



**SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY**  
**FACULTY OF COMPUTER SCIENCE AND INFORMATION**  
**TECHNOLOGY**

# **TRACKING STOLEN ANDROID PHONES SYSTEM**

**نظام تعقب اجهزة الاندرويد المسروقة**

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS OF B.Sc. (HONOR) DEGREE IN SOFTWARE  
ENGINEERING**

**OCTOBER 2015**

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**SUDAN UNIVERSITY OF SCIENCE AND  
TECHNOLOGY**

**FACULTY OF COMPUTER SCIENCE AND  
INFORMATION TECHNOLOGY**

**SOFTWARE ENGINEERING DEPARTMENT**

**TRACKING STOLEN ANDROID PHONES**

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENTS OF B.Sc. (HONOR) DEGREE IN SOFTWARE  
ENGINEERING**

**PREPARED BY:**

**NASHWA TAJ EL-DEAN OSMAN**

**SARA MOHAMMED AL-NOOR**

**TASNEEM MOHAMMED ALI**

**SIGNATURE OF SUPERVISOR:**

**AL-SHARIF HAGO AL-MOGADAM ..... DATE /OCTOBER/2015**

## الآية

قال تعالى:

**(وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ)**

هود الآية 88

## الحمد لله

الحمد لله الذي بعزّته وجلاله تتمّ الصالحات، يا ربّ لك الحمد كما ينبغي لجلال وجهك ولعظيم سلطانك، اللهم اغفر لنا وارحمنا وارض عنا، وتقبّل منا وأدخنا الجنّة ونجّنا من النّار، وأصلح لنا شأننا كلّه، اللهم أحسن عاقبتنا في الأمور كلّها، وأجرنا من خزي الدّنيا وعذاب الآخرة، اللهم يا من أظهر الجميل وستر القبيح، يا من لا يؤاخذ بالجريرة ولا يهتك الستر، يا عظيم العفو وحسن التجاوز.

اللهم إنّنا نحمدك ونستعينك ونستهديك ونستغفرك ونتوب إليك، ونثني عليك الخير كلّه، نشكرك ولا نكفرك، ونخلع ونترك من يهجرك، اللهم إياك نعبد ولك نصلي ونسجد، وإليك نسعى ونحمد، نرجوا رحمتك ونخشى عذابك، إنّ عذابك الجدّ بالكفار ملحق، اللهم لك الحمد كلّه، ولك الشكر كلّه، وإليك يرجع الأمر كلّه علانيته وسره، فأهل أنت أن تحمد، وأهل أنت أن تعبد، وأنت على كلّ شيء قدير، اللهم لك الحمد حتّى ترضى، ولك الحمد إذا رضيت، ولك الحمد بعد الرّضى لك الحمد كاللذين قالوا خيراً ممّا نقول، ولك الحمد كأذني تقول، ولك الحمد على كلّ حال، اللهم لك الحمد، أنت نور السماوات والأرض، وأنت بكلّ شيء عليم.

# Dedication

To those who gave us drops of love, to those who tired their fingertips to give us a moment of happiness, to those who displaces thorns from our way to pave it for science, to big hearts:

Mohammed Ali Ahmed

Mohammed Annour Ibrahim

Taj El-dean Osman Ali

To a symbol of love and healing balm, to white heart our beloved:

Eshraga Izz El-Dean said

Maaza Siddig Ibrahim

Rajaa Mohammed Ahmed

To the pure and innocent and kind hearts:

Our brothers and sisters

From me Sara Mohammed Annour to the soul that inhabited my soul:

Bakheet Hussein Mohammed

To those who were our salvation, to those who we spent the most beautiful moments with them:

Our colleagues

To those who stay with us in happiness and sadness, to those who we hope to mention them, to those who we wish to keep their pictures in our eyes

Dedicate this thesis and wish from God obtain acceptance and success.

# Acknowledgements

Thanks and appreciation goes to who offers his time and effort to help us to complete this thesis our supervisor Al-Sharif Hago Al-Mogadam.

Sincere respect goes to our teacher Mohammed Osama, and we cannot forget our dear teacher Hanaa Al-Tybe and Ghazy Mohammed, and all teachers especially in Software Engineering department and generally in Faculty of Computer Science and Information Technology.

And our redolence thanks to all of our colleagues and specifically to Safwan Mohammed Ali, Ahmed Taj-Elsir, Ahmed Mohammed, Nahla Taj El-Dean, and to everyone who participate in success of this thesis and thanks firstly and finally to God.

# Abstract

Smart mobile phones are considered as the most important devices currently used in everyday life, human beings use devices to save some personal and necessary information either in work or in public life.

The aim of this study is to keep the mobile phone from theft or loss by certain characteristics, such as locate it when loss and transform the situation to normal mode to facilitate finding device location by making call, and many other characteristics such as making a backup copy of the essential data.

After the implementation of the system and applying tests in many devices we reached to several results, most notably result is enabling person to control his mobile phone via a web page and to activate the services provided by the system by installing the application in mobile phone and logging into system, this can make a backup copy of the data, determine phone's location, control the SIM card, diversion phone to the normal mode and wipe private data in case of theft.

## المستخلص

تعتبر الهواتف النقالة الذكية من اهم الاجهزة المستخدمة حاليا في الحياة اليومية و يستخدمها الانسان في تلبية معظم احتياجاته حيث يحتفظ فيها ببعض المعلومات الشخصية و الضرورية سواء في عمله او حياته العامة.

الهدف من هذه الدراسة هو الحفاظ على الهاتف النقال من السرقة و الضياع و ذلك عن طريق بعض الخصائص مثل تتبعه عند الفقدان و تحويل الوضع الى عام حتى يستطيع ايجاد مكانه بالاتصال فيه و عدد من المميزات الاخرى ابرزها عمل نسخة احتياطية للبيانات الضرورية.

بعد تطبيق النظام و تجربته على عدد من الاجهزة، توصلنا الى عدة نتائج ابرزها تمكن الشخص من التحكم في هاتفه النقال عن طريق صفحة ويب و يقوم بتفعيل الخدمات المقدمة من النظام عن طريق تثبيت التطبيق في هانفة و تسجيل الدخول الى النظام و بهذا يمكنه عمل نسخة احتياطية من البيانات، تحديد مكان الهاتف، التحكم في الشريحة، تحويل الهاتف الى الوضع العام، ومسح البيانات الخصوصية في حالة السرقة.



# Acronyms

SIM	Subscriber Identity Module
GSM	Global System for Mobiles
LTE	Long Term Evolution
UML	Unified Modeling Language
IMSI	International Mobile Subscriber Identity
GPS	Global Positioning System
IMEI	International Mobile Station Equipment Identity
SMS	Short Message Service
API	Application Programming Interface
SDK	Software Development Kit
IDE	Integrated Development Environment
JRE	Java Runtime Environment
JVM	Java Virtual Machine
WAMP	Windows Apache MySQL PHP
HTML	Hyper Text Markup Language
XML	Extensible Markup Language
CSS	<i>Cascading Style Sheets</i>
PHP	Hypertext Preprocessor
AES	Advanced Encryption Standard
HTTP	Hypertext Transfer Protocol
UI	User Interface

# List of Figures

Figure [2.1] Anti-Theft Droid Application .....	6
Figure [2.2] Android Anti-Theft Application .....	7
Figure [2.3] Anti-theft Alarm Application .....	8
Figure [2.4] Total Equipment Protection Application .....	9
Figure [2.5] Bitdefender Anti-Theft Application .....	10
Figure [2.6] Plan B Application .....	10
Figure [2.7] Cerberus Application .....	11
Figure [2.8] Prey Anti-Theft Application .....	11
Figure [2.9] Avast Anti-Theft Application .....	12
Figure [3.1] Mobile Owner’s Use Case Diagram.....	20
Figure [3.2] System’s Use Case Diagram .....	21
Figure [3.3] User Registration Sequence Diagram .....	22
Figure [3.4] User Login Sequence Diagram .....	23
Figure [3.5] View data Sequence Diagram .....	24
Figure [3.6] Control SIM Card Sequence Diagram .....	25
Figure [3.7] Normal Mode Sequence Diagram .....	26
Figure [3.8] Tracking Phone Sequence Diagram .....	27
Figure [3.9] Wipe Data Sequence Diagram .....	28
Figure [3.10] System Activity Diagram .....	29
Figure [3.11] View Data Activity Diagram .....	30
Figure [3.12] Control SIM Card Activity Diagram .....	31
Figure [3.13] Wipe Data Activity Diagram .....	32
Figure [3.14] Tracking Phone Activity Diagram .....	32
Figure [3.15] Normal Mode Activity Diagram .....	33
Figure [4.1] Home Page.....	37
Figure [4.2] Help Screen.....	38
Figure [4.3] Features Screen.....	39

Figure [4.4] Registration Screen.....	40
Figure [4.5] Login Screen in Web Page .....	41
Figure [4.6] Login Screen in Android .....	42
Figure [4.7] User Profile in Web .....	42
Figure [4.8] User Profile in Android .....	43
Figure [4.9] Backup Page .....	43
Figure [4.10] View of User’s Data .....	44
Figure [4.11] Wipe Data Page .....	44
Figure [4.12] Lock SIM Page .....	45
Figure [4.13] Transfer Balance Page .....	46
Figure [4.14] Tracking Page .....	46
Figure [4.15] Phone Mode Page .....	47
Figure [5.1] Comparison between STN and Prey .....	50
Figure [5.2] Performance of AES Algorithm .....	51

# Table of Contents

## 1. Introduction

1.1 Introduction.....	1
1.2 The Problem.....	1
1.3 Research Questions.....	1
1.4 Objectives .....	1
1.5 Scope.....	2
1.6 Thesis Layout.....	2

## 2. Background And Previous Studies

2.1 Introduction.....	4
2.2 Anti-Theft System Background.....	4
2.2.1 Tracking .....	4
2.2.2 Backup Data .....	4
2.2.3 Normal Mode .....	5
2.2.4 Control SIM Card .....	5
2.2.5 Wipe Data .....	5
2.3 Literature Review .....	5
2.3.1 Control mobile remotely.....	5
2.3.2 Anti-Theft Droid Free .....	6
2.3.3 Android Anti-Theft .....	6
2.3.4 Anti-theft Alarm .....	7
2.3.5 Total Equipment Protection .....	8
2.3.6 Bitdefender Anti-Theft .....	9
2.3.7 Plan B .....	10
2.3.8 Cerberus .....	11

2.3.9 Prey Anti-Theft .....	11
2.3.10 Avast Anti-Theft .....	12
2.3.11 Comparison between all Applications and STN Antitheft .....	12
<b>3. Techniques Used And Proposed System Analysis</b>	
3.1 Introduction.....	15
3.2 System Requirements Specification .....	15
3.3 Techniques and Tools Used.....	15
3.3.1 Android .....	15
3.3.2 Eclipse .....	16
3.3.3 GPS Technology .....	16
3.3.4 Java .....	17
3.3.5 Web Technologies .....	17
3.3.6 UML .....	19
3.3.7 MD5 .....	19
3.3.8 AES Algorithm .....	19
3.3.9 Google Maps.....	20
3.4 System Analysis.....	20
3.4.1 Use Case Diagram .....	20
3.4.2 Sequence Diagram .....	22
3.4.3 Activity Diagram .....	29
<b>4. Implementation</b>	
4.1 Introduction.....	35
4.2 How the System Works .....	35
4.2.1 Using the Apach HttpClient .....	35
4.2.2 Using the AsyncTask .....	35

4.3 System Screens .....	37
4.3.1 System’s Main Screen .....	37
4.3.2 Registration Screen .....	39
4.3.3 Login Screen .....	40
4.3.4 User Profile Screen .....	42
4.3.5 Backup Screen .....	43
4.3.6 Wipe Data Screen .....	44
4.3.7 Lock SIM Screen .....	45
4.3.8 Transfer Balance Screen .....	45
4.3.9 Tracking Screen .....	46
4.3.10 Normal Mode Screen .....	47
<b>5. Results</b>	
5.1 Results.....	49
5.2 Comparison between STN Anti-Theft and other applications in Google play .	49
5.3 Comparison between STN Anti-Theft and Prey Anti-Theft .....	50
5.4 AES Algorithm Performance.....	50
<b>6. Conclusion And Recommendations</b>	
6.1 Conclusion .....	53
6.2 Recommendations .....	53
<b>Appendix I</b> .....	55
<b>Appendix II</b> .....	58
<b>References</b> .....	61

# **CHAPTER 1**

## **INTRODUCTION**

## **1.1 INTRODUCTION:**

Theft of phones has become one of the most widespread in the world of crimes in spite of that the phone has become one of the most important sources in our daily lives, which contains many of the confidential information, which helps to retrieve this information in any place and time, but Equally, this information cause many problems when the loss of the telephone.

Component-based software engineering is an approach to software development that depends on software reuse. It emerged from the failure of object-oriented development to support effective reuse. Single object classes are too detailed and specific. Components are more abstract than object classes and can be considered to be stand-alone service providers. A software component is a software element that conforms to a component model and can be independently deployed and composed without modification according to a composition standard [1].

The concept of the system is creating an application to backup data from device, change mode, and other features based on android platform.

## **1.2 THE PROBLEM STATEMENT:**

Tracking and find out the location of thieves phones is very difficult if you don't work in one of the communication companies. Also phone owners want to keep backup confidential information when the phone theft and know who thief their phones.

## **1.3 RESEARCH QUESTIONS:**

- How to integrate components to form the final product?
- How to remotely control the theft device and SIM card?

## **1.4 OBJECTIVES:**

- Track and find out the location of thieves phones.
- Backup confidential information when the phone theft.
- Change mode of device to normal mode.
- Enable user to control SIM card.



- Enhance and secure connection between android applications and web applications.

## **1.5 SCOPE:**

This research targets any one has android device, helps tracking and controlling devices remotely when lost or theft.

## **1.6 THESIS LAYOUT:**

Chapter two contains two parts; part one represents a general background about anti-theft and its features, and part two is the literature review. Chapter three has two parts; first part explains the tools and techniques used in this project, and the second part is the project analysis and design. Chapter four represents project implementation. Chapter five lists results and discuss. Finally chapter six includes conclusion and recommendations .

