Boomerang

MINOR PROJECT I

Submitted by:

Aditya Bakliwal (9914103132)

Rishabh Jain   (9914103137)

Tarun Agarwal   (9914103141)

Under the supervision of:

Mrs. Ambalika Sarkar

Department of CSE/IT

Jaypee Institute of Information Technology University, Noida

December 2016

ACKNOWLEDGEMENT

Signature of Students

Aditya Bakliwal (9914103132)

Rishabh Jain (9914103137)

Tarun Agarwal (9914103141)

Abstract

Our project 'Boomerang' is a security based anti-theft android application which helps the user to protect their smartphones from being used by someone or being stolen. In today's time, android devices range from low budget devices to high-end flagship devices. Whatever may be the case, a user has a deep connection with his and this application thrives to maintain that connection by trying its best not to get it lost or stolen. It even provides some very basic security features so that the users can be made aware if any installed application is trying to steal data from them.

Overall "Boomerang" is a must have anti-theft security application as it provides an all-round protection to the device.

TABLE OF CONTENTS

Chapter 1: INTRODUCTION

Chapter 2: LITERATURE REVIEW

Chapter 3: OVERALL DESCRIPTION

Chapter 4: SPECIFIC REQUIREMENTS

Chapter 5: Testing

Chapter 6: CONCLUSION AND FUTURE SCOPE

References:

Lists of Abbreviations

GPS   Global Positioning System

API   Application Programming Interface

AOSP   Android Open Source Project

SDK   Software Development Kit

JDK   Java Development Kit

AVD   Android Virtual Device

UI   User Interface

JSON   JavaScript Object Notation

TCP/IP   Transmission Control Protocol/Internet Protocol

HTTP   Hypertext Transfer Protocol

OS   Operating System

SQL   Structured Query Language

Lists of Figures

Grantt Chart

Anti Theft Boomerang																
Project Started Date : 07-Aug-16																
Module/Week	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Project Planning	█															
Requirement Analysis		█														
Overall Architecture		█														
Login Activity			█													
Ringer			█		█											
Apps Permissions			█		█											
SignUp Activity						█										
Ringer :Set Password						█										
List App Permissions						█										
Creative User Interface							█									
Forget Your Password									█			█				
Sms Activitity : Get Location									█							
Pattern Camera : Device Admin									█							
Google/Facebook Sign In												█	█			
Sms Activty : Alarm													█			
Pattern Camera : Auto Capture													█	█		
Delete Account														█		
Signal Flare Activity														█		
Pattern Camera : Send Email														█		
Testing															█	
Bugs Fixing															█	

1 Introduction

This application serves anti-theft and security features to the user running any device which is dependent on android platform. It tries to keep the user updated about the permissions that all the installed applications require and also provides some basic anti-theft features.

1.1 Purpose

The purpose of this document is to present a detailed description of the Android Application that is created to specifically provide users with some security related features which will help them protecting their device. It will explain the features of the system, the interfaces of the system, what the system will do, the constraints under which it must operate and how the system will react to external stimuli in case the device is lost or stolen. This document is intended for the users, evaluator and the developers of the application.

1.2 Scope of the Project

The scope of our project are the users which are using android devices. Our aim is to provide our user with one application that covers their full set of basic security and anti-theft features. The application provides many different various features which increases the security of the android device. From remotely controlling some features to getting the location of the device, all can be achieved using the messaging feature of the android device. This application even tries to capture the photograph of any user who has entered a wrong password/pattern of the device for more than specified number of times. It even intelligently senses low battery in a device, and sends the last known location to an emergency contact/email for added security reasons.

We have used a free database service, Google's firebase, at the backend which provides the user with a reliable and secure experience.

1.3 Intended Audience and Document Review

Our document is broken down into various chapters for a better over-view. The Literature review section of this document describes briefly about Android and its technologies and basically the overall motivation behind the project and its uses.

The Overall Description section of this document gives an overview of the functionality of the product. It describes the informal requirements and is used to establish a context for the technical requirements specification in the next chapter.

The fourth chapter, Requirements Specification section, of this document is written, primarily for the developers and describes in technical terms the details of the functionality of the product. The final chapter of the document mentions the limitations and conclusion of the project along with its future aspects.

