and constantly refine a realistic prototype. The reason for this approach is that the evolutionary prototype is the backbone of the new system when the application is built. Improvement and additional requirement will be added while developing the application.

3.2.3 Incremental Prototyping

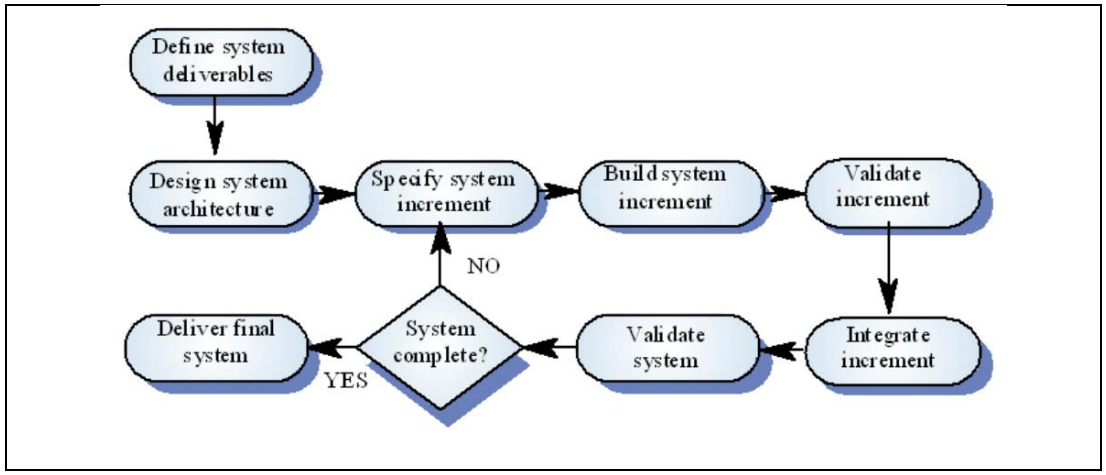

Figure 3.3: Incremental Prototyping Process (Pressman, 2010).

Refer to Figure 3.3, there are the processes that need to be followed while using incremental prototyping method. Incremental Prototyping is a software development methodology in which the product is developed, implemented and tested progressively until the product is finished. The incremental model applies the waterfall model incrementally (Pressman, 2010). System using this methodology is broken down into many mini development projects and partial systems are constructed to generate the final system.

3.2.4 Comparison of Prototyping Methodology

Table 3.1: Comparison of Prototyping Methodology

Prototype Methodology / Characteristic	Throwaway	Evolutionary	Incremental
Period	Very Short Period	Short Period	Long Period
Testing	Not Used for Testing	Used for Testing & Training	Used for Testing & Training
User Understanding	Hardest (Prototype produce to validate requirement)	Easy (Stages prototype to become final system)	Easiest (Prototype is produced by parts)

Based on Table 3.1, Evolutionary Prototyping Methodology is used because its support short period development time and can be used for testing functionality. Furthermore, the prototype application can be extended for developing the actual application. Refer to this comparison, the proposed project will be implemented using Evolutionary Prototype Methodology.

3.3 Evolutionary Prototype Methodology Phases

Evolutionary prototype methodology phase consists of 5 phases namely planning phase, analysis phase, design phase, prototype phase and testing phase.

3.3.1 Planning Phase

During planning phase, objective of developing the application has been defined. All the problem statements already stated, and the project is acceptable to be developed. In the planning phase for Xecret applications, all mobile operating systems are examined to select the most appropriate operating system to be developed the application. The Android operating system was chosen because of it allow developer to build their own application and the most widely used operating system in the world.

3.3.2 Analysis Phase

Analysis phase is conducted, at this phase all important information and jargon words are reviewed to determine which technique and software are suitable while developing this project. Furthermore, Techniques of data wiping have been analyzed and Single-Pass Write Zero technique were chosen in wiping data process. Then, the Java language was used to develop the Xecret application because it is Object-Oriented Programming (OOP). This programming language makes it easy for the developer to create classes and inherited information from another class.

3.3.2.1 Hardware Specification

Table 3.2: Hardware Specification

Hardware	Specification
Laptop Lenovo Y700	Central Processing Unit (CPU): Intel Core i7 6th Generation Hard Disk Drive (HDD): 1 TB Random Access Memory (RAM): 12 GB Operating System (OS): Windows 10 Display Size: 15.6'' inches
Mobile Xiaomi Mi5s	Central Processing Unit (CPU): Qualcomm Snapdragon 821 Hard Disk Drive (HDD): 128 GB Random Access Memory (RAM): 4 GB Operating System (OS): Android 7.0 (Nougat) Display Size: 5.1'' inches

Table 3.2 shows the hardware used for Xecret application development. The laptop Lenovo Y700 was used to develop the application. To test the application, Xiaomi Mi5s mobile phone has been used. All specifications for the hardware were given in Table 3.2.

3.3.2.2 Software Specification

Table 3.3: Software Specification

Software	Function
SQLite	Database
Android Studio Android Software Development Kit (SDK) Android Development Tool (ADT)	Develop Android Application

Table 3.3 shows the software used for Xecret application development. Several main software was used for example SQLite, Android Studio, Android Development Kit (SDK) and Android Development Tool (ADT). SQLite is purposely for handle database and other software are for development application interface and programming.

3.3.3 Design Phase

Design phase is carried out to design the interface of the application for user. Proper design should be user friendly to ensure that user can understand and manage to use the application without any problems. All buttons, font types and colors used in the interface design must be suitable to avoid burdens on the user while using the application.

Xecret application was develop native application-based. Native application is a software program developed use on device. Native application can quickly access multiple services on a device such as microphone and camera. Xecret application interface was build using Android Studio using XML language.

3.3.4 Prototype Phase

Prototype phase is process of development application will be conducted. The application will have many versions during the development of the prototype due to errors and errors. Every bug and error that the developer solves will create a new prototype version to distinguish between old and new applications. The Xecret application prototype will be tested on the mobile phone to determine the functionality and interface design.

3.3.5 Testing Phase

Finally, testing phase will be conducted before delivered the final version of application to end user. Xecret application will be tested all their functionality to ensure there is no bug and error occur before handed to end user. User feedback also will be determined by using questionnaire, user will test the application based on their interface design and functionality.

3.4 Xecret Application Framework

There are 3 stages in Xecret secure wiping application as shown in Table 3.2, which comprises of two steps in stage 1 (Installation Process), followed by three steps in stage 2 (Wiping Process) and finally 2 steps in stage 3 (Notification Process)

Table 3.4: Xecret Application Framework

Phone 1 (Stolen Phone)	Phone 2 (Initiator Phone)
Before the phone was stolen or lost	
Stage 1: Installation Process	
Step 1: Download & install Xecret application into the Stolen Phone.	
Step 2: Complete all the configurations in the application. e.g.: Password setting, enter emergency contact and select important files into designated folder.	
After the phone have been stolen or lost	
Stage 2: Wiping Process	
	Step 3: Owner sends wiping command with password via SMS using initiator phone.
Step 4: Agent read all incoming SMS and compare with the configured wiping command in Step 2. If match is found, wiping process will be triggered in the background.	
Step 5: Secure deletion based on SMS command received from Initiator Phone using (a) single-pass overwrite or (b) default factory reset.	
Stage 3: Notification Process	
Step 6: Agent will send an acknowledgement to Initiator Phone after successful wiping (Only for secure deletion).	
	Step 7: Initator phone receives wiping acknowledgement succeed from the Stolen Phone.