# **CHAPTER 2**

## **BACKGROUND AND LITERATURE REVIEW**

**2.1 SECTION ONE: INTRODUCTION**

**2.2 SECTION TWO: ANTI-THEFT OVERVIEW**

**2.3 SECTION THREE: LITERATURE REVIEW**

## **2.1 INTRODUCTION:**

This chapter includes two parts, the first part gives a general description of Anti-Theft and its features, and the second one describes the literature review of research project.

## **2.2 ANTI-THEFT SYSTEM**

### **BACKGROUND:**

Anti-theft system is any device or method used to prevent or deter the unauthorized appropriation of items considered valuable [2].

Android phones are now so prevalent widespread, become the best platform for social networking and collaboration, people can track information on the fly and mobile technology is the center of innovation, so we need for the anti-theft mobile applications to prevent phones from theft.

#### **2.2.1 Tracking:**

Tracking is used for the observing of persons or objects on the move and supplying a timely ordered sequence of respective location data to a model.

Tracking system is generally a system capable of rendering virtual space to a human observer while tracking the observer's body coordinates [3].

#### **2.2.2 Backup Data:**

In information technology, a backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event. Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by data deletion or corruption. The secondary purpose of backups is to recover data from an earlier time, according to a user-defined data retention policy, typically configured within a backup application for how long copies of data are required [4].

### **2.2.3 Normal Mode:**

Normal mode is a setting available in mobile phones that enables the ringtones when it is activated. It allows the device to receive and send calls and messages with sounds.

### **2.2.4 Control SIM Card:**

SIM card is a smart card that gives a cell phone its phone number and customer identity. Introduced in 1991 for GSM phones, most cards are removable. Satellite and LTE phones also use SIM cards [5].

By controlling we mean two things; first is transferring balance, second is locking SIM card, which means restriction the use of SIM card.

### **2.2.5 Wipe Data:**

Wipe means making something clean by rubbing something on it. It is used for preventing data from attacks when phone is theft.

## **2.3 LITERATURE REVIEW:**

### **2.3.1 Control Mobile Remotely by Reem AL-Raiah and Others in July 2012:**

The purpose of this study was to remotely control phone by locating phone, wiping data, locking phone, and specifying a password to lock the phone.

#### **Results:**

Important results of this study were control phone, locate phone, specify a password to lock the phone, and wipe data.

#### **Important recommendations:**

1. The possibility of developing the application to include all android devices and other devices.
2. Add new features to control the phone remotely.
3. Enhance and secure connection between android applications and web applications [6].

## 2.3.2 Anti-Theft Droid Free:

The Droid antitheft application was developed to solve your problem if your Android device is stolen or is lost.

How it works: If you misplaced or stolen your phone you can control your phone via text messages to get exact location of your phone. This app automatically activates the GPS and WiFi connection if it is turned off at time of application the location of the device. Anti-Theft Droid app includes alarm feature. And it identifies the exchange of phone chip, returning the phone's location at the time of exchange of information In the new Chip Carrier, IMEI, phone number [7].



Figure [2.1] Anti-Theft Droid Application

## 2.3.3 Android Anti-Theft:

Android Anti-Theft is a cool application for android users developed by Snuko. With Snuko anti-theft applications installed you can have the confidence that your personal data will always be safe.

How it works: With Snuko you can track location of your stolen android phone using GPS, WiFi and cell tower. And you can transfer all important data such as SMS, contacts, and call logs from your stolen device to new

one. Snuko having other important features are SMS command, spy camera, sound audible alarm, SIM card change detection and more [7].



Figure [2.2] Android Anti-Theft Application

### 2.3.4 Anti-theft Alarm:

Anti-theft Alarm is one of the famous and best Anti-theft applications available for iPhone and Android users. In iTunes store sold out 1million copies, now it is available for Android users for free. If you have Anti-theft Alarm application in your Android phone there is no way for your phone to be stolen.

How it works: If you leave your phone around or anywhere. This application plays an ALARM OUT LOUD as soon as someone moves your phone or touches your phone. The alarm will mute only after you enter your Secret Pin. So no one will be able to touch your phone, change its place or even look at its screen. Best thief prevention and extensive burglar alarm [7].

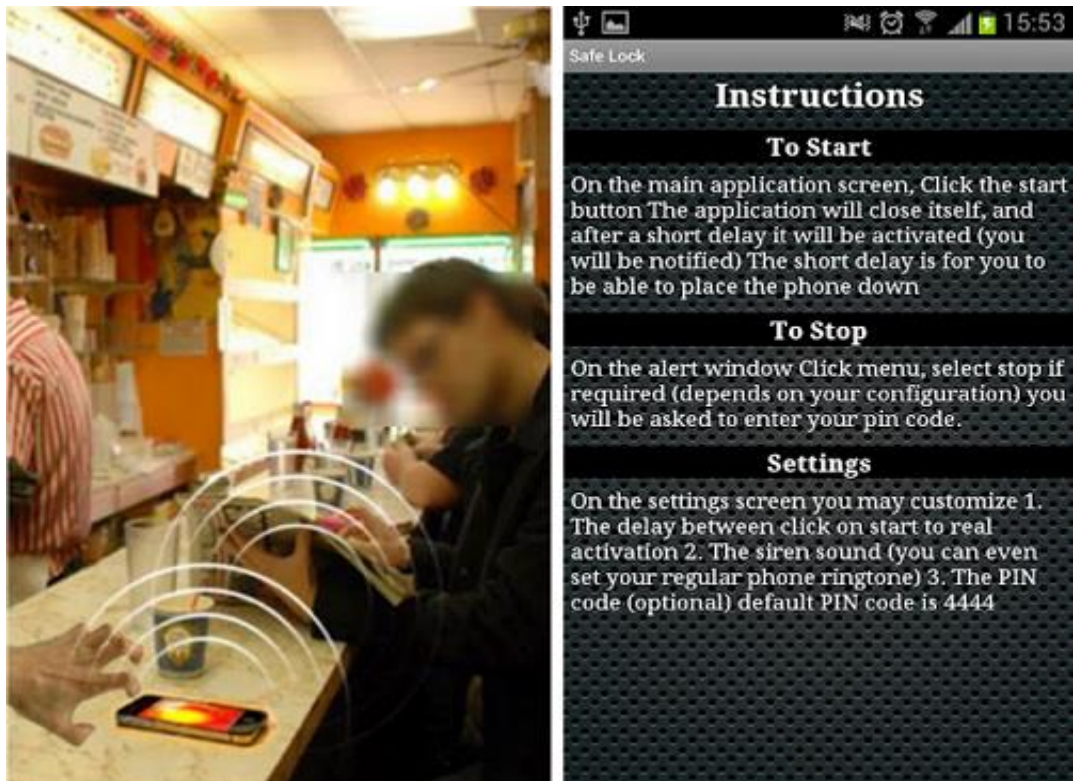


Figure [2.3] Anti-theft Alarm Application

## 2.3.5 Total Equipment Protection:

The application is included with Total Equipment protection .Look to Total Equipment Protection with the all-new protection app as your single source for phone protection.

How it works: if your phone is lost, stolen or just stops working, this application allows you to easily retrieve contacts, and transfer them easily to your new device and you can lock the device remotely so your private information can't be accessed. The application website allows you to locate your phone on a map and trigger an alarm, even if the volume is turned off [7].



Figure [2.4] Total Equipment Protection Application

### 2.3.6 Bitdefender Anti-Theft:

Bitdefender Anti-Theft is the easiest way to get your lost or stolen phone back.

How it works: you can transfer all important data such as SMS, Contacts, and Call logs from your stolen device to new one. Get last calls, thief phone number, IMEI and network operator name when new SIM card detected and more same as above mentioned applications features [7].





Figure [2.5] Bitdefender Anti-Theft Application

### 2.3.7 Plan B:

If you had not install any theft tracking app to your Android before it gets stolen, then need not worry as in this case, Plan B will act as a life saver. This app can easily locate your cell towers and GPS and will send its accurate location to your Gmail inbox. This will keep you updating the exact location of your phone in every 10 minutes [27].



Figure [2.6] Plan B Application

## 2.3.8 Cerberus:

It do includes all influential features like remote alarm, GPS tracking, wipe off SD card and internal storage, remote or track lock of phone and last SIM alerts. You can even record audio from microphone. The account of this app will allow you use over at least 5 devices [27].



Figure [2.7] Cerberus Application

## 2.3.9 Prey Anti-Theft:

To utilize this application, you need to install it before the loss of your device. To locate your lost device, you need to activate Prey SMS by typing "GO PREY" in caps and then log into the control panel and mark your phone as missing and you will start getting the SMS regarding the location of your android [27].



Figure [2.8] Prey Anti-Theft Application

### 2.3.10 Avast Anti-Theft:

This is a pretty decent offering from AVAST, and while it does mostly what others do there are a few stand outs. For one, their website is very well put together and easy to use, and you can lock your device with a custom text message. So perhaps your address, your phone number or just a healthy warning that you know where the thief is. Either way, this covers all the bases and does so with ample amount of polish [27].



Figure [2.9] Avast Anti-Theft Application

### 2.3.11 Comparison between all Applications and STN Antitheft:

This table shows the features that are applied in STN Antitheft, and whether it is found in other applications by a tick.

Feature \ Application	Location	Backup	Wipe Data	Change Mode	Transfer Balance	Lock SIM Card
STN	✓	✓	✓	✓	✓	✓
Plan B	✓					
Prey	✓					
Avast	✓	✓				
Cerberus	✓		✓			
Droid Free	✓					
Bitdefender		✓				

Total Equipment Protection	✓	✓		✓		
Android Anti- Theft	✓			✓		
Control Mobile Remotely	✓		✓			
Anti-Theft Alarm				✓		

Table [2-1] Comparison between Applications

# **CHAPTER 3**

## **TECHNIQUES USED AND PROPOSED SYSTEM ANALY**

**3.1 SECTION ONE: INTRODUCTION**

**3.2 SECTION TWO: TECHNIQUES USED**

**3.3 SECTION THREE: PROPOSED SYSTEM  
ANALYSIS**

## **3.1 INTRODUCTION:**

This chapter describes specification of devices, operating system, programming language, and techniques used to build the system, and the system analysis using UML technology.

## **3.2 SYSTEM REQUIREMENT**

### **SPECIFICATION:**

The operating system that will be used in the development of this system is Android, and the SIM card that is required to implement control SIM card feature is MTN Sudan.

## **3.3 TECHNIQUES AND TOOLS USED:**

This section describes the tools and techniques that were used in the system.

### **3.3.1 Android:**

Android is a software stack for mobile devices that includes an operating system, middleware and key applications. Android is a software platform and operating system for mobile devices based on the Linux operating system and developed by Google and the Open Handset Alliance. It allows developers to write managed code in a Java-like language that utilizes Google-developed Java libraries, but does not support programs Developed in native code.

#### **3.3.1.1 Advantages:**

- Open - Android allows you to access core mobile device functionality through standard API calls.
- All applications are equal - Android does not differentiate between the phone's basic and third-party applications.
- Breaking down boundaries - Combine information from the web with data on the phone to create new user experiences.

- Fast and easy development - The SDK contains what you need to build and run Android applications.

### **3.3.1.2 Disadvantages:**

- Security - Making source code available to everyone inevitably invites the attention of black hat hackers.
- Open Source - Anyone can scrutinize the source code to find vulnerabilities and write exploits.
- Login - Platform doesn't run on an encrypted file system and has a vulnerable log-in.
- Incompetence – Google's dependence on hardware and carrier partners puts the final product out of their control [8].

## **3.3.2 Eclipse:**

Eclipse is a general purpose open platform that facilitates and encourages the development of third party plug-ins.

It is known as IDE. It provides tools for coding, building, running and debugging applications. Originally designed for Java, now supports many other languages.

### **3.3.2.1 Advantages:**

- Code completion.
- Faster code/compile/run cycles (real time).
- Open source (free).
- Extensible (plug-in).

### **3.3.2.2 Disadvantages :**

- Pretty heavyweight.
- Requires JRE.
- Difficult to Learn [9].

## **3.3.3 GPS Technology :**

GPS is an earth orbiting satellite based navigation system. It is an operational system, providing users worldwide with twenty four hour a day

precise position in three dimensions and precise time traceable to global time standards [10].

### **3.3.4 Java :**

Java is a computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that code that runs on one platform does not need to be recompiled to run on another. Java applications are typically compiled to byte code (class file) that can run on any JVM regardless of computer architecture. Java is, as of 2012, one of the most popular programming languages in use, particularly for client-server web applications, with a reported 30 million developers. Java was originally developed by James Gosling at Sun Microsystems (which has since merged into Oracle Corporation) and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++, but it has fewer low-level facilities than either of them [11].

### **3.3.5 Web Technologies:**

The following technologies will be used in the system in both server and client sides.

#### **3.3.5.1 WAMP Server:**

The acronym WAMP refers to a set of free (open source) applications, combined with Microsoft Windows, which are commonly used in Web server environments. The WAMP stack provides developers with the four key elements of a Web server: an operating system, database, Web server and Web scripting software [12].

#### **3.3.5.2 HTML:**

HTML is a markup language for describing Web documents (Web pages), it is a set of markup tags. HTML documents are described by HTML tags, and each HTML tag describes different document content [13].



### **3.3.5.3 XML:**

XML is a markup language much like HTML it was designed to store and transport data was designed to be self-descriptive [14].

### **3.3.5.4 JavaScript :**

JavaScript is a dynamic computer programming language. It is most commonly used as part of Web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. It is also used in server-side network programming with runtime environments [15].

### **3.3.5.5 CSS:**

CSS is a style sheet language used for describing the look and formatting of a document written in a markup language [16].

### **3.3.5.6 JQuery:**

JQuery is a lightweight "write less, do more" JavaScript library. The purpose of jQuery is to make it much easier to use JavaScript on your website. JQuery takes a lot of common tasks that requires many lines of JavaScript code to accomplish, and wraps it into methods that you can call with a single line of code [17].

### **3.3.5.7 PHP :**

PHP is an HTML-embedded Web scripting language. This means PHP code can be inserted into the HTML of a Web page. When a PHP page is accessed, the PHP code is read or "parsed" by the server the page resides on. The output from the PHP functions on the page is typically returned as HTML code, which can be read by the browser. Because the PHP code is transformed into HTML before the page is loaded, users cannot view the PHP code on a page. This make PHP pages secure enough to access databases and other secure information [18].