All sections of the document describe the same application in its entirety, but are intended for different audiences. The audience can be a user, an evaluator or a developer.

1.4 Glossary

Term	Definition
Firebase	Firebase is a cloud services provider and backend as a service company.
Database	Collection of all information monitored by the system.
User	The end users who uses the application.
Software Requirements Specification	A document that completely describes all of the functions of a proposed system and the constraints under which it must operate. For example, this document.
Developer	A person who develops standalone software and gets involved in all the phases of the development.

Fig1.4 Glossary

2   Literature Review

As android is an open source platform, it supports third party applications development that technically could have full access to data and hardware. Using this and Google's official website for android development, we were able to gain knowledge about the various fields of android development.

2.1 Literature Review

Android is leading the market share in mobile applications downloads since 2011. To secure users' information and resources, the platform uses a permission-based model. We have learned our concepts using the freely available courses on Udemy and from the official android application development help material.

2.2 Motivation

We chose the Android platform because it is one of the fastest growing mobile operating systems on the market and is an open source development. According to IDC, Android absolutely dominated the number of smartphones shipped worldwide in the first three months of 2015, with 78% market share. Taking this project allowed us to gain an understanding of how some of the built in frameworks can be utilised to develop application and help in securing users data. Further, we are provided with Android Studio. Android Studio is an excellent IDE, based on the equally excellent IntelliJ IDE. It is blazingly fast and efficient, and you can setup a new Android project for different types of Android apps within seconds. Also, apps deployed to the Google Play store are available for download by users within a few hours, compared to a few weeks for Apple's App Store. Furthermore, this project demonstrates how mobile applications can contribute to secure the data of the user with ease.

3 Overall Description

This section comprises of the application's different aspects including its perspective, functionalities, environment and design constraints.

3.1 Product Perspective

The application works on the principle of Client server model. Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A client need not share any of its resources with clients, but requests a server's content or service function. Clients therefore initiate communication sessions with the servers which await incoming requests. In our case the user can access different type of security related features through the fragments in our Home activity. The user (client) registration will lead to an entry in the firebase's database (server).

3.2 Product Functionality

The product makes use of many open source applications under the GNU General Public License. It is a mobile based system implementing the client-server model.
The following are the main features that are included in the Android based Application:

- Secure Login: Using Firebase as our backend database, the security for activities such as sign-up (register) or login has considerably increased. The passwords are stored in hashed form and are verified by Google's own hashing techniques.

- SMS Control: This feature of our application lets the user remotely control some basic functionality which would come in handy if the device was lost or stolen. It provides the user with a random generated password which user can use to access this feature. The user can either change their phone's profile from silent to ringer, make their devices ring an alarm, or even get the last known location of their devices.

- Application Permission Management: This application lets users check the permissions of the installed applications in their devices. Users are provided with the option to uninstall the application, if he/she feels that it is accessing any unnecessary permissions which seems fishy.

- Signal Flare: This feature is based upon GPS tracking. This feature intelligently check the user's device for low battery. If it is so, the app sends the device's location to registered email or number of the user.

- Pattern-Unlocking: This feature uses the in-built pattern/password unlocking system to detect if the user using the device is genuine or not. After a specified number of incorrect password

attempts, the application shall take the photo of the user using the front camera and will send it to the registered email/phone number.

3.3 Operating Environment

The application is designed to work only on the Android Operation System and its supporting devices. The Android OS on the device should be a minimum of Ice Cream Sandwich (4.0.2) API 15 and a maximum of Android Marshmallow (6.0.1) API 23. Requirements for the minimum amount of RAM for device running Android 6.0 range from 1 GB of RAM for normal density screens, whereas the recommendation for Android 4.4 is to be at least 512MB of RAM.

Android devices incorporate many optional hardware components including GPS, orientation sensors, dedicated proximity sensors, the application will use all the mentioned sensors if permitted by the user. The app will rely on several functionalities built into Android's Application Programming Interface (API), so ensuring appropriate usage of API will be a major concern. Beyond that, the application is a self-contained unit and will not rely on any other Android-related software components.

3.4 Design and Implementation Constraints

The primary design constraint is the mobile platform. Since the application is designated for mobile handsets, limited screen size and resolution will be a major design consideration. Creating a user interface which is both effective and easily navigable will pose a difficult challenge. Other constraints such as limited memory and processing power are also worth considering. The app is meant to be quick and responsive, even when dealing with large groups, so each feature must be designed and implemented with efficiency in mind.