3.5 System Architecture

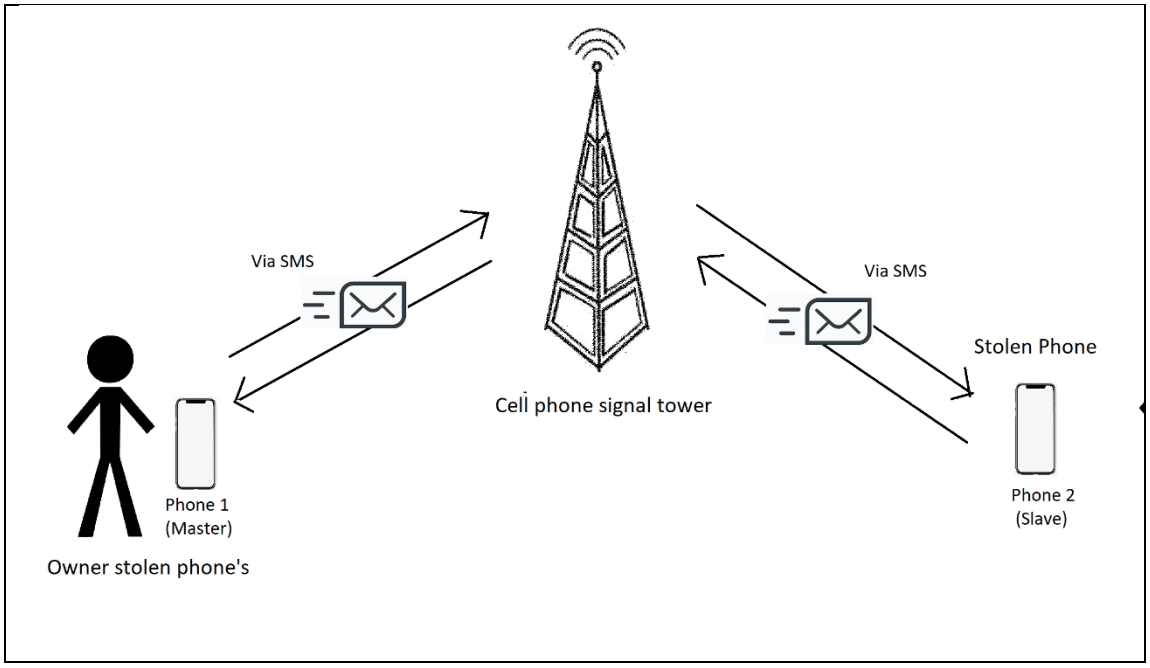

Figure 3.4: System Architecture Diagram

Figure 3.4 shows the diagram of the Xecret Application Architecture. During the wiping process, two mobile phones are needed, the phone 2 acts as a Stolen Phone and the remote phone acts as a Initiator Phone. All the wiping command requests and successful notification is received are via SMS.

3.6 Chapter Summary

Xecret application is developed using prototype software development method. There are three type of Prototype Software Development Methodology. Evolutionary prototyping methodology was chosen, and it consists five phases in developing the application which are planning phase, analysis phase, design phase, prototype phase and testing phase before delivered final version of the application. The Xecret application framework consists of 3 stages with total 7 steps. The first stage is “Installation Process”, second stage is “Wiping Process” and the last stage is “Notification Process”.

CHAPTER 4

ANALYSIS AND DESIGN

4.1 Introduction

The analysis and design process for the development of the Xecret application is discussed in detail in this chapter. The application components and structure are discussed to produce better illustration on how the application works with the user. Unified Modeling Language (UML) is used to create illustrations between users and the application and to explain the application workflow using case diagram, sequence diagram and flowchart. The flowchart is used to show the process user in the application step by step.

In addition, database design was also included in this chapter to show how the data stored in the application is managed. The design of the database is important for the proper management of the data without redundancy occur. Lastly, interface design for each page has been created to show the application environment to the user.

4.2 System Requirement Analysis

System requirement analysis consists two tasks that determining the needs or conditions based on user and system requirement. All system requirements must be documented and explained clearly in order to prevent misunderstanding and misinterpretation. The

analysis must be carried out carefully and in detail to avoid the frequent modification of the process.

4.2.1 User Requirement Analysis

User requirements are part of the design of systems that lead to the success of interactive application. To avoid system failures due to insufficient information on the requirement system, understanding of user requirements is important. Analysis of user requirements is carried out to improve the satisfaction of users, increase productivity and improve work quality. (User flowchart at the next page)

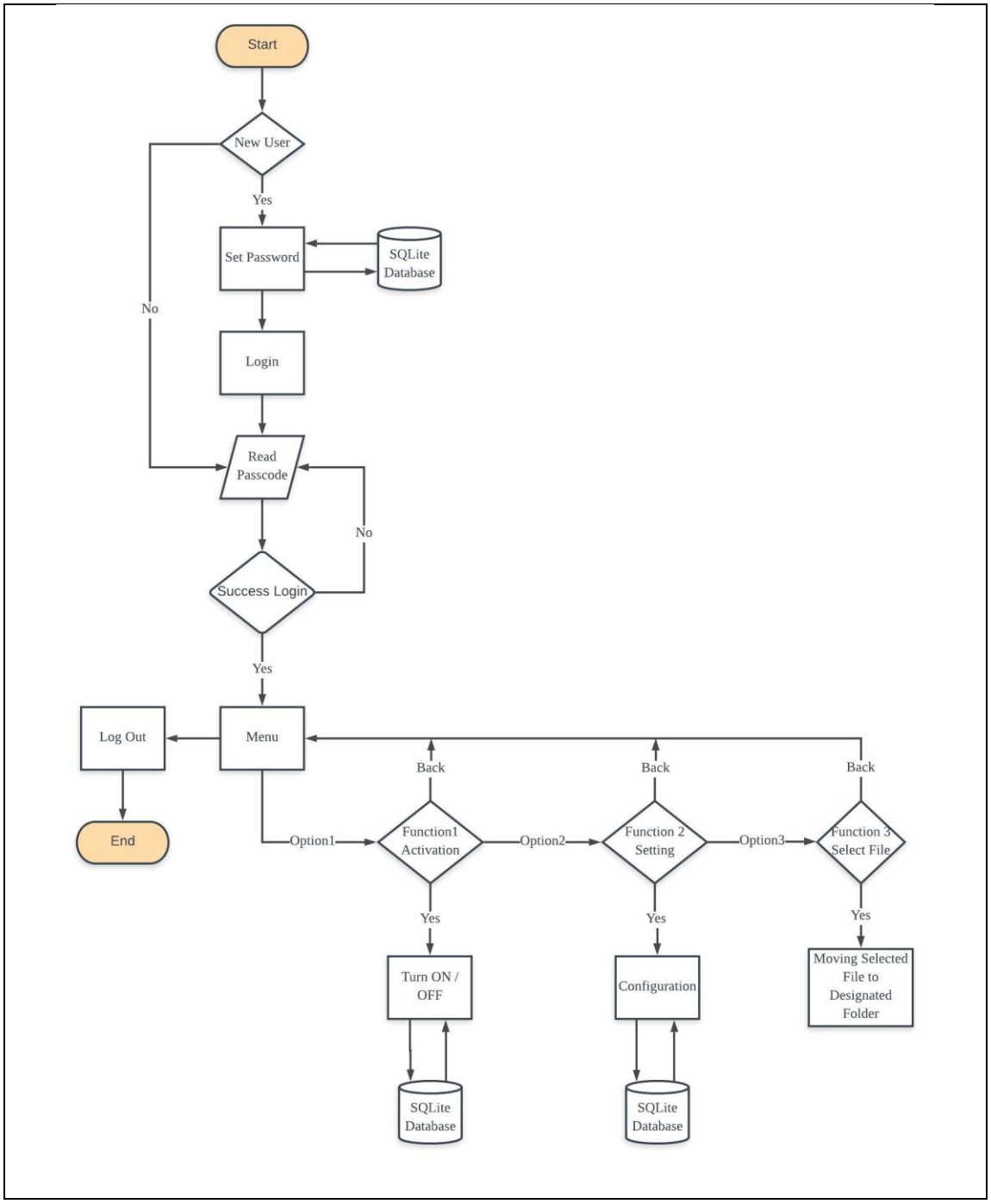

Figure 4.1: User Flowchart

Figure 4.1 shows the user flows in the application. After user installed the application inside their mobile phone, user needs to set passcode before user can use the application. Then, user can enter to the menu interface using passcode. Otherwise, user

have to re-login. At the main menu give three pages which are home page, setting page and features page.

On home page, it displays on / off button that allow user to activate and deactivate the Xecret application function. Next, on setting page allow user to enter emergency contacts, only two contacts allocated to the user and user also can change their passcode. Changing passcode needs user to enter the new passcode and confirm new passcode then press save button. If the both new passcode that user entered is same, then it will save the changes. Else, error message will display on the application.