### **3.3.5.8 Bootstrap :**

Bootstrap is a free collection of tools for creating websites and Web applications. It contains HTML and CSS-based design templates for typography, forms, buttons, navigation and other interface components, as well as optional JavaScript extensions.

Front-end frameworks are toolkits that help Web developers create the front-end, the visible user interfaces of Web pages. They do so by offering many prepackaged user interface components (written in HTML + CSS) and functionalities (written in Javascript) that the web developer can then add to their own pages easily. They are generally created in such a way that the web designer need not know how they work, but simply must know how to integrate them into the page properly. Bootstrap is one such framework [19].

### **3.3.6 UML :**

UML is a general-purpose modeling language in the field of software engineering, which is designed to provide a standard way to visualize the design of a system [20].

### **3.3.7 MD5:**

MD5 is one of the most widely used cryptographic hash functions nowadays. It was designed in 1992 as an improvement of MD4, and its security was widely studied since then by several authors. The best known result so far was a semi free-start collision, in which the initial value of the hash function is replaced by a non-standard value, which is the result of the attack [21].

### **3.3.8 AES Algorithm:**

AES is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

In December 2001, the National Institute of Standards approved the AES as Federal Information Processing Standards Publication, which specifies application of the Rijndael algorithm to all sensitive classified data.

The Advanced Encryption Standard was originally known as Rijndael [22].

### 3.3.9 Google Maps:

Google Maps is a Google service offering powerful, user-friendly mapping technology and local business information-including business locations, contact information, and driving directions [26].

## 3.4 SYSTEM ANALYSIS:

This section represents proposed system analysis including use case diagram, sequence diagram, and activity diagram.

### 3.4.1 Use Case Diagram:

Use case diagram describes functions and actors.

#### 3.4.1.1 Use Case Diagram of Mobile Owner's Operations:

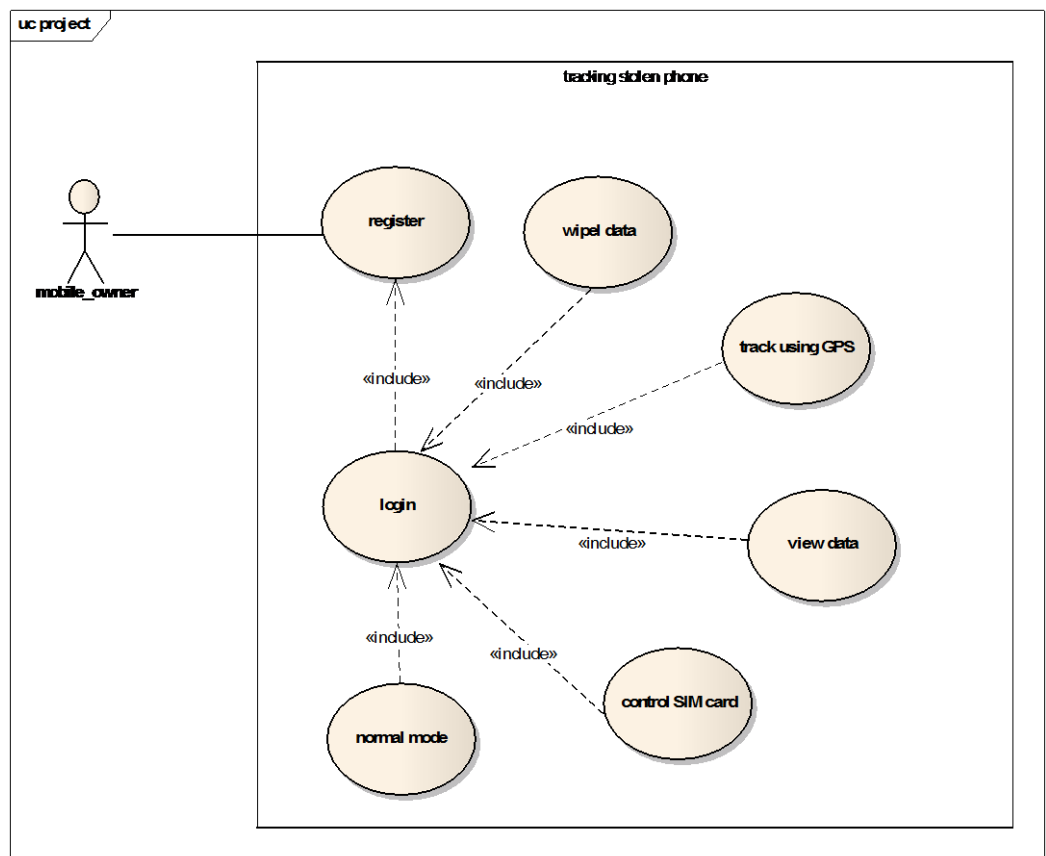


Figure [3.1] Mobile Owner's Use Case Diagram

### 3.4.1.2 Use Case Diagram of System's Operations:

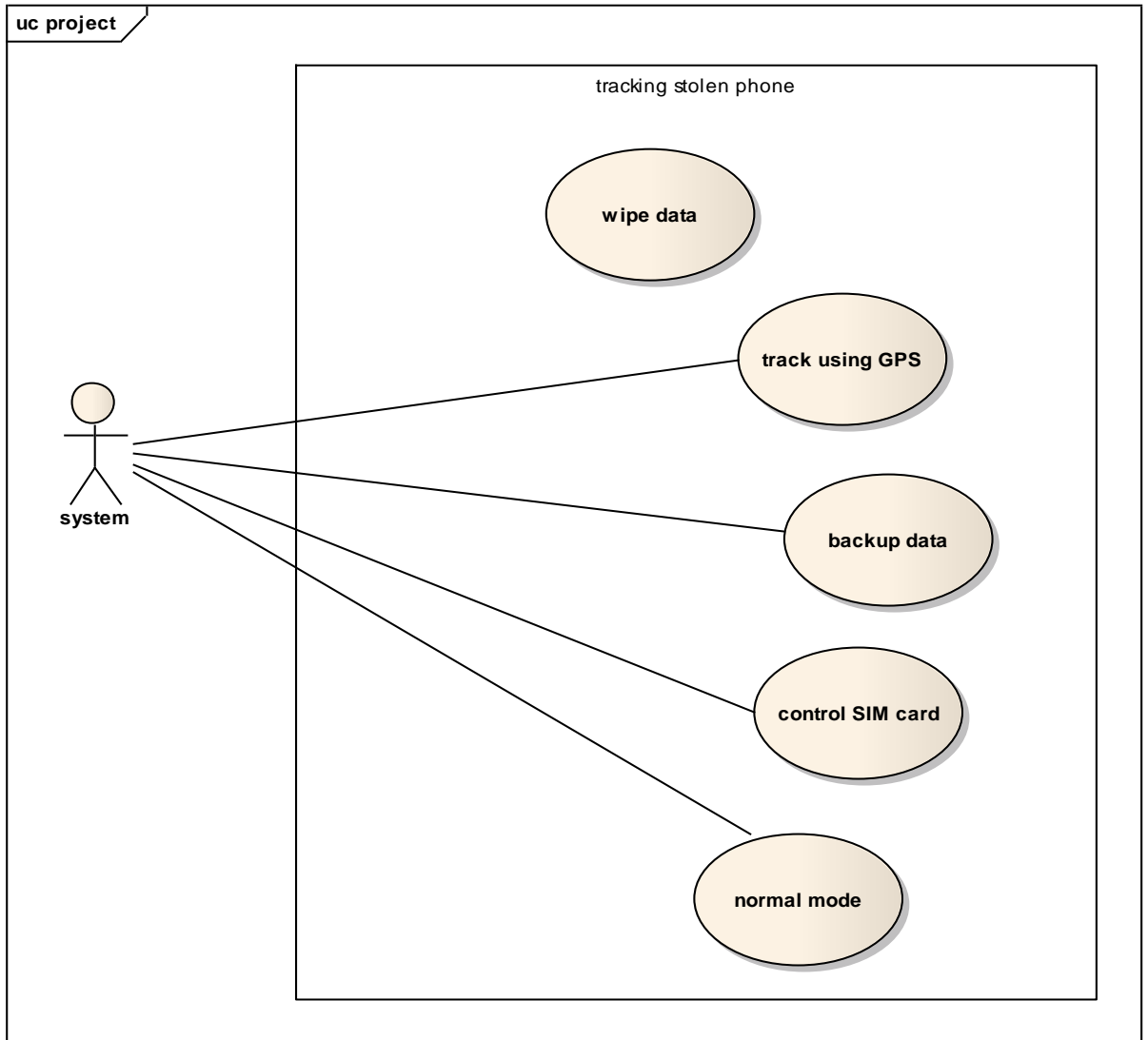


Figure [3.2] System's Use Case Diagram

## 3.4.2 Sequence Diagram:

Sequence diagram shows function sequencing.