3.5 Assumptions and Dependencies

This provides some assumptions that we made while making our application as well as a set of libraries that we will be importing to make our application more useful for the user.

Assumptions

The few assumptions that we took while building our android application were that the user shall provide us with the required permissions and shall not deny any permission. Denial of any core permission shall lead the application useless. We also assumed that the user does not force close the application or clear it's RAM via a full clean RAM Management software, which will stop our background services and the application would not be able to monitor anything.

Time Dependencies

The features of our Application are basically divided into two groups: Core Features and additional features. Core Features are crucial to the basic functionality of the application. These features must all be implemented in order for the application to be useful. These include the libraries that comes preinstalled with the Android Studio IDE, such as, the Google Repositories, Google SDK, etc. Additional libraries that we have imported are those of Google Play Services and Firebase.

Hardware Dependencies

Some of the application's features depend upon some hardware components present in Android handsets. For instance, the GPS will be used to track the current location of the user. The Pattern lock functionality is entirely dependent upon the ability to access the front camera. The android device must also meet the minimum specified hardware requirements so that the application can run smoothly on it.
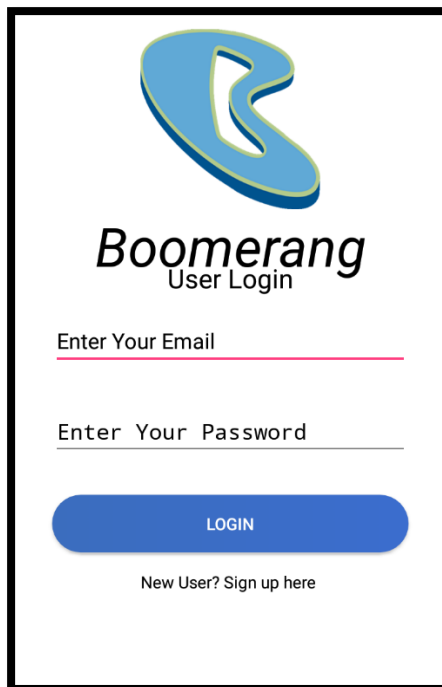
4   Specific Requirements

This defines the minimum specification that the android device must have in order to have a smooth functionality and great user experience.
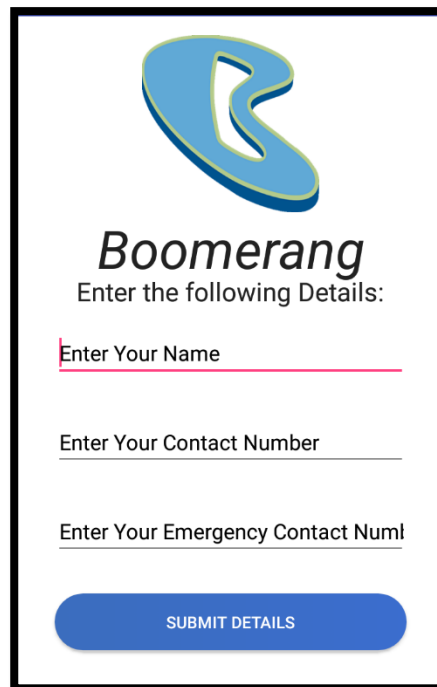
4.1 External Interface Requirements

Various interfaces of the application and their design have been described in the User Interface Section below.