Besides, features page displays all the features that Xecret application provides. User can select which features user want by clicking button at the right side of every feature. After finish selecting the features, user needs to press save button to save all the configuration into the database.

4.2.2 Application Requirement Analysis

The purpose of the analysis of application requirements is to obtain a detailed understanding of the application function. Application requirement analysis consists with two components which are functional requirement and non-functional requirement. These analyses intended to collect information about the task and action will be taken in the application.

4.2.2.1 Functional Requirement Analysis

Table 4.1 shows the functional requirement of Xecret application. Functional requirement defined what was done by identifying the tasks or actions to be carried out.

Table 4.1: Functional Requirements of Xecret Application.

Page	Functionalities
Login	✓ Application allow user to login using passcode
Register	✓ Application allow new user to setup passcode
Setting	✓ Application allow user to configure all the information needed such as emergency contact, change passcode and choose whether user want to turn on or off features provided.

4.2.3.2 Non-Functional Requirement Analysis

Non-functional requirements describe how the application behavior in term of efficiency and performance. Non-functional requirement analysis is described in Table 4.3, the main requirements for non-functional requirement are performance, operational and security.

Table 4.2: Non-Functional Requirements of Xecret Application.

Requirements	Descriptions
Performance	✓ The application should be able be used at anytime ✓ Use less storage and memory to minimize the battery consumption
Operational	✓ The application features can fully functional without any error and bug. ✓ The application will be running at the background.
Security	✓ The application locked using passcode.

4.3 System Analysis

System analysis is the observation process for systems to detect specifications and procedures. System analysis is a problem-solving technique that enhances the system and ensures that all system components work effectively to achieve the objective. In this study, the results of system analysis in Unified Modeling Language (UML) diagrams consist of use case diagram and sequence diagram.

4.3.1 Use Case Diagram

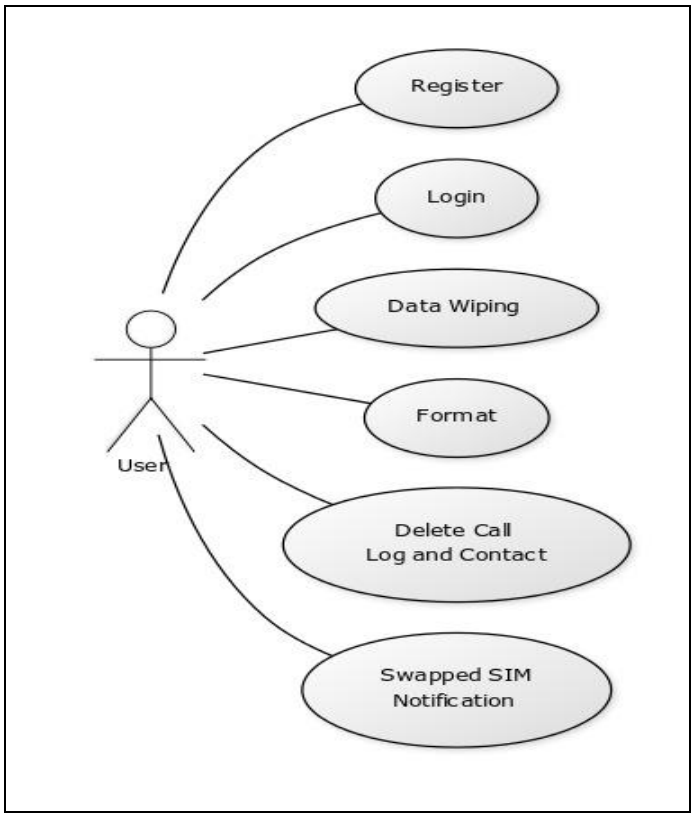

Figure 4.2: Use Case Diagram

Figure 4.2 displays the application case diagram for Xecret. First, users must register by entering passcode before the application can be used by the user. After register, user can

login using passcode that user have entered during the registration. If the passcode is true, users can access the application's menu interface and used all the features provided.

4.3.2 Sequence Diagram

The sequence diagram models the collaboration of objects on a time sequence. Sequence diagram shows interaction of object with others scenario of use case. Sequence diagram also are construct of a Message Sequence Chart (MSC). All the processes interact in sequence diagram are arranged in time sequence that shows operation works.

4.3.2.1 User Registration Sequence Diagram

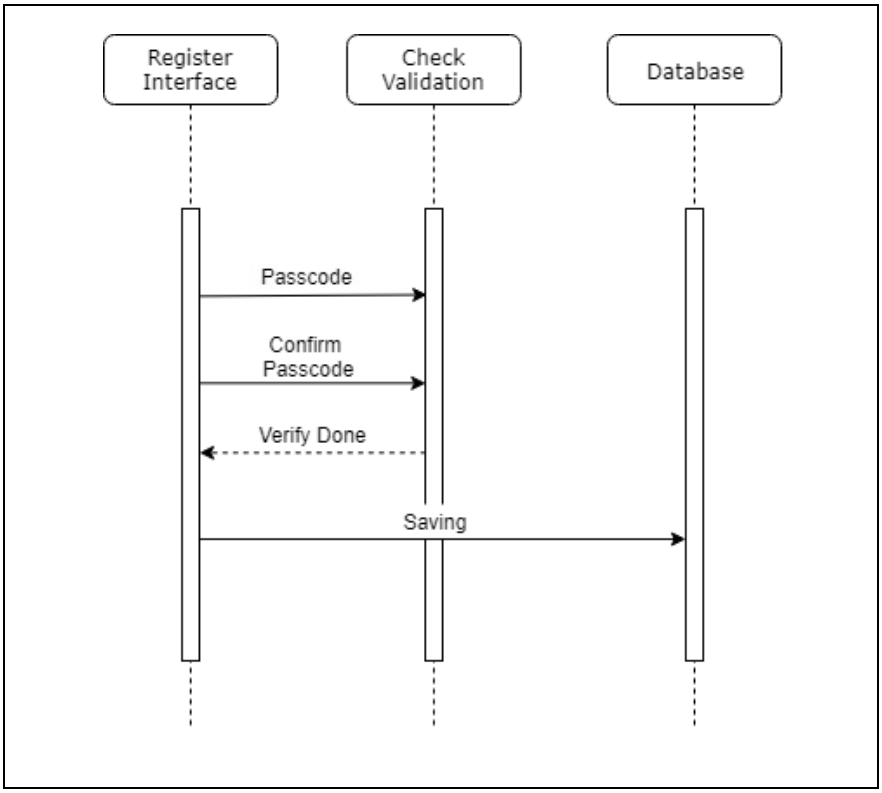

Figure 4.3: User Registration Sequence Diagram

Figure 4.3 shows the user registration sequence diagram. User needs to enter passcode twice in their first login information into the registration form. Then, the data will be

collected and saved in database. After registration, user not require registering anymore because it only for one-time action.