### 3.4.2.1 Sequence Diagram of Registration for Any User:

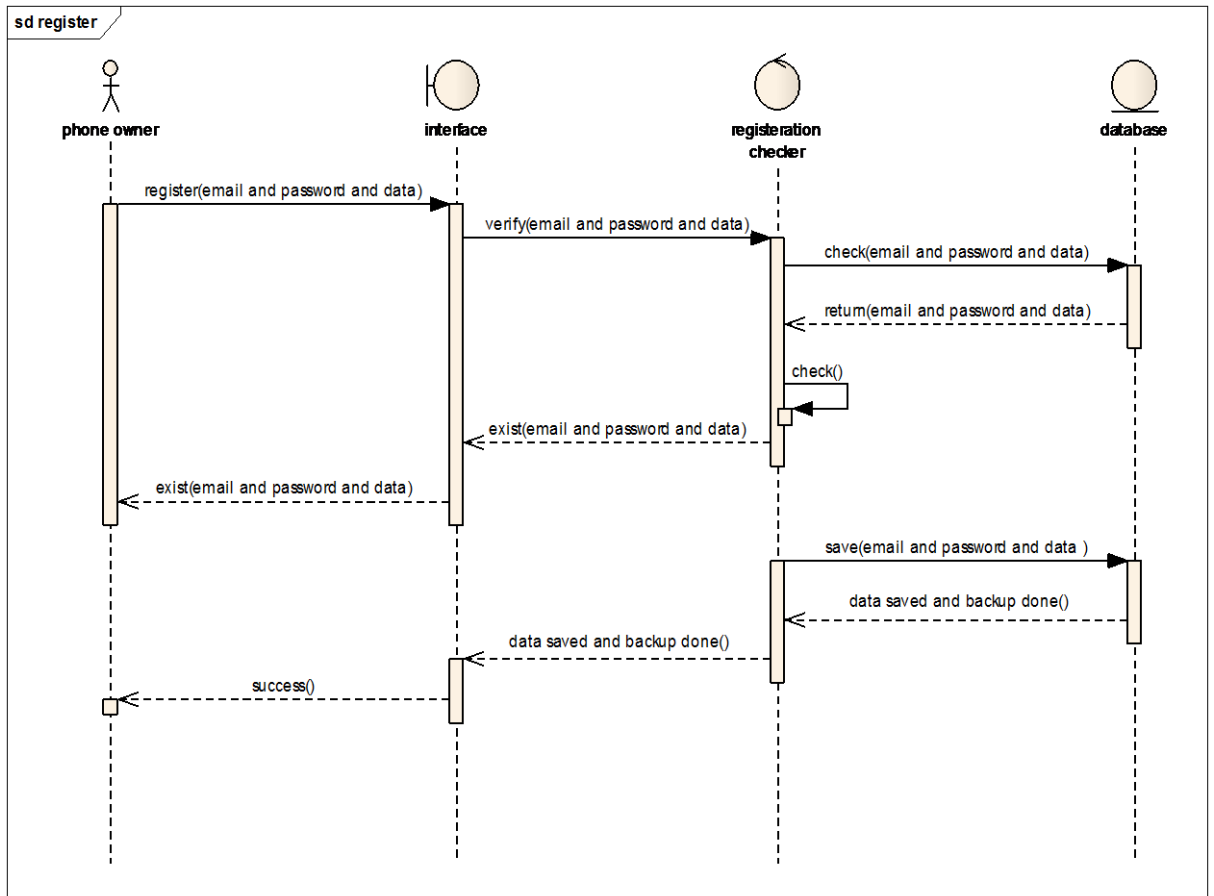


Figure [3.3] User Registration Sequence Diagram

### 3.4.2.2 Sequence Diagram of Login for Any User:

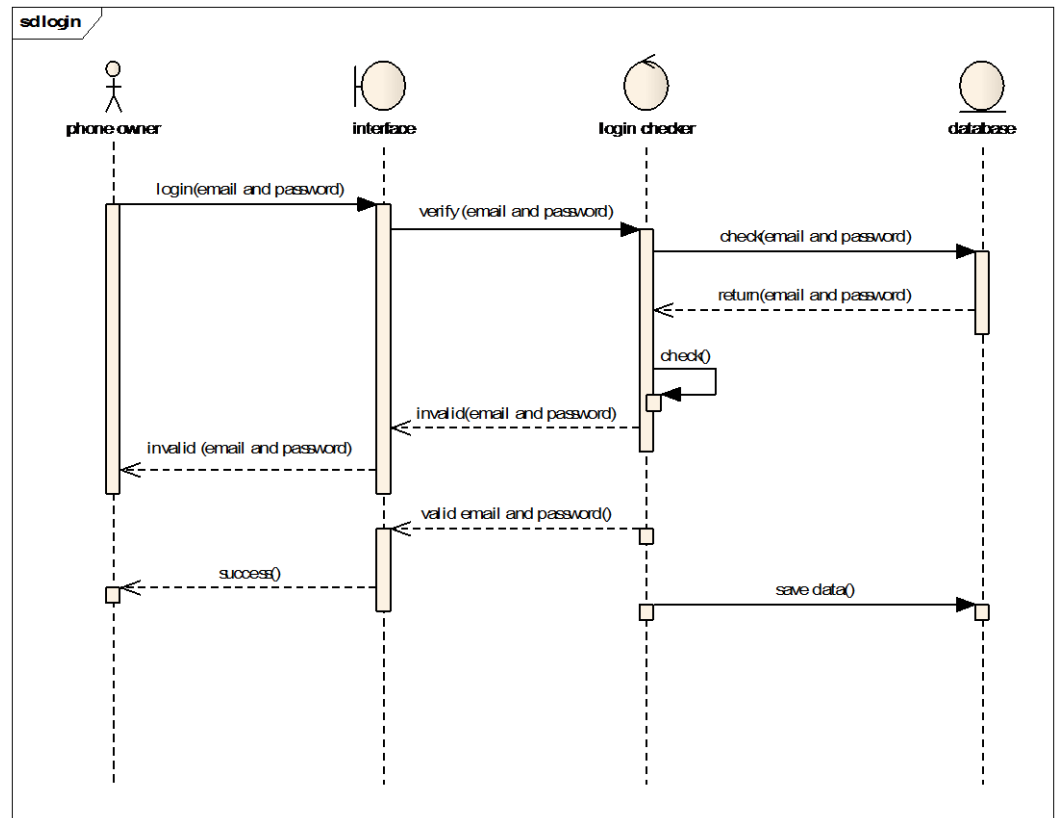


Figure [3.4] User Login Sequence Diagram

### 3.4.2.3 Sequence Diagram of View Data:

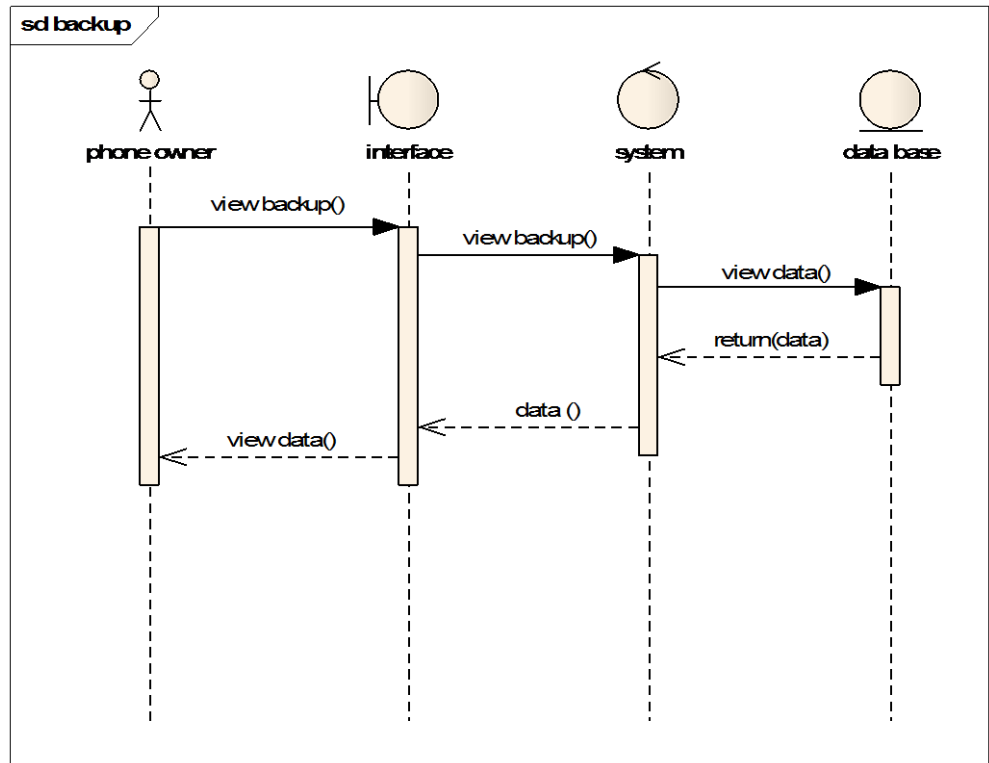


Figure [3.5] View data Sequence Diagram

### 3.4.2.4 Sequence Diagram of Controlling SIM Card:

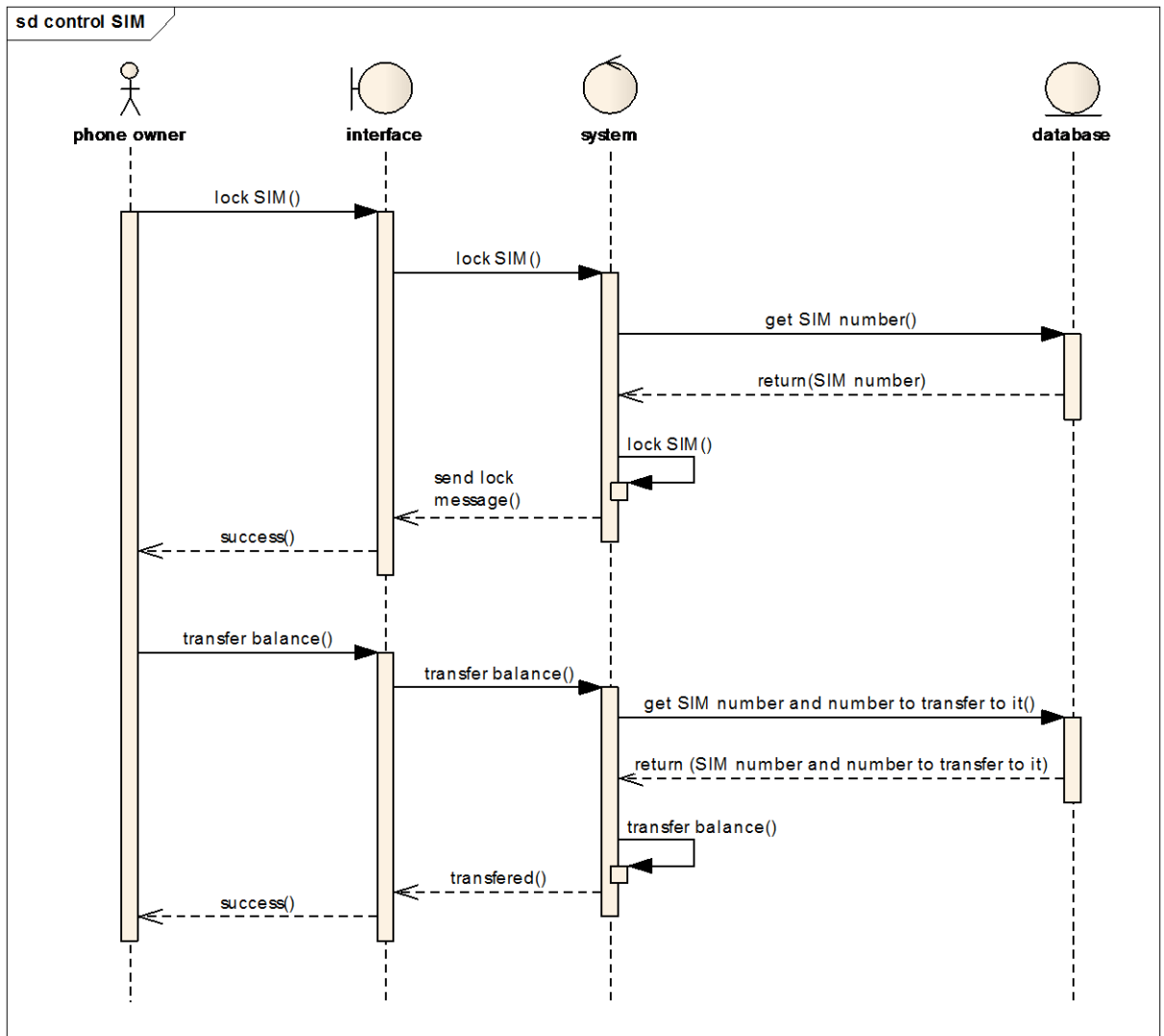


Figure [3.6] Control SIM Card Sequence Diagram



### 3.4.2.5 Sequence Diagram of Changing Mode to Normal:

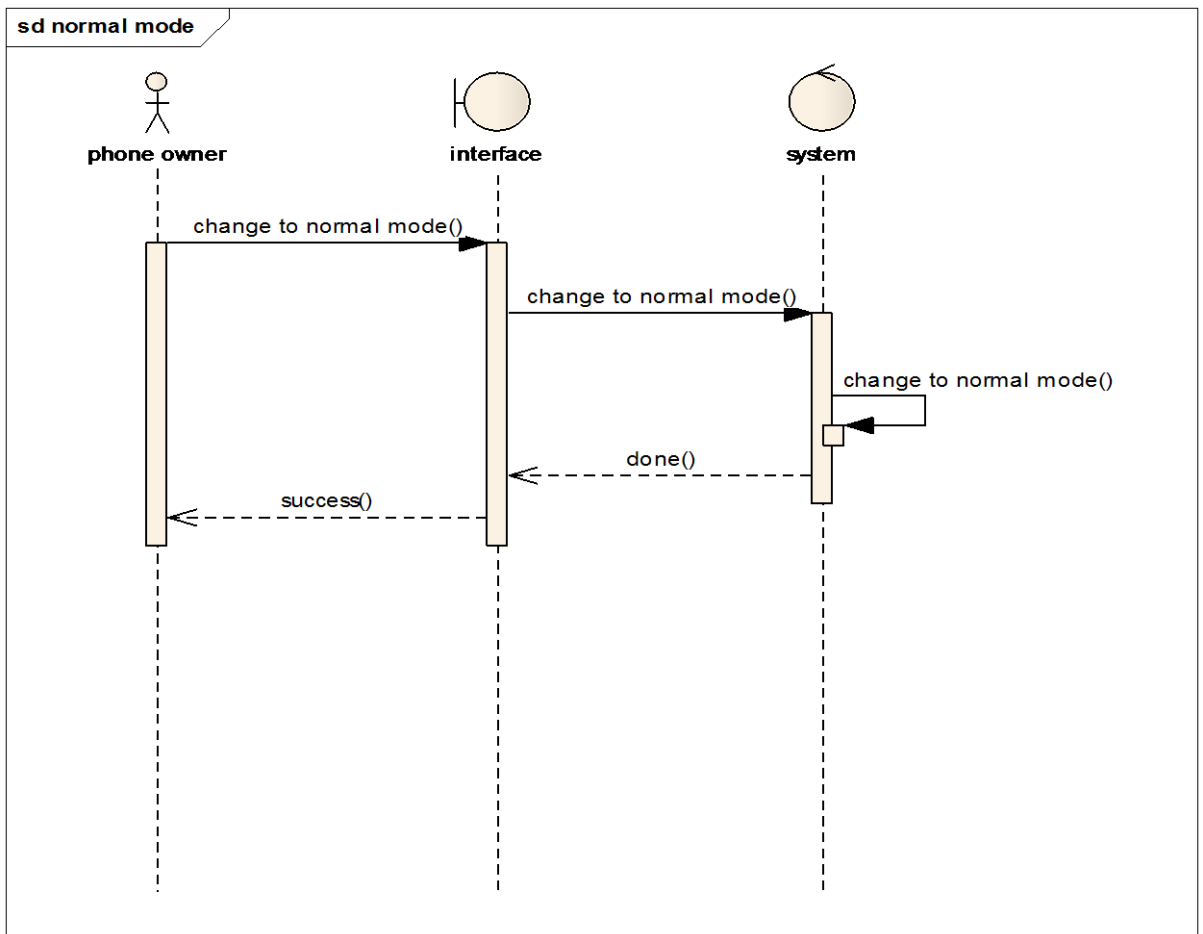


Figure [3.7] Normal Mode Sequence Diagram

### 3.4.2.6 Sequence Diagram of Tracking Phone:

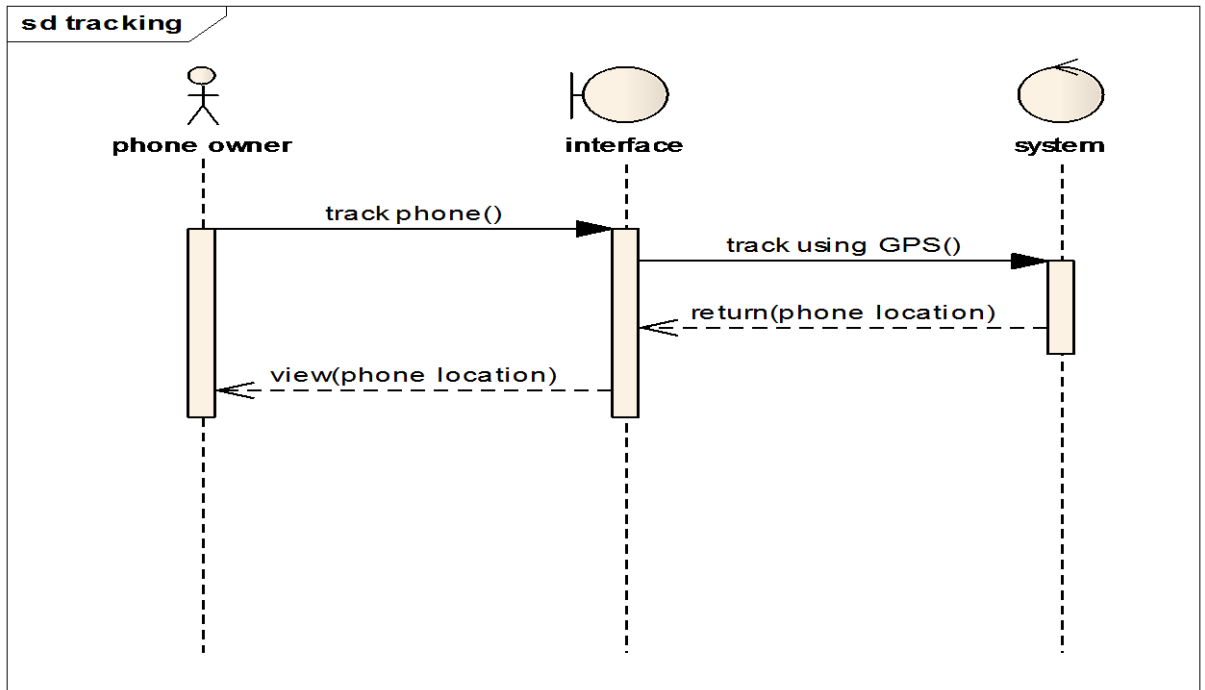


Figure [3.8] Tracking Phone Sequence Diagram

### 3.4.2.7 Sequence Diagram of Wiping Data:

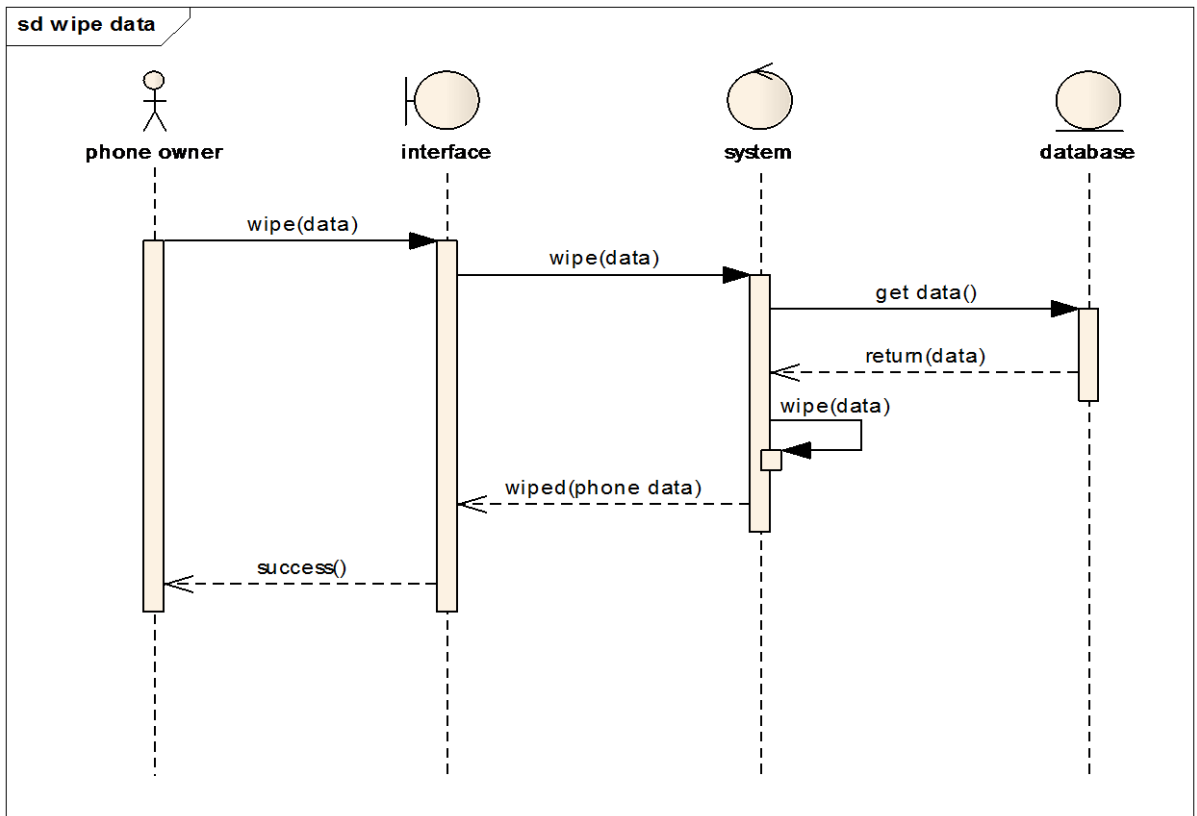


Figure [3.9] Wipe Data Sequence Diagram

### 3.4.3 Activity Diagram:

Activity diagram describes how system works.