4.1.1 User Interface

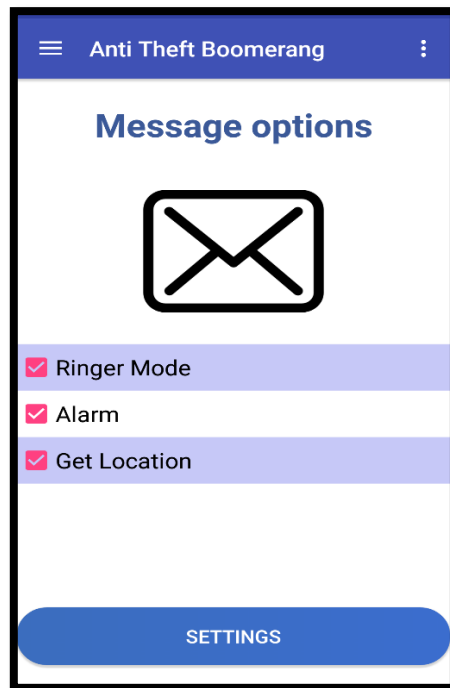**Fig 4.1.1.a** User Registration   **Fig 4.1.1.b Profile Activity**
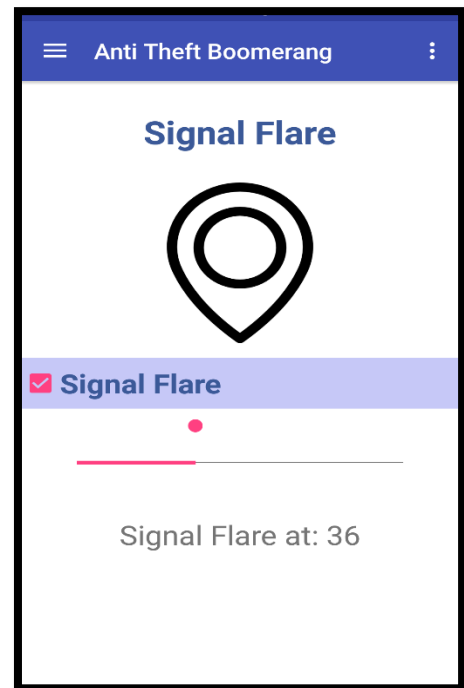
Fig 4.1.1.c Profile Details
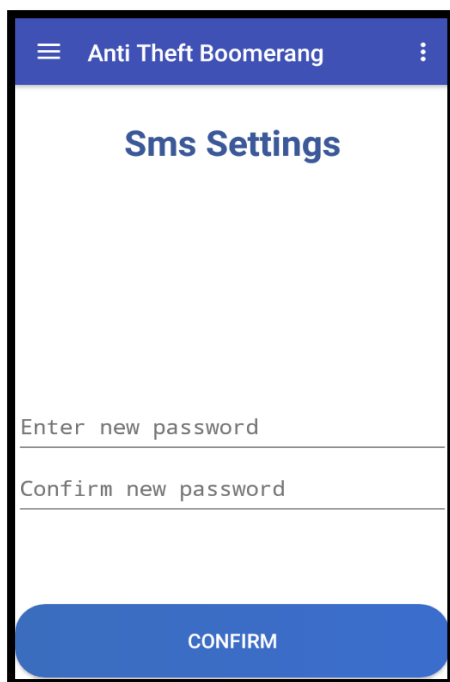

Fig 4.1.1.d Homepage

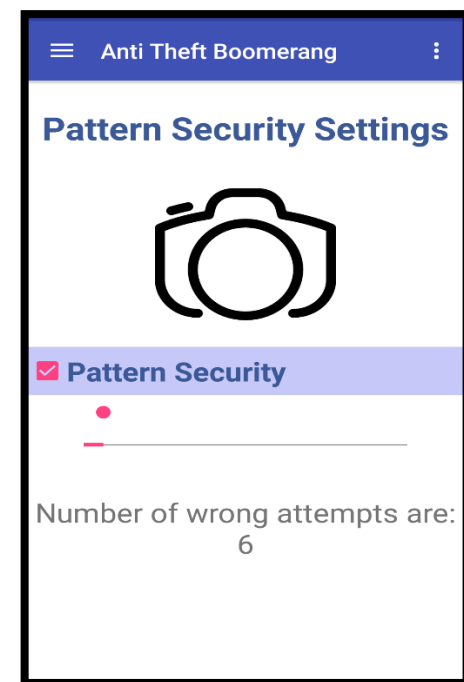**Fig 4.1.1.e** Generating
Messaging Key
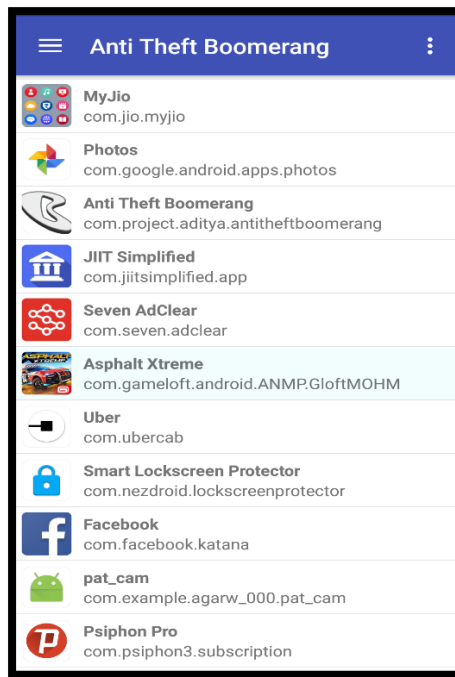