4.3.2.2 User Login Sequence Diagram

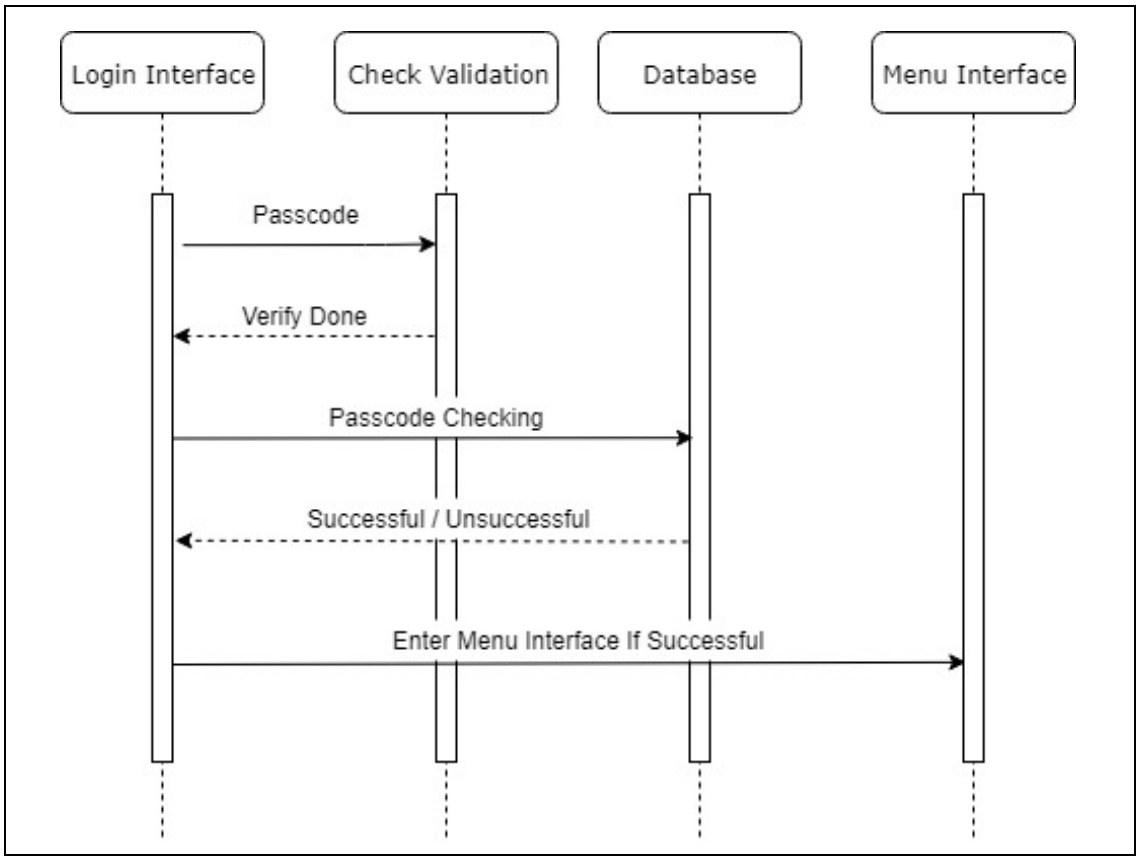

Figure 4.4: User Login Sequence Diagram

Figure 4.4 shows the user login sequence diagram. User require to enter passcode to login into the application. The passcode will be verified with the registered passcode that contain in database. If the passcode is true, then user will go to the menu interface where it will display all the function on the application.

4.3.2.3 Features Sequence Diagram

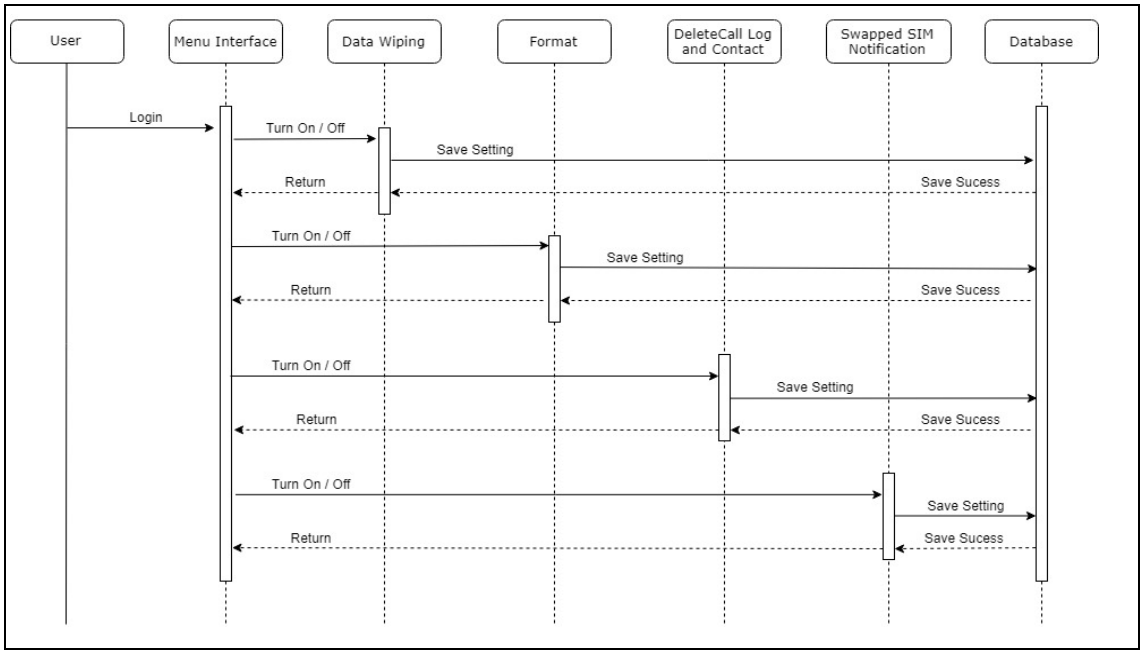

Figure 4.5: Features Sequence Diagram

Figure 4.5 shows the features sequence diagram. User can decide the four main functions which are data wiping, format, delete call log & contact and swapped SIM notification. User can choose whether to turn on or off the features provided. After finish choose the features, user need to save all the configuration by pressing the save button at the bottom of the screen. Then, all the configuration of setting will be stored in the database.

4.3.3 Activity Diagram

The activity diagram displays the message flow from one activity to another. Activity is a specific operation of the system. Activity diagrams are used not only to visualize the dynamic nature of a system, but also to create the executable system using forward and reverse engineering techniques.

4.3.3.1 Register Activity Diagram

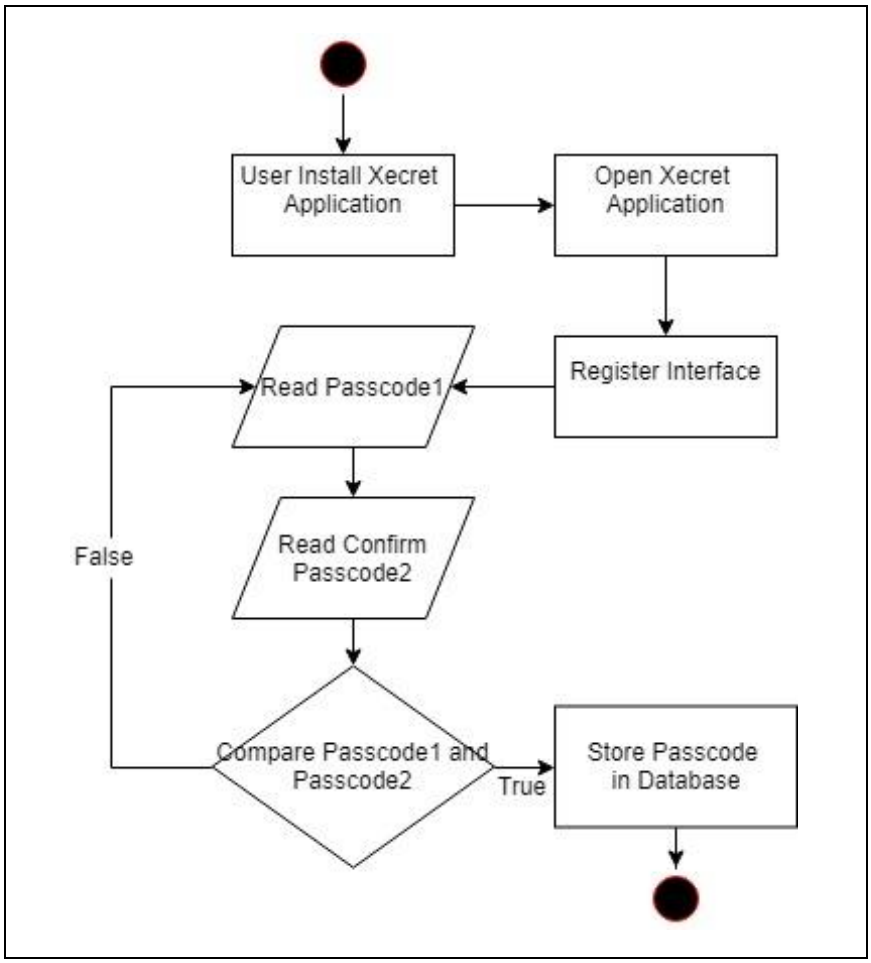

Figure 4.6: Register Activity Diagram

Figure 4.6 shows the register activity diagram. First, the user needs to install the Xecret application inside mobile phone. When the installation is complete, the application appears as the registration interface for the first time. User needs to enter passcode and confirm passcode. If the passcode entered by the user is same, the passcode will be stored in the database for the future used.