#### 3.4.3.1 Activity Diagram for System:

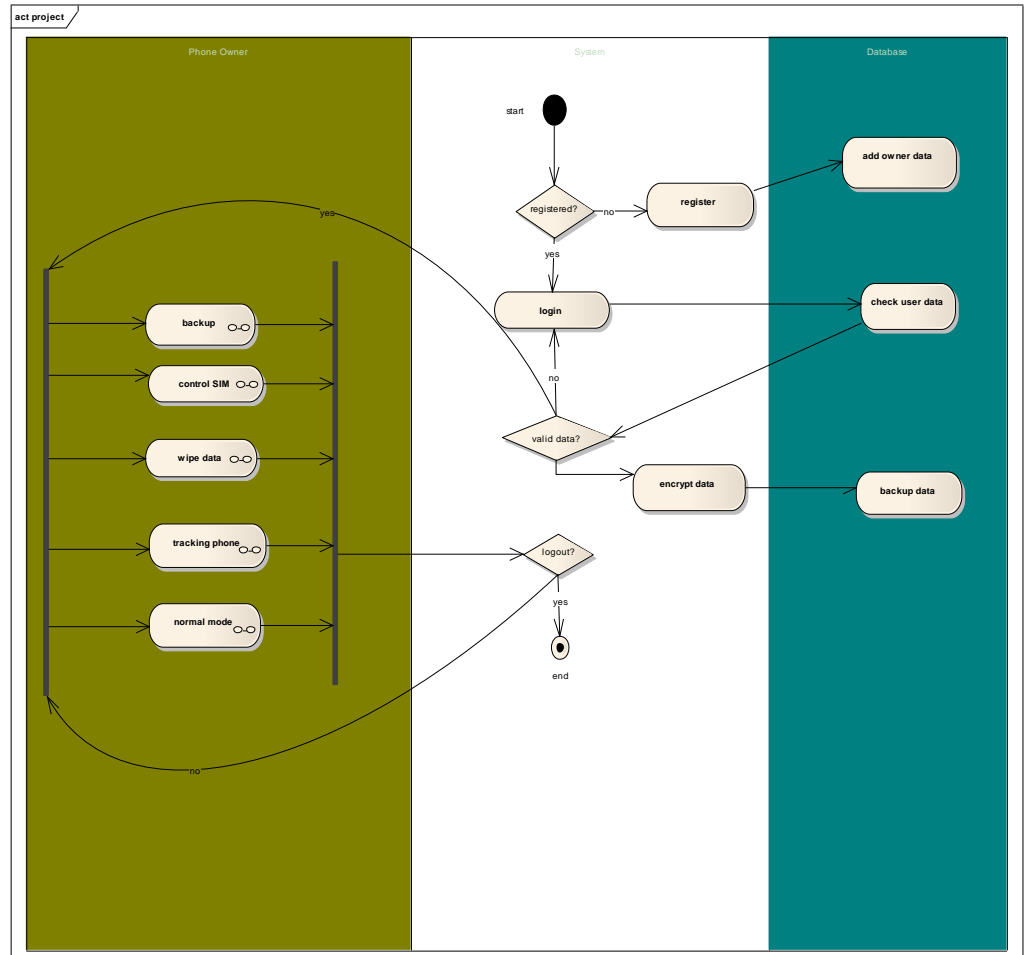


Figure [3.10] System Activity Diagram

### 3.4.3.2 View Data Activity Diagram:

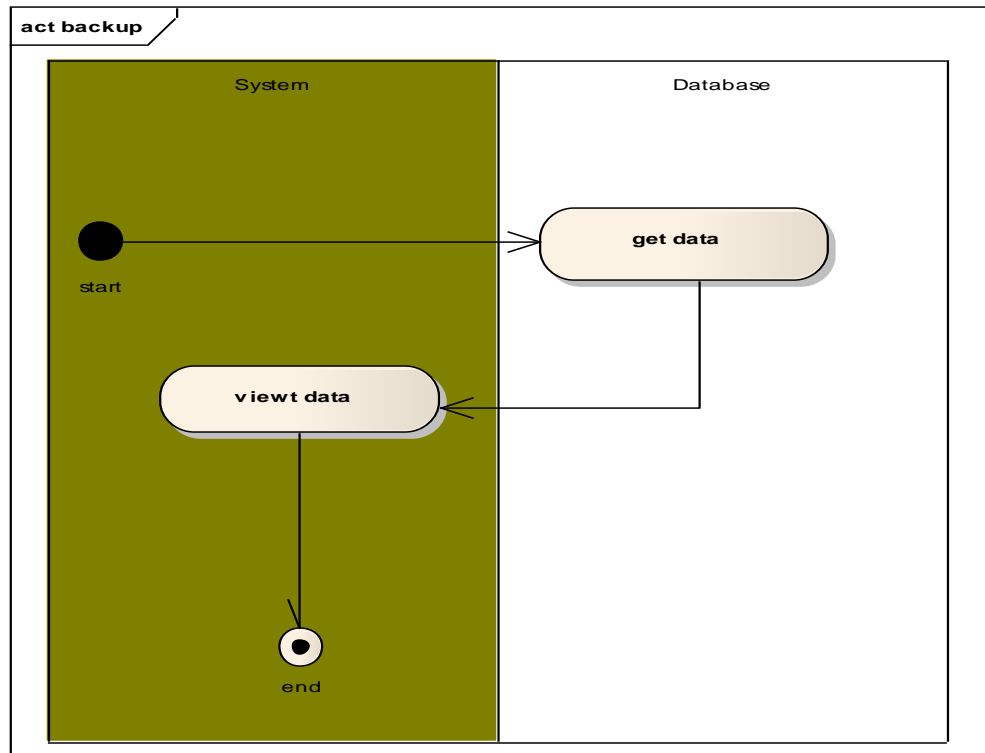


Figure [3.11] View Data Activity Diagram

### 3.4.3.3 Control SIM Card Activity Diagram:

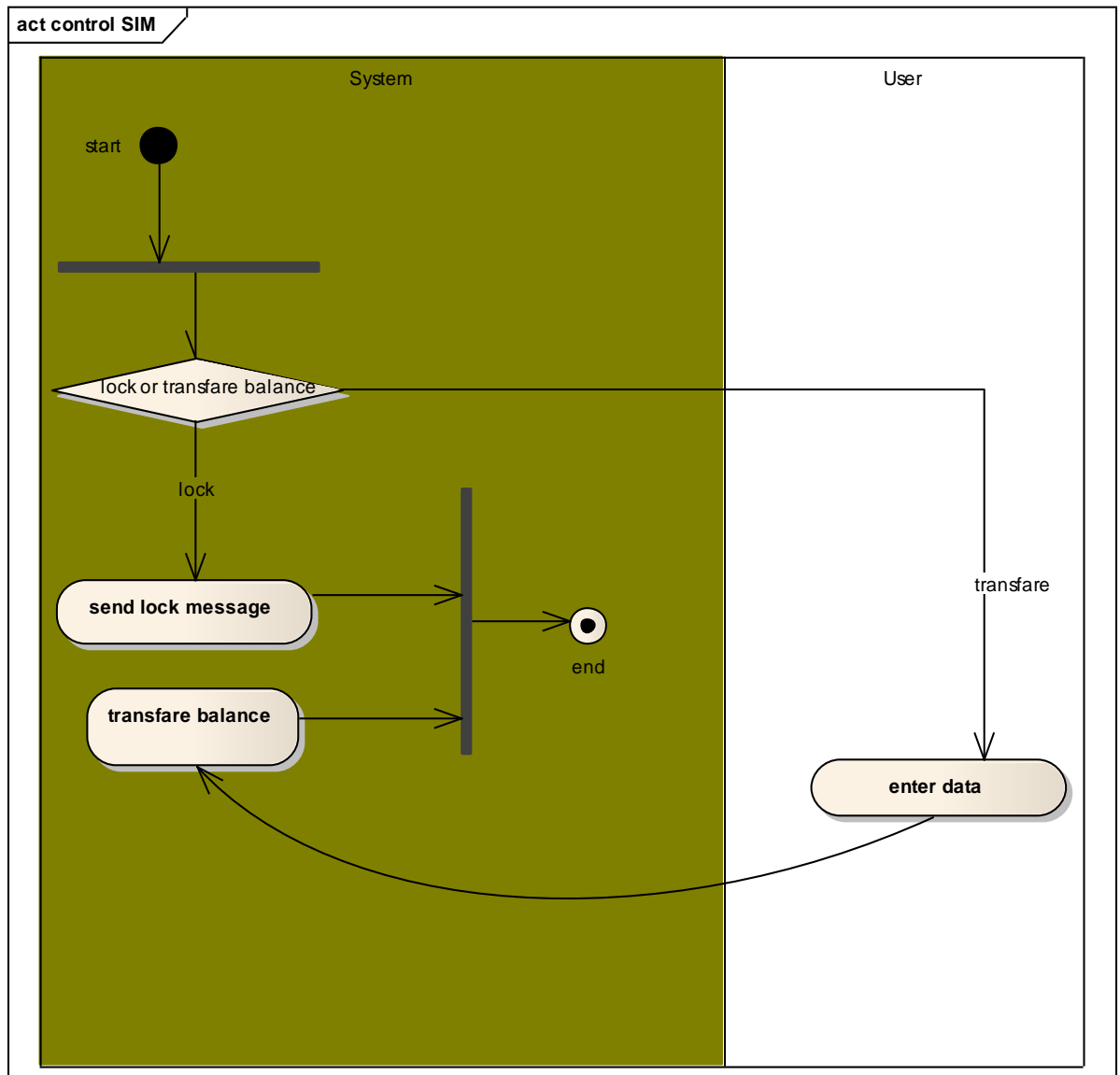


Figure [3.12] Control SIM Card Activity Diagram

### 3.4.3.4 Wipe Data Activity Diagram:

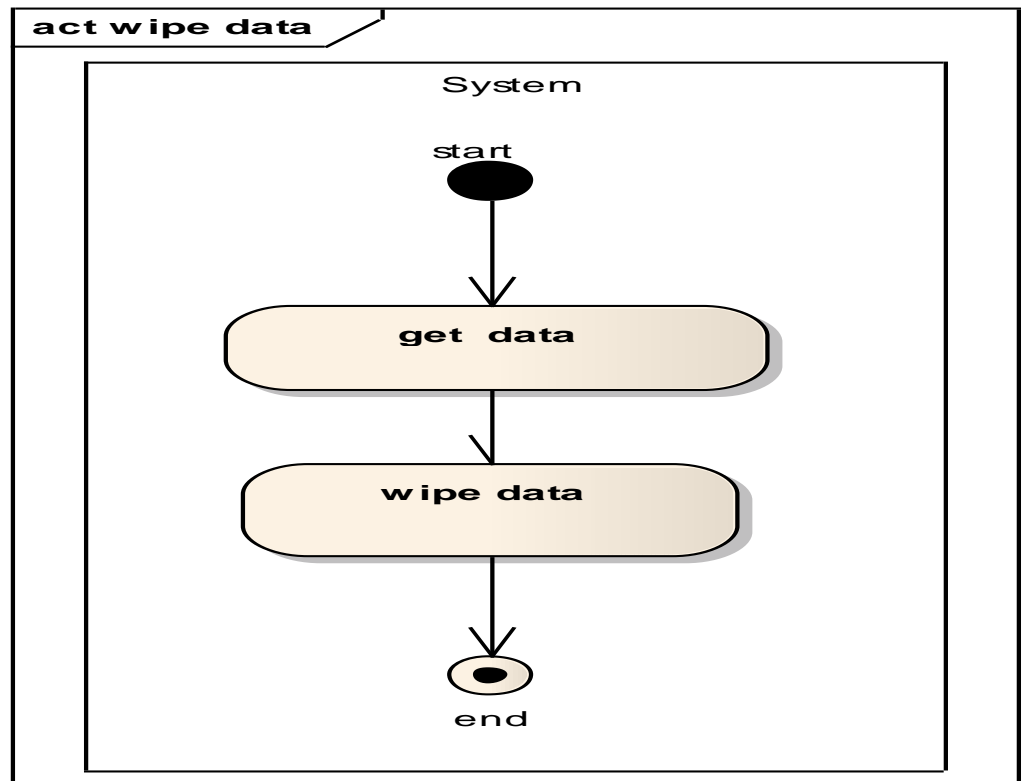


Figure [3.13] Wipe Data Activity Diagram

### 3.4.3.5 Tracking Phone Activity Diagram:

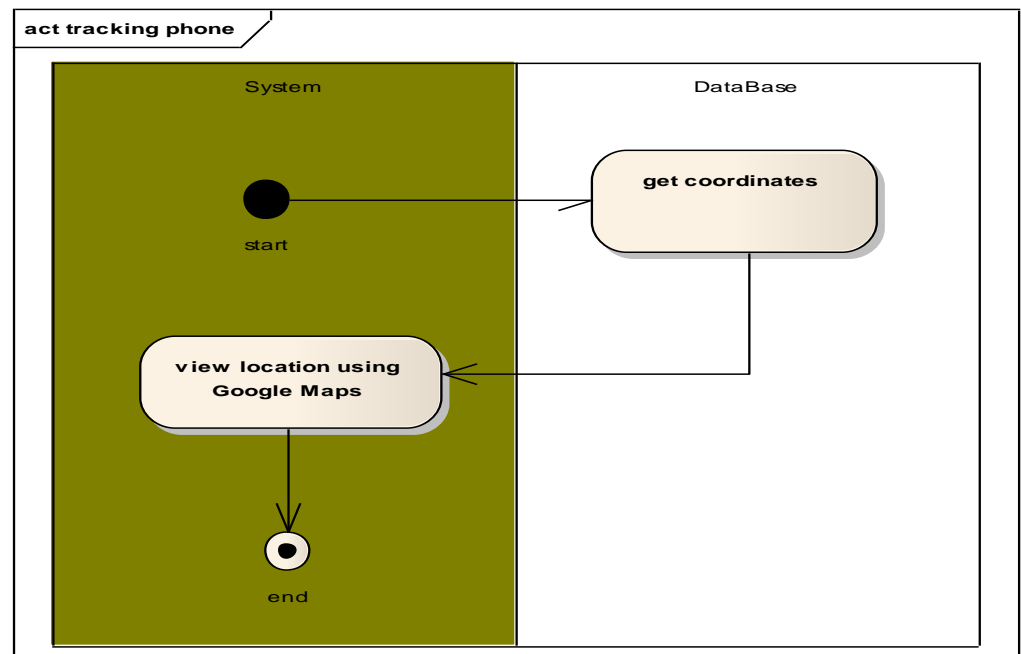


Figure [3.14] Tracking Phone Activity Diagram

### 3.4.3.6 Normal Mode Activity Diagram:

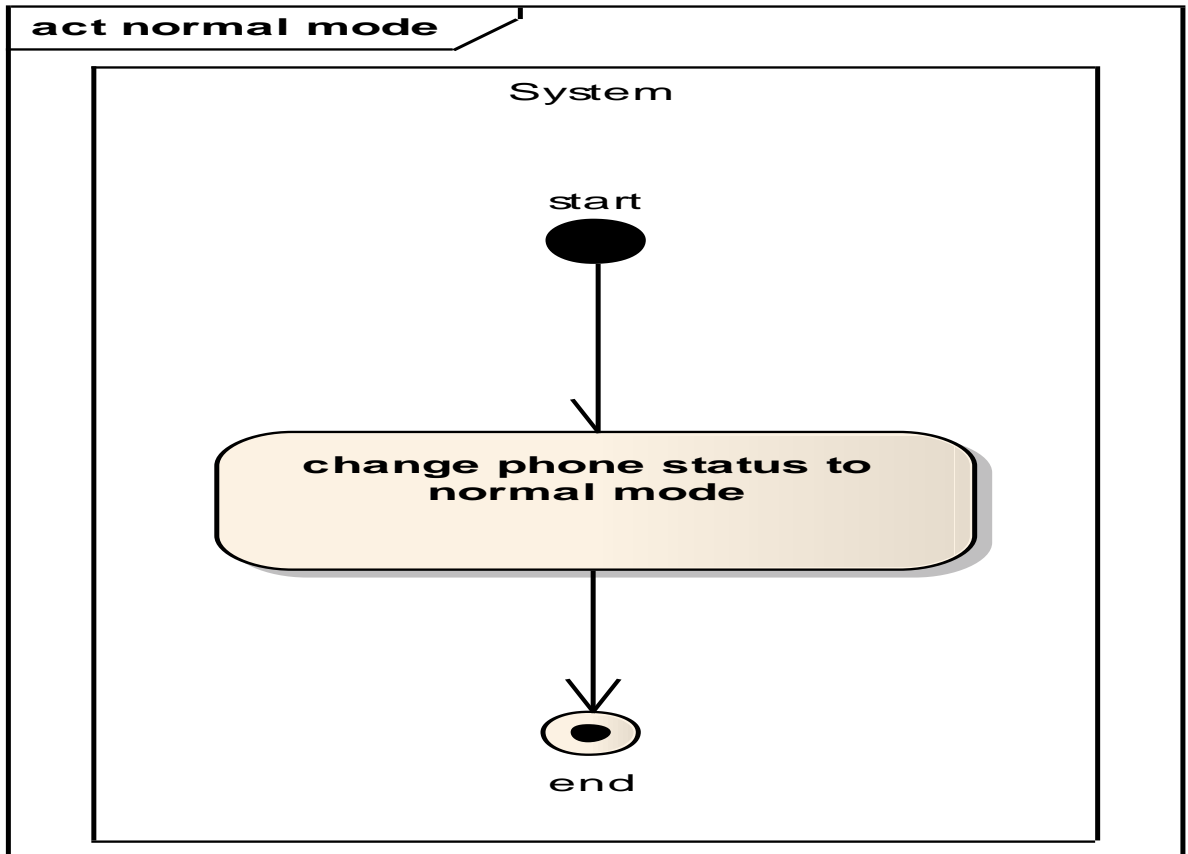


Figure [3.15] Normal Mode Activity Diagram



# **CHAPTER 4**

## **IMPLEMENTATION**

**4.1 SECTION ONE: INTRODUCTION**

**4.2 SECTION TWO: HOW THE SYSTEM  
WORKS**

**4.3 SECTION THREE: SYSTEYM SCREENS**

## **4.1 INTRODUCTION:**

This chapter contains two sections, the first section is about how system works, this section shows important classes that are used in implementation, and the second one is about system screens.

## **4.2 HOW THE SYSTEM WORKS:**

This section describes important libraries and classes that are used to develop the system.

### **4.2.1 Using the Apache HttpClient:**

The Apache HttpClient library simplifies handling HTTP requests. You retrieve and send data via the HttpClient class. An instance of this class can be created with `new DefaultHttpClient ()`.

`DefaultHttpClient` is the standard `HttpClient` and uses the `SingleClientConnManager` class to handle HTTP connections.

`SingleClientConnManager` is not thread-safe; this means that access to it via several threads will create problems.

The `HttpClient` uses an `HttpRequest` to send and receive data. Important subclasses of `HttpRequest` are `HttpGet` and `HttpPost`. You can get the response of the `HttpClient` as an `InputStream` [23].

In implementation we use this technology to connect android with web pages. The class is called `HttpRmi` this class contains URL to web pages and execution of requests. Requests are sent by `AsyncTask` class in android and wait for response from web page.

### **4.2.2 Using the AsyncTask class:**

`AsyncTask` is an abstract class provided by Android which helps us to use the UI thread properly. This class allows us to perform long/background operations and show its result on the UI thread without having to manipulate threads.