Fig 4.1.1.f Pattern Security
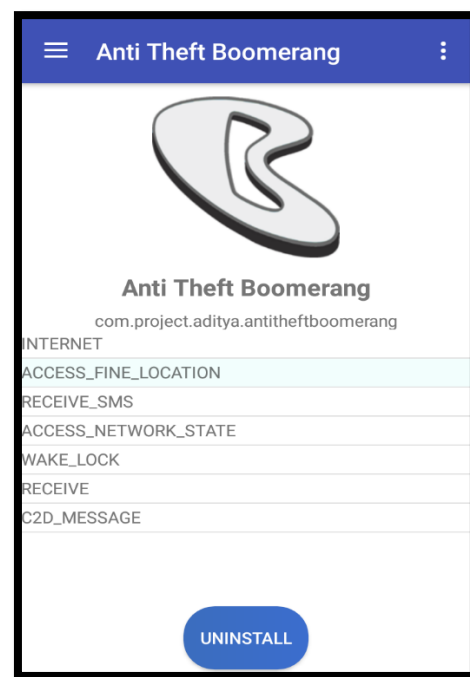
Fig 4.1.1.f Installed Apps   **Fig 4.1.1.e** App Permissions

4.1.2 Hardware Interface

The Application is intended as a mobile application for the Android Devices and hence is solely supported on Android-powered devices. Updates and data exchanged between Android devices are transmitted to and handled by the host server. It basically replicates a client server model, where a user requests certain data from the user and the server replies with the most suitable results.

We are basically using the cloud services provided by the Google Firebase. Firebase lets you store data on their database and can be retrievable easily in list or recycler view. Information will be sent using TCP/IP and the HTTP protocol using the port number 80.

The Android platform provides abstractions for all network communications interfaces and thus thee hardware as well.

9

4.1.3 Software Interface

The app is to be developed under the Android operating systems using the Java JDK, the Android SDK tools.

4.1.4 Communication Interface

The application will have a cloud server that is web-based and created using the JAVA language. The server exists to retrieve information from the database. The product also calls for a database system that stores user's information and preferences. The HTTP server will use a push protocol to push notifications of updates onto the Android phones. Furthermore, whenever a user opens the app from their phone, a pull protocol will be used to retrieve and sync the latest updates from the firebase server.

4.2 Functional Requirements

Internet: This app requires internet to access the features of firebase such as Login and Signup. It also takes the required permission from the user**.**

SMS: This application further uses the messaging capability of the device. It uses a Broadcast Listener to read user's messages and take action according to its content. If the user has messaged the correct keywords along with the verified password, then he/she will be able to access the ringer functionality of the application. This functionality is used to change the user's profile from silent to ringer.

Location: The location permission of the device is needed for the core functionalities of the application. Without the device's location, the Get Location feature of the application would not be accurate.

Device Administration: The device administration is required to read the pattern of the user to determine if the user has entered a wrong pattern/password.

Camera: A front camera is required to take the photos of the user that has not been able to bypass the lock screen and has entered the password/pattern wrong several times.

4.3 Non-Functional Requirements

Scalability

With regards to the intended number of users and the projected load scenarios, the intentions are for the system to able to serve multiple queries /day (in large during peak traffic hours) in terms of multiple users accessing at the same time. Firebase Database is very efficient in handling such

queries. Firebase uses JSON as its language, which is much faster than PHP. This helps it to parse the queries faster and hence provide the user with the correct data at a reliable rate.

Security and Privacy

The Firebase domain has a privacy sensitive nature, specifically with regards to the authentication of the users. The Firebase cloud services have their own encryption features which helps user by providing more privacy with their passwords as they are stored in hashed form and not visible at the server.