4.3.3.2 Login Activity Diagram

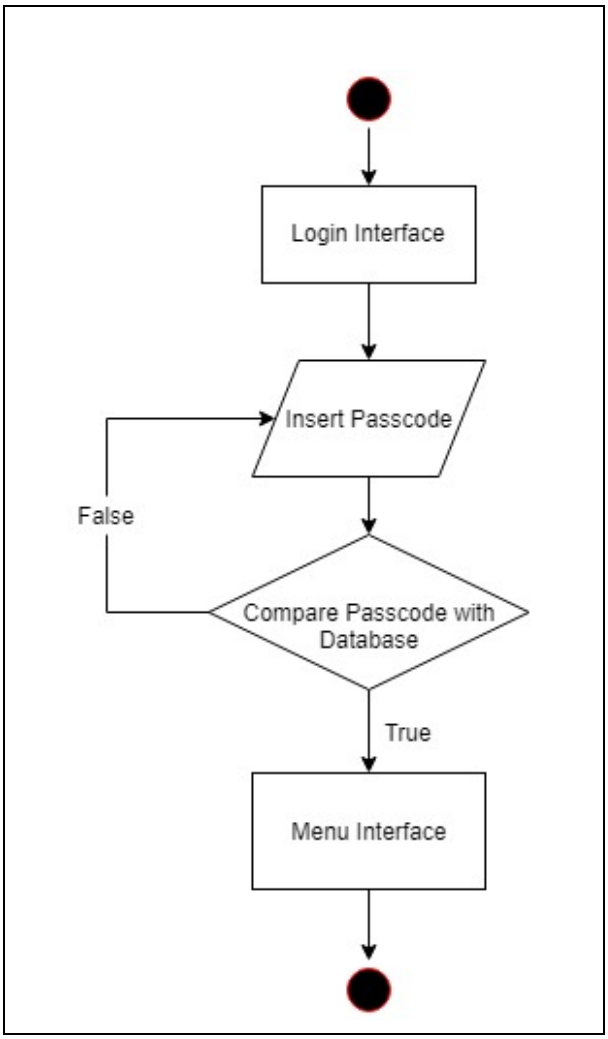

Figure 4.7: Login Activity Diagram

Figure 4.7 shows the login activity diagram. During the login session, the application will display login interface. User needs to enter passcode in order to get access to the menu interface. When user enter passcode, the application will check the passcode with database. If the passcode is true, then the user will gain access. Else, user needs to re-login passcode again.

4.3.3.3 Data Wiping Activity Diagram

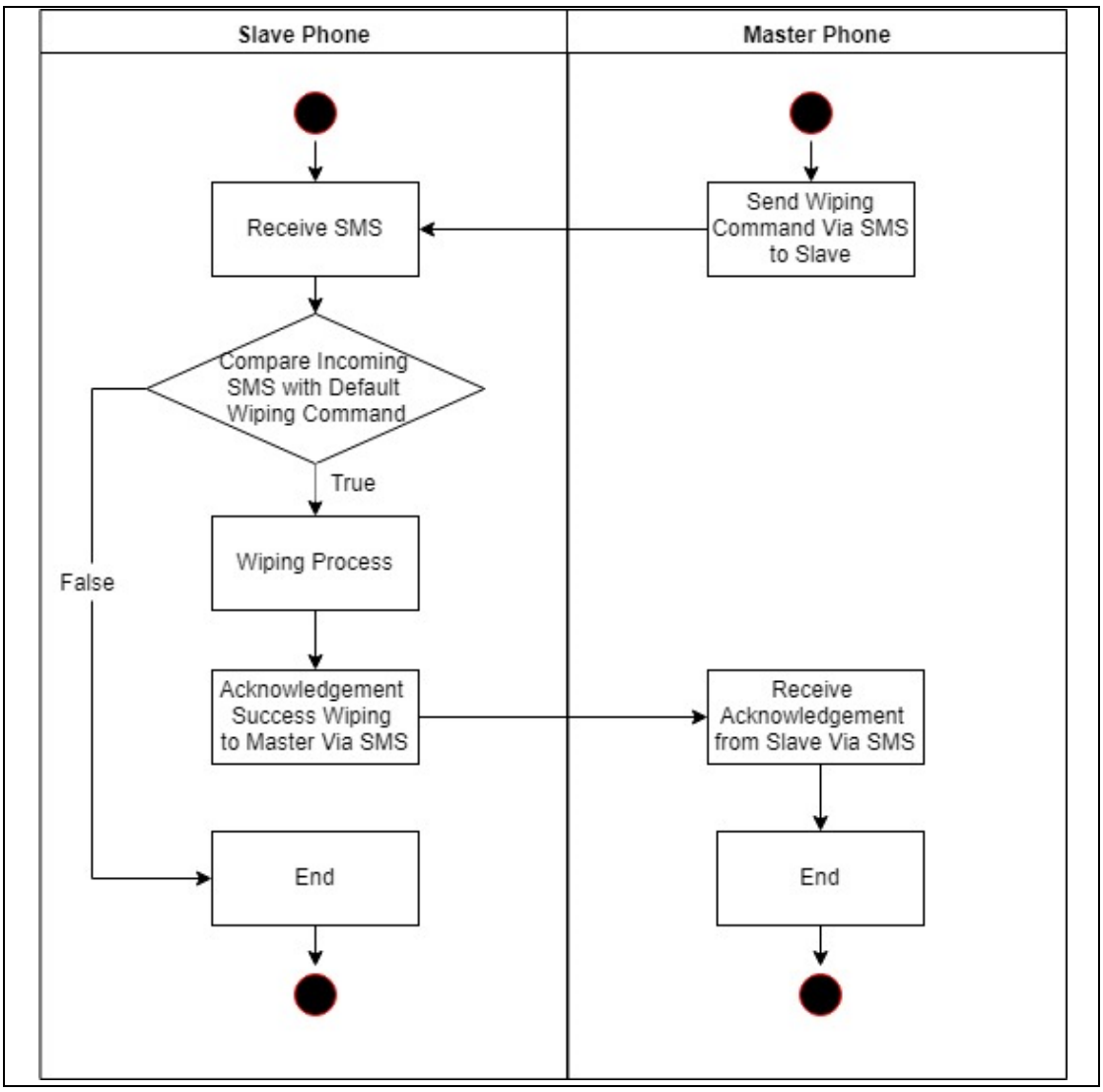

Figure 4.8: Data Wiping Activity Diagram

Figure 4.8 shows data wiping activity diagram. During data wiping process involve two mobile phone, Stolen Phone and Initiator Phone. Initiator Phone will send wiping command via SMS to the Stolen Phone. Then, Stolen Phone will receive the SMS and compare the SMS with default wiping command. If the comparison is true, Xecret application will trigger the wiping process. After finished the wiping process, Stolen Phone will send acknowledgement to the Initiator Phone via SMS.