Android implements single thread model and whenever an android application is launched, a thread is created. Assuming we are doing network

operation on a button click in our application. On button click a request would be made to the server and response will be awaited. Due to single thread model of android, till the time response is awaited our screen is non-responsive. So we should avoid performing long running operations on the UI thread. This includes file and network access.

To overcome this we can create new thread and implement run method to perform this network call, so UI remains responsive.

But since Android follows single thread model and Android UI toolkit is not thread safe, so if there is a need to make some change to the UI based on the result of the operation performed, then this approach may lead some issues. So the Android framework has given a very good pattern which is enveloped into AsyncTask.

The AsyncTask class has four methods:

1. **doInBackground**: Code performing long running operation goes in this method. When onClick method is executed on click of button, it calls execute method which accepts parameters and automatically calls doInBackground method with the parameters passed.
2. **onPostExecute**: This method is called after doInBackground method completes processing. Result from doInBackground is passed to this method.
3. **onPreExecute**: This method is called before doInBackground method is called.
4. **onProgressUpdate**: This method is invoked by calling publishProgress anytime from doInBackground call this method [24].

## 4.3 SYSTEM SCREENS:

This section represents screens that are provided by the system.

### 4.3.1 System's Main Screen:

The screen represents main screen to everyone visits the site. A user can login or register from this page by clicking the button either for login or register. Figure [4.1] shows the home page.

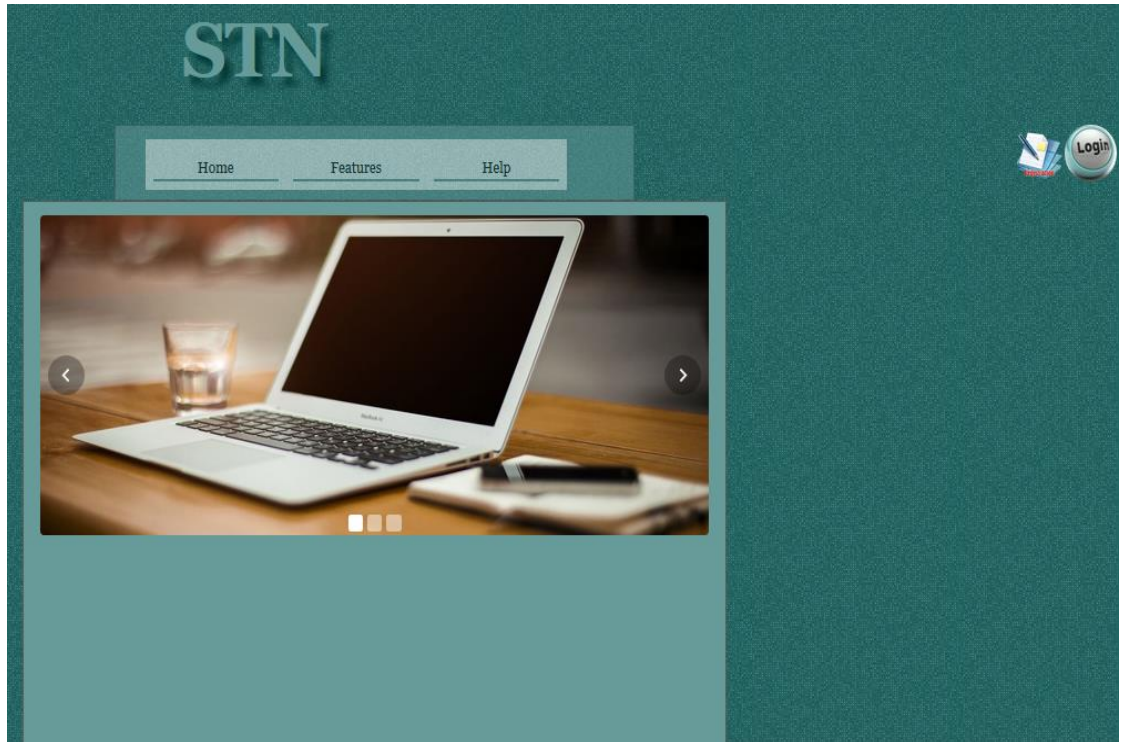


Figure [4.1] Home Page

Also there is a help page appears after pressing in a button which is found in home page. Help page views tips to how system works and how to use it. Figure [4.2] shows the help screen.

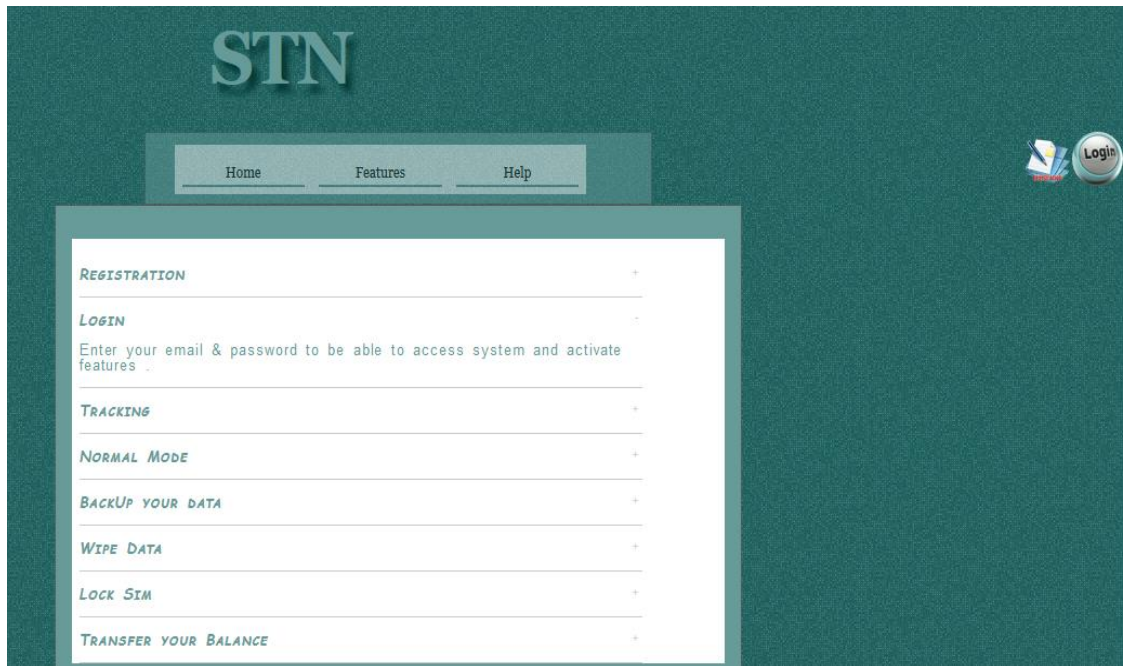


Figure [4.2] Help Screen

There is another page appears after pressing button called features. Features page views main features in the system. Figure [4.3] shows the features screen.