4.3.3.1 Format Activity Diagram

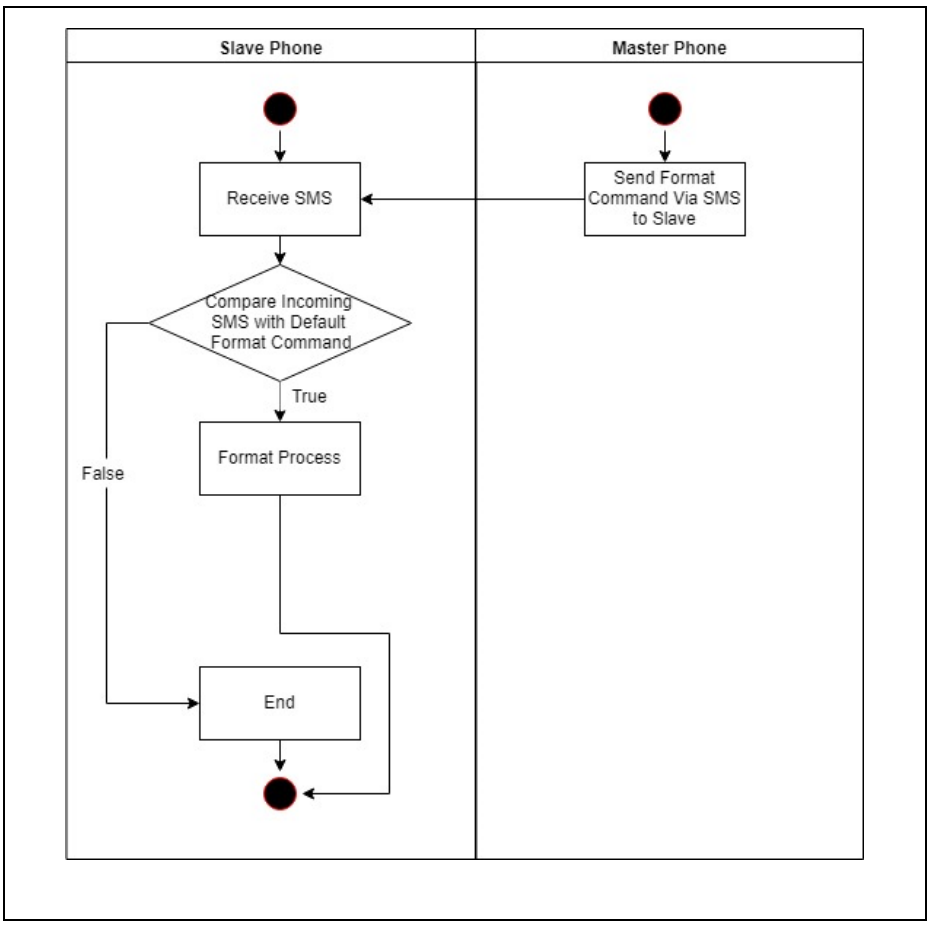

Figure 4.9: Format Activity Diagram

Figure 4.9 shows the format activity diagram. During the format process, involve two mobile phone which are Stolen Phone and Initiator Phone. First, Initiator Phone will send a format command via SMS to the Stolen Phone. Then, Stolen Phone will receive the SMS and compare with default format command. If the comparison is true, Xecret application will trigger the Format (reset factory) process.

4.3.3.2 Delete Call Log and Contact Activity Diagram

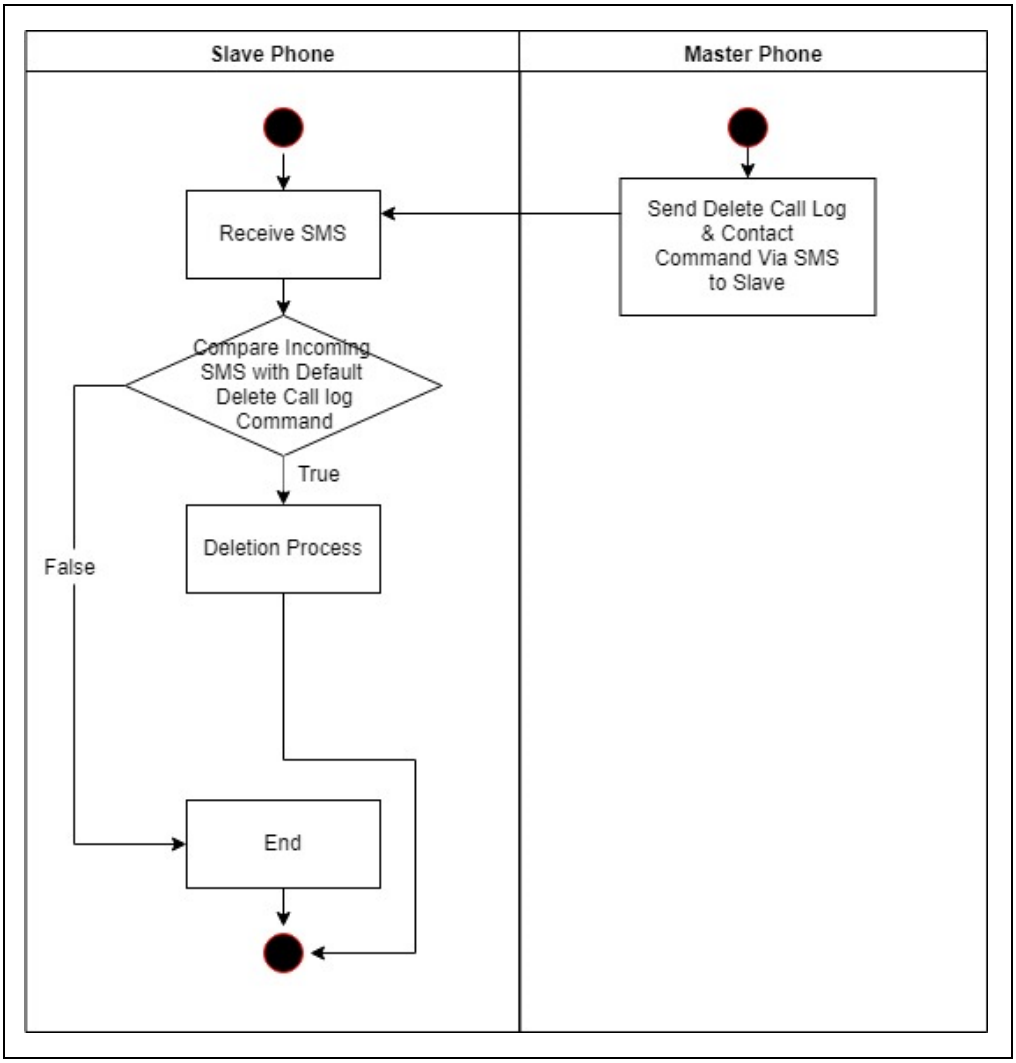

Figure 4.10: Delete Call Log and Contact Activity Diagram

Figure 4.10 shows delete call log and contact activity diagram. During this process involves two mobile phone which are Stolen Phone and Initiator Phone. First, Initiator Phone will send delete call log command via SMS to Stolen Phone. Then, Stolen Phone will receive SMS and compare the SMS with default delete call log command. If the comparison is true, the Xecret application will trigger the deletion process.

4.3.3.3 Swapped SIM Notification Activity Diagram

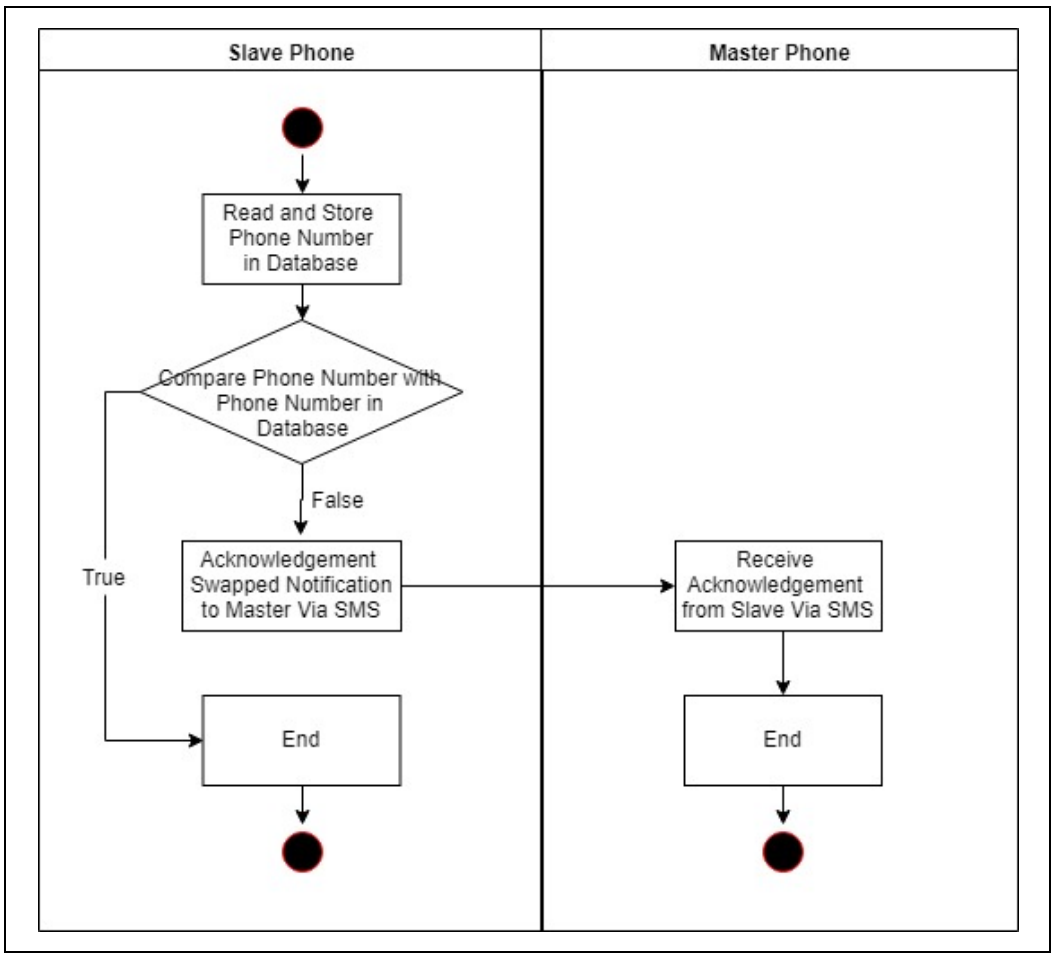

Figure 4.11: Swapped SIM Notification Activity Diagram

Figure 4.11 shows swapped SIM notification activity diagram. When user installed Xecret application inside their mobile phone. Xecret application will read current phone number and saved in the database. If phone number have any changes, the application will trigger notification to all emergency contacts via SMS.

4.4 Database Design

Table 4.3: User Information Table

No	Attribute	Data Type	Description	Key
1	User_ID	Integer	Unique ID	PK
2	Passcode	Integer	Passcode for user login to the application	
3	User_number	Integer	Current phone number based on SIM card attached	

Table 4.3 shows the user information table that contain information about the user, the attribute for user information table are `User_ID, Passcode` and `User_number.` All the attributes are using integer data type and `User_ID` act as primary key in this table.

Table 4.4: Setting Configuration Table

No	Attribute	Data Type	Description	Key
1	User_ID	Integer	Foreign key	FK
2	Xecret_wiping	Boolean	Configuration in setting whether turn on or off	
3	Xecret_format	Boolean	Configuration in setting whether turn on or off	
4	Xecret_call	Boolean	Configuration in setting whether turn on or off	
5	Xecret_swapsim	Boolean	Configuration in setting whether turn on or off	

Table 4.4 shows the setting configuration table that contain data of configuration in setting, the attribute for setting configuration table are `User_ID`, `Xecret_wiping`, `Xecret_format`, `Xecret_call`, and `Xecret_swapsim`. All the attributes are using Boolean except `User_ID` using integer data type and `User_ID` act as primary key in this table.

Table 4.5: Emergency Contact Table

No	Attribute	Data Type	Description	Key
1	Row_ID	Integer	Unique ID	PK
2	Xecret_contact	Integer	Emergency contact for acknowledgement	

Table 4.4 shows the emergency contact table that contain information about the emergency contact lists, the attribute for emergency contact table are `Row_ID`, `Passcode` and `Xecret_contact`. All the attributes are using integer data type and `Row_ID` act as primary key in this table.

4.5 Application Interface Design

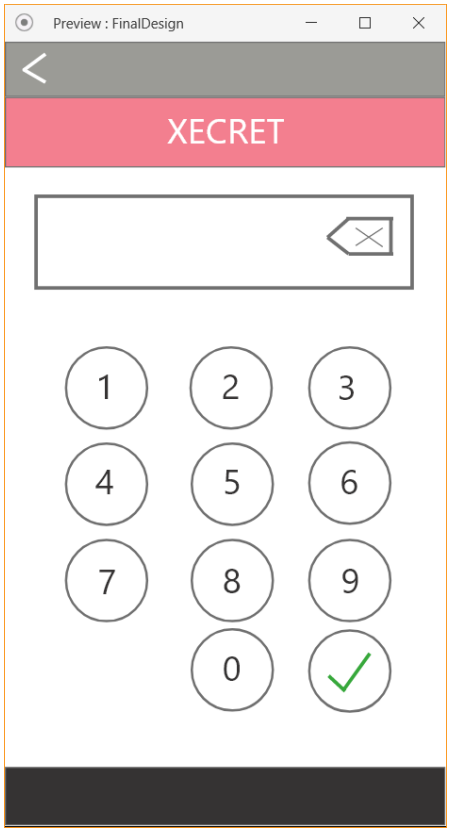

Figure 4.12: Login Page

Figure 4.12 shows the Xecret application login page. On this page, users can enter passcode and delete the passcode entered by pressing the backspace button on the right side of the textbox. The number 0 - 9 numeric button is displayed with the circle button, including the numbering inside the circle button. User must press the " tick " button to verify the passcode after entering the passcode. If the code is true, it goes to the menu interface.

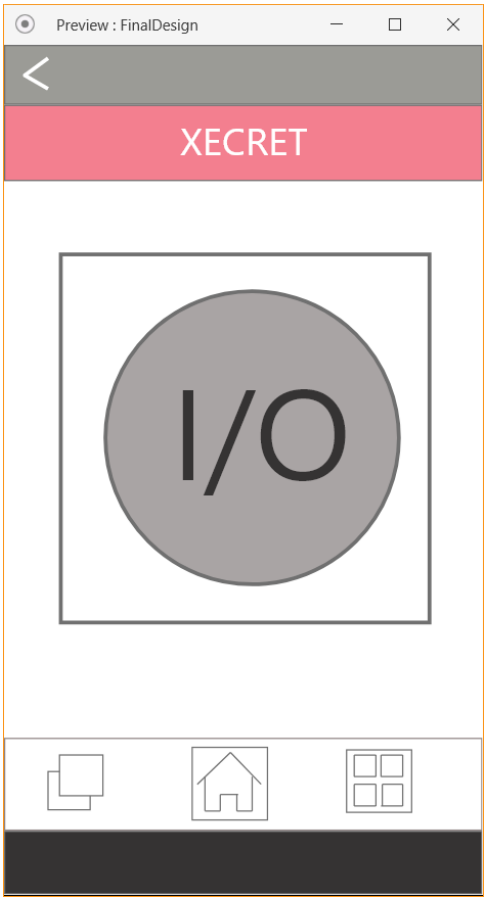

Figure 4.13: Home Page

Figure 4.13 shows the homepage of the Xecret application. On this page the button on / off is displayed in the center of the screen, this button allows users to activate or deactivate the Xecret application function. On the top left of this page you have the back button where it goes back to the previous page. Then, at the bottom of the page, three buttons are displayed that are redirected to the home page, the home page and the features page respectively.

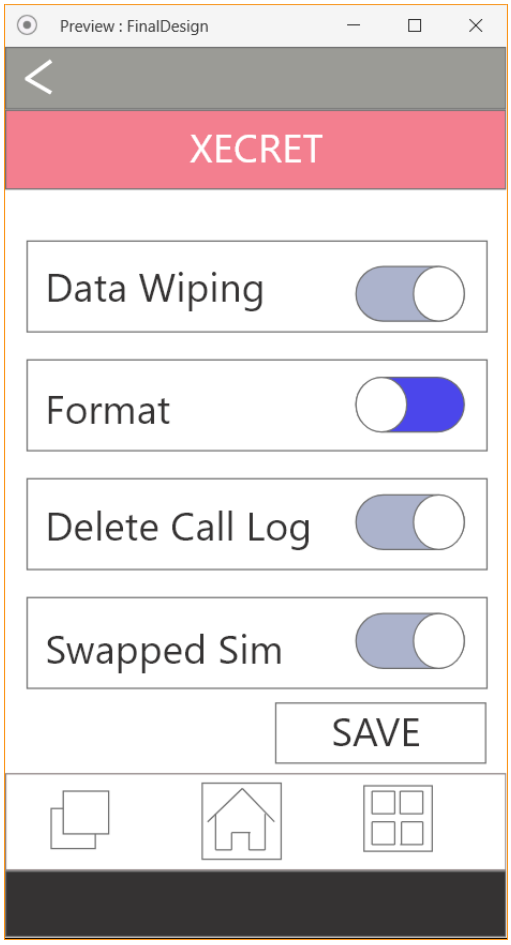

Figure 4.14: Features Page

Figure 4.14 displays the page for Xecret application features. In this page, the user can choose which features the user wants to choose, which includes data wiping, format, call log deletion and SIM notification swapped. After the user has selected the functions, the user must press the save button at the bottom of the function box. On the top left of this page you have the back button where it goes back to the previous page. Then, at the bottom of the page, three buttons are displayed that are redirected to the home page, the home page and the features page respectively.