Figure [4.3] Features Screen

### 4.3.2 Registration Screen:

The screen appears after user's click the registration button in home page. This process enables user to have a new account by entering the required fields of data. Figure [4.4] shows the screen of registration.



Figure [4.4] Registration Screen

### 4.3.3 Login Screen:

After registration, the user can access to system by login to profile by entering E-mail and password .This screen appears when you press on login button in home page. Figure [4.5] shows login screen in web page.



Figure [4.5] Login Screen in Web Page

The user also must login from his/her android device to enable and start all features in the system. Figure [4.6] shows login screen in android application.



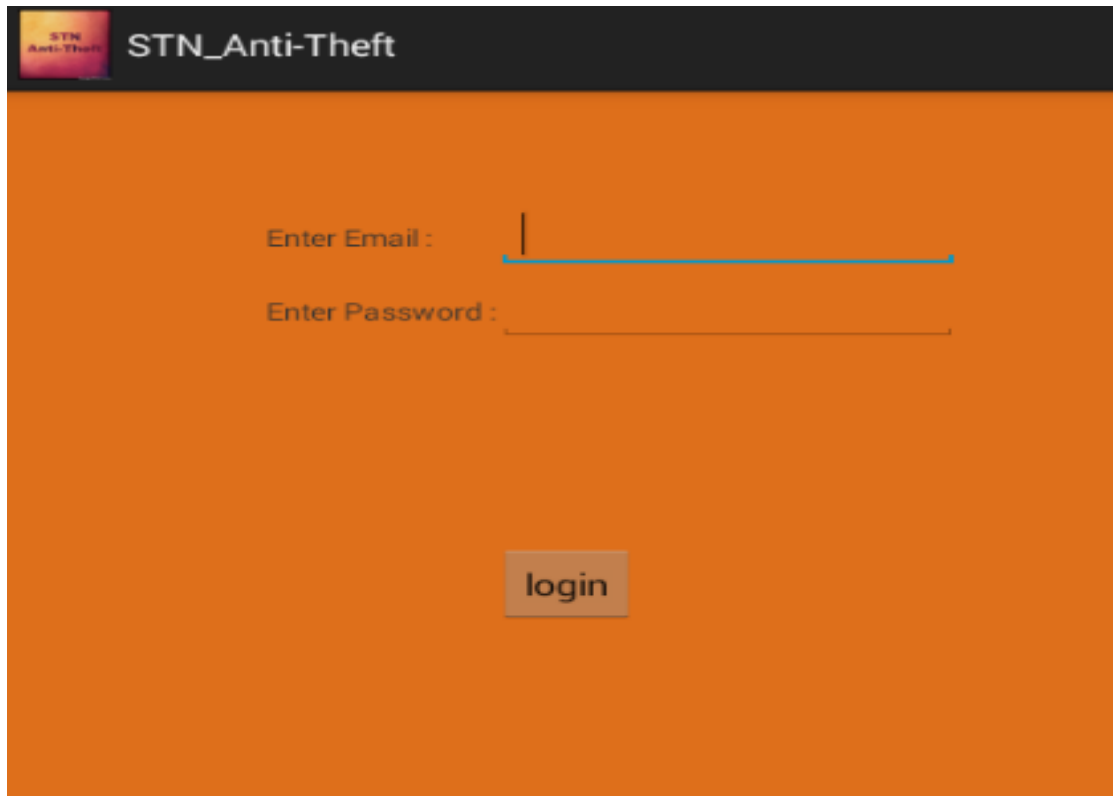


Figure [4.6] Login Screen in Android

#### 4.3.4 User Profile Screen:

After login the user can control his phone from this web page that shows features in menu. Figure [4.7] shows user profile in web.

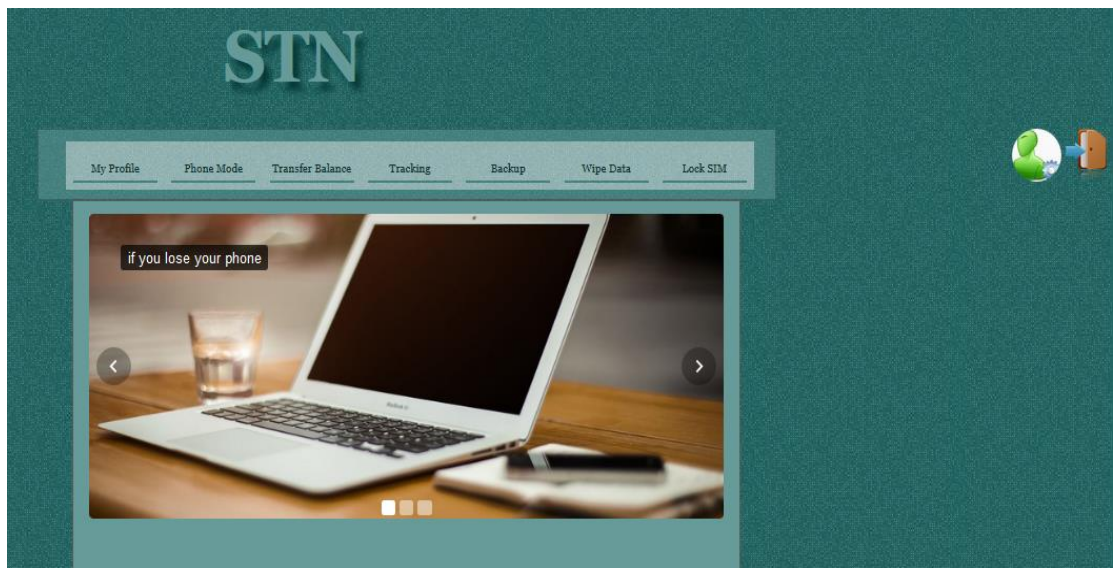


Figure [4.7] User Profile in Web

A user profile screen also appeared in android after login. This screen shows to user that all services started and there is a button to disable normal mode. Figure [4.8] shows user profile in android.

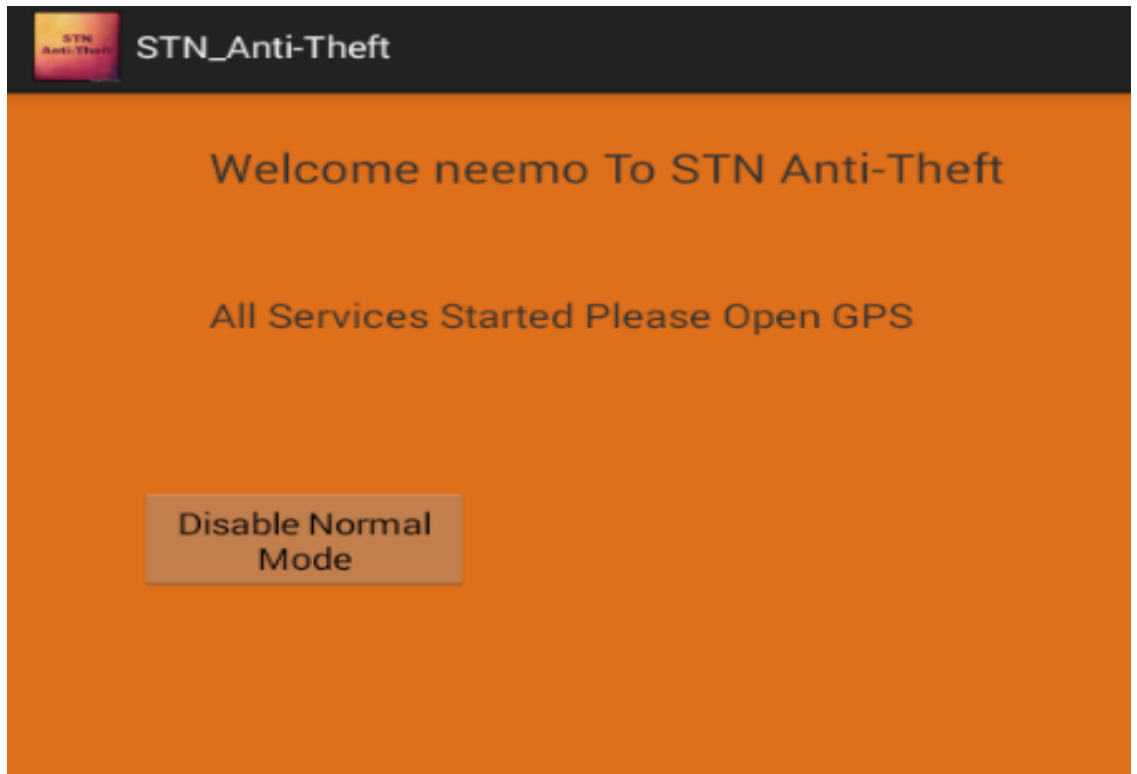


Figure [4.8] User Profile in Android

### 4.3.5 Backup Screen:

In user profile page there is a button which is called backup that the user can view its data by pressing button which found in this page. Figure [4.9] shows backup page in web.

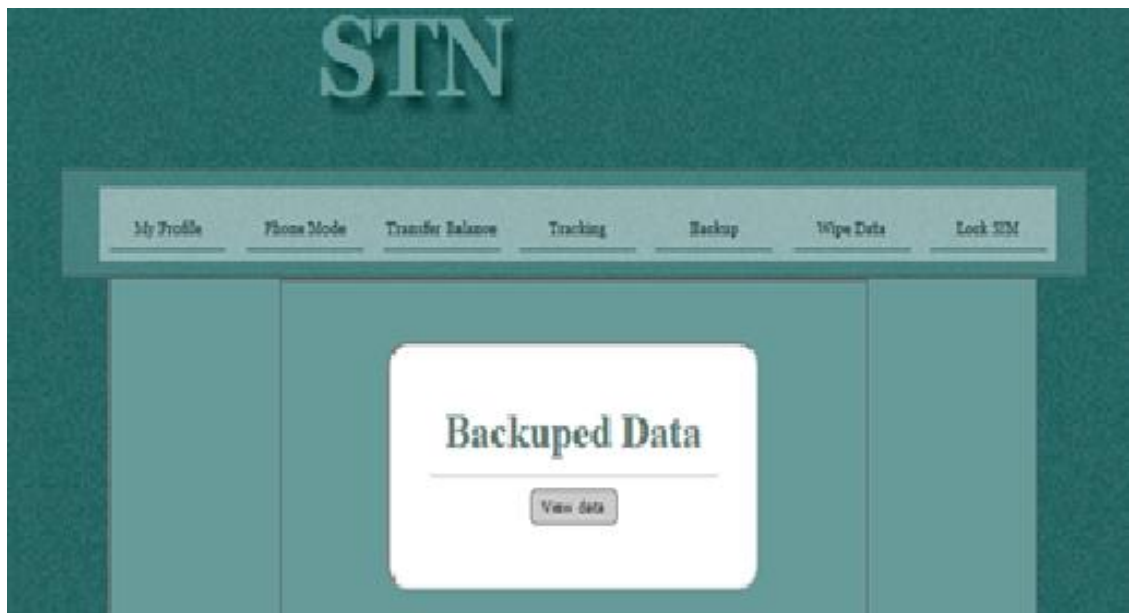


Figure [4.9] Backup Page

When user clicks on view data button his/her data will appear. Figure [4.10] shows the view of user's data.



Figure [4.10] View of User's Data

### 4.3.6 Wipe Data Screen:

In user profile page there is also a button which is called wipe data .The user can wipe data from phone by pressing it and this process must be done just one time after phone is theft. Figure [4.11] shows wipe data page in web.



Figure [4.11] Wipe Data Page

### 4.3.7 Lock SIM Screen:

In this page there is a button that allows lock SIM by sending a message from user device to administrator device after pressing lock SIM button.

This process must be done just one time after phone is theft. Figure [4.12] shows lock SIM page in web.



Figure [4.12] Lock SIM Page

### 4.3.8 Transfer Balance Screen:

The screen appears after a user presses on a transfer balance button in profile. There is a form in this page contains a number to receive transferred balance ,the amount of balance to be transferred and a button that confirm the process of transferring after pressing it. Figure [4.13] shows transfer balance page in web.



Figure [4.13] Transfer Balance Page

### 4.3.9 Tracking Screen:

The screen appears after pressing tracking button in user profile. After that a user can see the location of the device in Google Maps as a coordinates returned from the device itself via GPS. Figure [4.14] shows tracking page in web.



Figure [4.14] Tracking Page

### 4.3.10 Normal Mode Screen:

In user profile page there is also another button that shows normal mode page which allows to user changing his phone status to be normal continuously. Figure [4.15] shows normal mode page in web.



Figure [4.15] Phone Mode Page

The user can disable this service from the device. Figure [4.8] shows user profile in android.

# **CHAPTER 5**

## **RESULTS AND DISCUSS**

## 5.1 RESULTS:

These following results have been obtained after applying the system in more than one device:

1. Show device current location in web page using Google Maps by getting coordinates from the device via GPS.
2. Secure the channel between android and Web using AES Algorithm and MD5.
3. Send encrypted backup contacts to MySQL database.
4. Put the device in normal mode.
5. Wipe contacts from user's device.
6. Transfer balance that found in the SIM card.
7. Simulate locking SIM card via sending message to administrator number.