Figure 4.15: Setting Page

Figure 4.15 explains about the details of setting page of Xecret application. Users can enter emergency contact on this page. For the user, only two contacts are assigned. The emergency contacts listed on the setting page are notified if the SIM card is changed. Besides, user can also change their passcode. To verify it, user must enter new passcode twice. After entering the information, user must press the save button to save all the settings in the database.

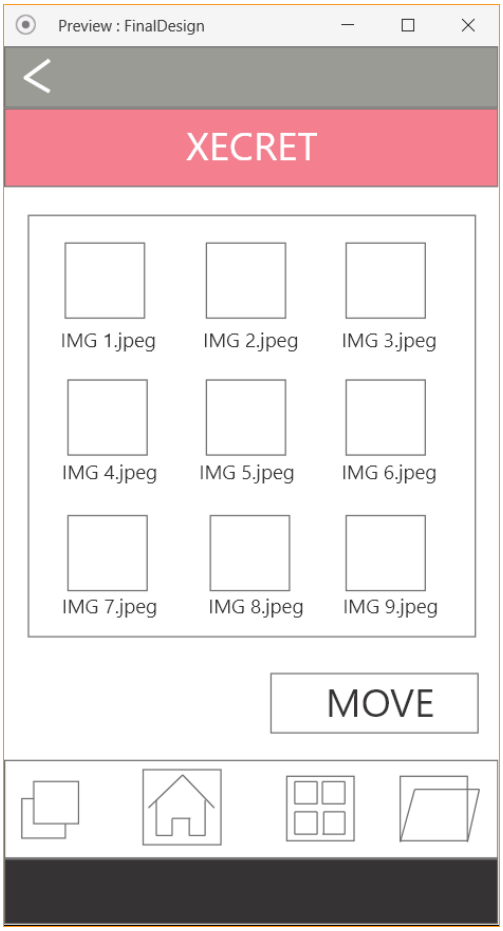

Figure 4.16: Select File Page

Figure 4.16 explains about the details of select file page of Xecret application. User can select which file(s) that important to user to be deleted when their mobile phone have been stolen or lost. User can select more than one file and after finished selecting the important files, user need to press move button to move the selected files into Xecret's folder.

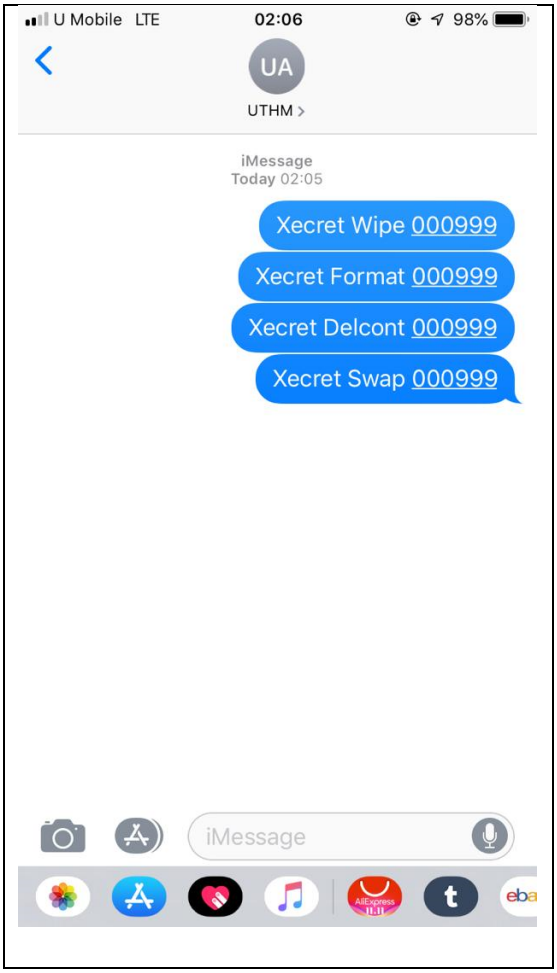

Figure 4.17: Default Command Via SMS

Figure 4.16 shows the sample default command that send by Initiator Phone via SMS. There are four default command which are for wiping, format, delete call log and swapped SIM notification. The structure of the command below: -

Xecret <space> “Action-Type” <space> passcode

Figure 4.18: Default Command Structure

Figure 4.17 shows the default command structure. The first word is “Xecret”, it indicates the Xecret application command format and followed by action-type. Action-type

comprises of “Wipe” (Data Wiping), “Format” (Reset Factory), “DelCont” (Delete Call Log) and “Swap” (Swapped SIM Notification).

4.6 Chapter Summary

This chapter illustrates the entire system development process of analysis and design. Among the processes involved are the design of user interfaces and databases, generating flow charts, use case diagram, sequence diagram and activity diagram that describe the processes involved from the beginning of the system to the end. System requirements are listed in detail to meet user requirements. Additionally, based on the processes that have been carried out, it can be used as a guideline to continue the development of a complete system. In the next chapter, the implementation and testing phase was being described.

REFERENCES

Burd, B. (2015). *Android Application Development All-in-One For Dummies*. 2nd ed. New York, NY: John Wiley & Sons.

Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., & Treichelt, J. (2007). *Is the Open Way a Better Way? Digital Forensics Using Open Source Tools*. Waikoloa: IEEE. pp 266b-266b.

Olvecky, M., & Gabriska, D. (2018). *Wiping Techniques and Anti-Forensics Methods*. 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY).

Reardon, J. (2016). *Secure data deletion from persistent media.* ln: Proceedings of the 2013 ACM SIGSAC conference on computer and communications security. Berlin: ACM New York. pp 271–284.

Stallings, W. (2013). *Operating Systems*. 7th ed. UK: Pearson Education.

Castiglione, A., Cattaneo, G., De Maio, G., & De Santis, A. (2011). *Automatic, Selective and Secure Deletion of Digital Evidence*. Barcelona: 2011 International Conference on Broadband and Wireless Computing, Communication and Applications. pp 92-98.

Reardon, J. (2016). *Flash Memory: Background and Related Work.* Secure Data Deletion Information Security and Cryptography. pp 47-55.

Lee, B., Son, K., Won, D., & Kim, S. (2011). *Secure data deletion for USB flash memory*. Journal of Information Science and Engineering, 27(3). pp 933-952.

Wright, C., Kleiman, D., & Sundhar R.s., S. (2008). *Overwriting hard drive data: The great wiping controversy*. ICISS 2008. Lecture Notes in Computer Science, vol 5352. pp 243-257.

Schneier, B. (2015). *Using Algorithms. Applied Cryptography*. Second Edition. New York, NY: John Wiley & Sons.

Xue, M., Zhu, C. (2009). *The Socket Programming and Software Design for Communication Based on Client/Server*. Chengdu: Pacific-Asia Conference on Circuits, Communications and Systems. pp 775-777.

Yeh, R. T., & Tanik, M. M. (1989). "*Rapid Prototyping in Software Development*" in Computer, 1989, vol. 22, pp. 9-11.

Jones, M., Li, Z., & Merrill, M. (1992). *Rapid prototyping in automated instructional design*. Educational Technology, 30(8), 42-47

Pressman, R. (2010). *Software Engineering: A Practitioner's Approach*. Boston: McGraw Hill. pp. 41–42.