## 5.2 COMPARISON BETWEEN STN ANTI-THEFT AND OTHER APPLICATIONS IN GOOGLE PLAY:

<b>Name</b>	<b>Size</b>	<b>Android Version</b>	<b>Functions And Requirements</b>
STN Anti-Theft	0.91M	2.2 and up	Location , SMS, network communication, personal info ,storage , services that cost you money
Prey Anti-Theft	4.2M	2.3 and up	Identity, Location ,SMS
Cerberus Anti- Theft	7.2M	4.0.3 and up	Identity, Contacts, Location, SM , Phone, Media, Camera, Other
Avast Anti-	Varies with	Varies with	Identity, Contacts, Calendar,



Theft	device	device	Location, SMS, Phone, Media , Camera, Other
-------	--------	--------	--

Table [5.1] Comparison between STN Application and Other Applications

## 5.3 COMPARISON BETWEEN STN ANTI-THEFT AND PREY ANTI-THEFT:

Figure [5.1] represents comparison between our application and Prey Ant-Theft application. The functionality of STN application is high compare to its size, but the functionality of Prey application is low compare to its size.

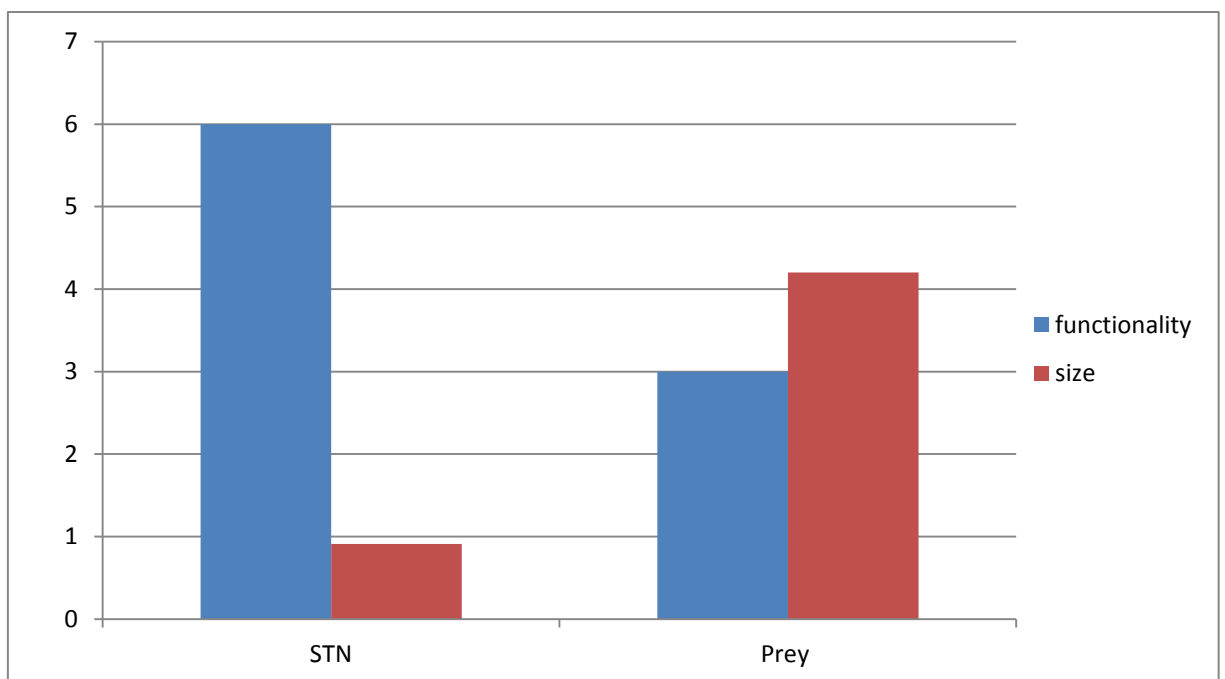


Figure [5.1] Comparison between STN and Prey

## 5.4 AES Algorithm Performance:

Figure [5.2] represents that AES and Rinjdael provide the best performance, partly due to the fact that they are purely managed. RC2, DES and 3DES are older algorithms and in term of security not the most reliable so best to be avoided [25].

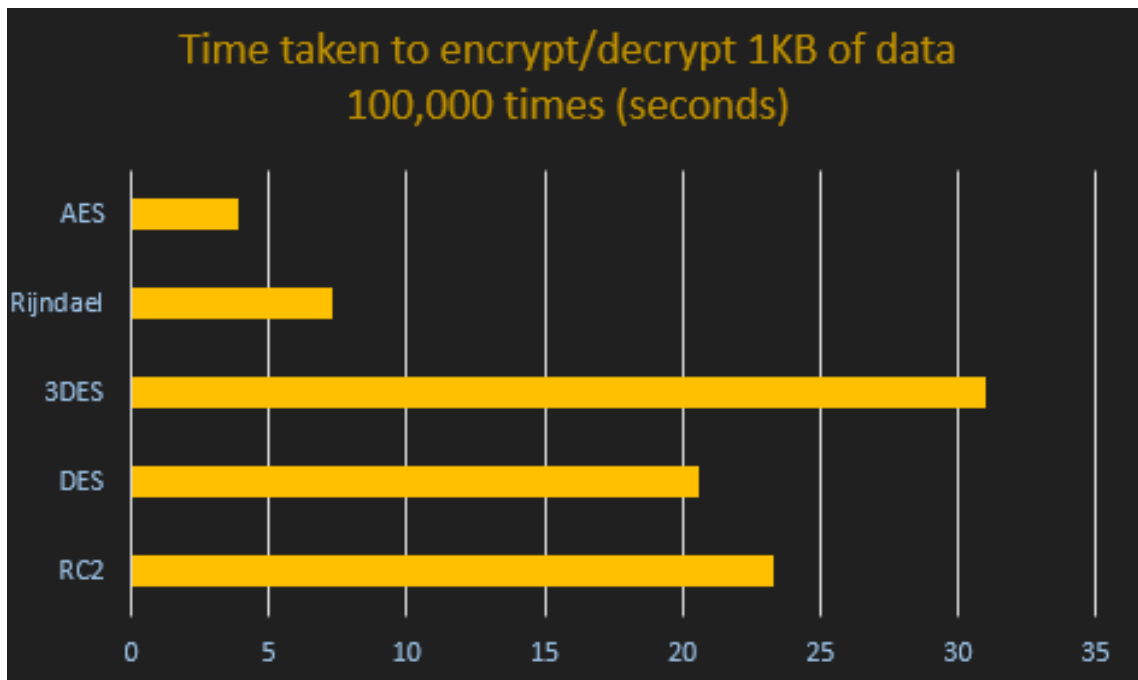


Figure [5.2] Performance of AES Algorithm

**CHAPTER 6**

**CONCLUSION AND  
RECOMMENDATIONS**

## **6.1 CONCLUSION:**

Smart phones become widely used in everywhere and everyone wants to save the data and phone from lost.

This research and by Anti-Theft application a person can save important data from loss and find the phone if it lost.

## **6.2 RECOMMENDATIONS:**

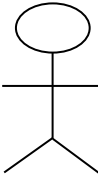


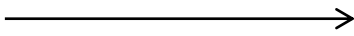
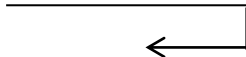
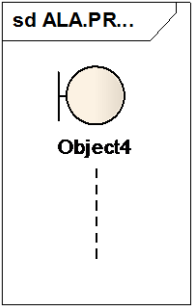
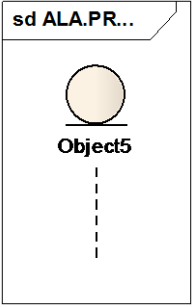
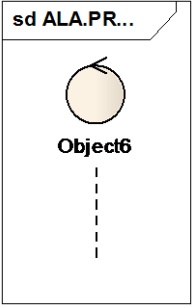
To make the application more strong and reliable we recommend doing more tasks that we didn't achieve:

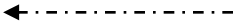
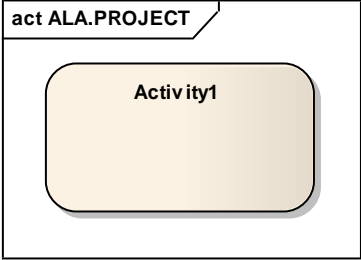
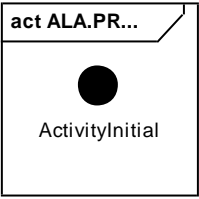
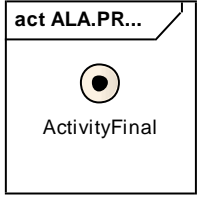

1. Run the application in different platforms not the android only.
2. Backup all storage of the device.
3. Make SIM control more powerful by achieving validation on transferring balance and locking SIM card, also add more features.
4. Apply more security levels.
5. Switch the device on by booting.

# **APPENDIXES**

# **Appendix I**

## **UML Notations**

	<p>Actor</p>
	<p>Use Case</p>
	<p>Association</p>
	<p>Message</p>
	<p>Self Message</p>
	<p>Boundary</p>
	<p>Entity</p>
	<p>Control</p>

	<p>Include</p>
	<p>Activity</p>
	<p>Initial Activity</p>
	<p>Final Activity</p>
	<p>Fork/Join</p>



# **Appendix II**

## **Eclipse Versions**

## Eclipse Releases:

Since 2006, the Eclipse Foundation has coordinated an annual Simultaneous Release. Each release includes the Eclipse Platform as well as a number of other Eclipse projects. Until the Galileo release, releases were named after the moons of the solar system.

So far, each Simultaneous Release has occurred at the end of June [28].

<b>Release</b>	<b>Date</b>	<b>Platform version</b>
Mars	24 June 2015	4.5
Luna	25 June 2014	4.4
Kepler	26 June 2013	4.3
Juno	27 June 2012	4.2
Indigo	June 2011	3.7
Helios	23 June 2010	3.6
Galileo	24 June 2009	3.5
Ganymede	25 June 2008	3.4
Europa	29 June 2007	3.3
Callisto	30 June 2006	3.2
Eclipse 3.1	28 June 2005	3.1
Eclipse 3.0	28 June 2004	3.0

Figure [II-1] Eclipse Versions

# REFERENCE

## References:

- [1] Ashima Singh & Navneet Kaur (2013), Generating More Reusable Components while Development: A Technique, International Journal of Innovative Technology and Exploring Engineering (IJITEE), p 215.
- [2] wikipedia (2015), [https://en.wikipedia.org/wiki/Anti-theft\\_system/](https://en.wikipedia.org/wiki/Anti-theft_system/), 9/10, 14:08.
- [3] Clancy, Heather (2015), [https://en.wikipedia.org/wiki/Tracking\\_system](https://en.wikipedia.org/wiki/Tracking_system), 25/9, 23:59.
- [4] Muheet Ahmed Butt, & Majid Zaman (2013), "Enterprise Data Backup & Recovery: A Generic Approach," IOSR Journal of Engineering (IOSRJEN), vol. 3.
- [5] Ziff Davis (2015), <http://www.pcmag.com/encyclopedia/term/61745/simcard>, 19/4, 12:40.
- [6] Reem Al-Rayah and others "Control Mobile Remotely ", July 2012.
- [7] Tech Shortly (2012), <http://www.techshortly.com/2012/07/5-best-free-anti-theft-apps-for-android.html>
- [8] W.M. Lee (2011), "Android Application Development", 16/10.
- [9] Eclipse Foundation (2015), <http://www.csee.umbc.edu/courses/undergraduate/341/fall08/Lectures/Eclipse/intro-to-eclipse.pdf>, 23/4.
- [10] P. H. DANA (1997), "Global Positioning System (GPS) Time Dissemination for Real Time Applications", 16/4.
- [11] Eightfold Infotech (2013), [http://www.eightfoldit.com/studyforjava/j2se/pro\\_fun/what\\_is\\_java.php](http://www.eightfoldit.com/studyforjava/j2se/pro_fun/what_is_java.php), 24/4, 4:40.

- [12]Vangie Beal(2015), <http://www.webopedia.com/TERM/W/WAMP.html>, 24/4, 4:45.
- [13] w3schools(2015), [http://www.w3schools.com/html/html\\_intro.asp](http://www.w3schools.com/html/html_intro.asp).
- [14] w3schools(2015),[http://www.w3schools.com/xml/xml\\_what\\_is.asp](http://www.w3schools.com/xml/xml_what_is.asp).
- [15] David, Ferguson. Flanagan, Paula (2006), "JavaScript: The Definitive Guide".
- [16]Scott Clark(2015),  
<http://www.htmlgoodies.com/beyond/article.php/3893911/Web-based-Mobile-Apps-of-the-Future-Using-HTML-5-CSS-and-JavaScript.html>, 13/8.
- [17]SethFreeman(2012),  
<http://www.ccc.commnet.edu/faculty/sfreeman/cst%20250/jQueryNotes>, 25/3, 10:15.
- [18]Sharpened (2015), <http://techterms.com/definition/php>, 25/4, 11:30.
- [19]Web\_design(2014),  
[http://cs.nyu.edu/~amos/courses/web\\_design/?title=Bootstrap](http://cs.nyu.edu/~amos/courses/web_design/?title=Bootstrap), 13/9, 17:01.
- [20] Addison-Wesley & Ivar (2005), "Unified Modeling Language User Guide", Grady Booch.
- [21] Xiaoyun Wang and Hongbo Yu, Shandong University, "How to Break MD5 and Other Hash Functions".
- [22]JanaltaInteractive(2010),  
<https://www.techopedia.com/definition/1763/advanced-encryption-standard-aes>, 11/10.
- [23]Vogella(2013),  
<http://www.vogella.com/tutorials/ApacheHttpClient/article.html>, 22/9.
- [24] Compiletimeerror(2012), [http://www.compiletimeerror.com/2013/01/why-and-how-to-use-async-task.html#.VgF5cH3EZ\\_k](http://www.compiletimeerror.com/2013/01/why-and-how-to-use-async-task.html#.VgF5cH3EZ_k), 22/9, 8:57.

[25]AwsesomeInc(2013), <http://byterot.blogspot.com/2013/01/net-framework-cryptography-symmetric-algorithm-performance-benchmark.html>, Sunday, 20 /6.

[26]Google(2015),  
[http://www.ig.utexas.edu/outreach/googleearth/pdf/Maps\\_JCescalante.pdf](http://www.ig.utexas.edu/outreach/googleearth/pdf/Maps_JCescalante.pdf), 22/2,  
8:02.

[27] kabu(2014), <http://www.onlinetechguru.org/10-best-anti-theft-tracking-apps-for-android-smartphones/>, 26/10/2015, 12:00.

[28] Pascal Thivent(2015), <http://stackoverflow.com/questions/4008976/difference-between-eclipse-europa-helios-galileo>, 23/10, 11:21.