4.4 Behavior Requirements

UML behavioral diagrams visualize, specify, construct, and document the dynamic aspects of a system. Some of the behavior diagram of our projects are shown below.
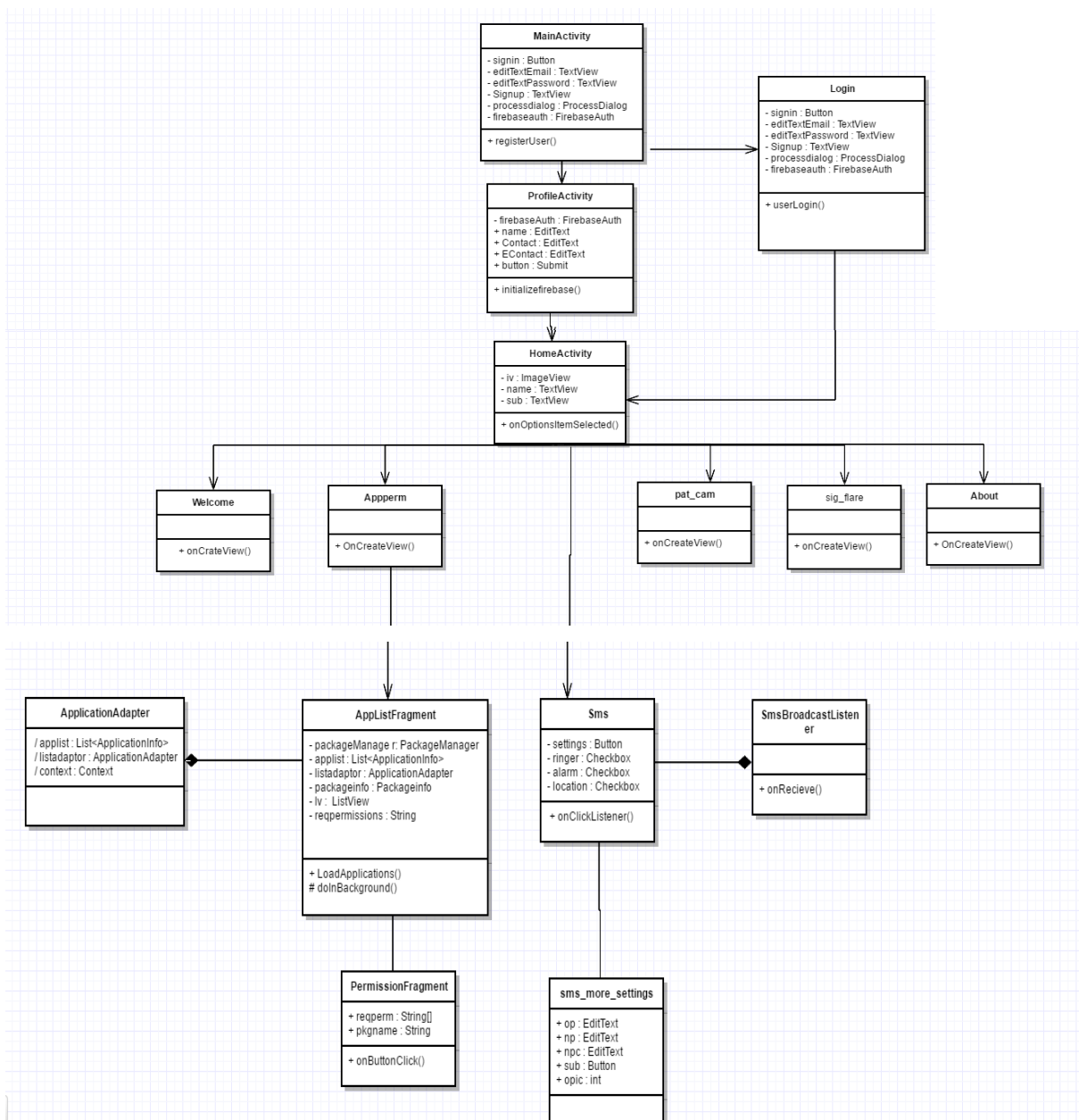
4.4.1 Class Diagram

Fig 4.4.1 Class Diagram

4.4.2 Block Diagram
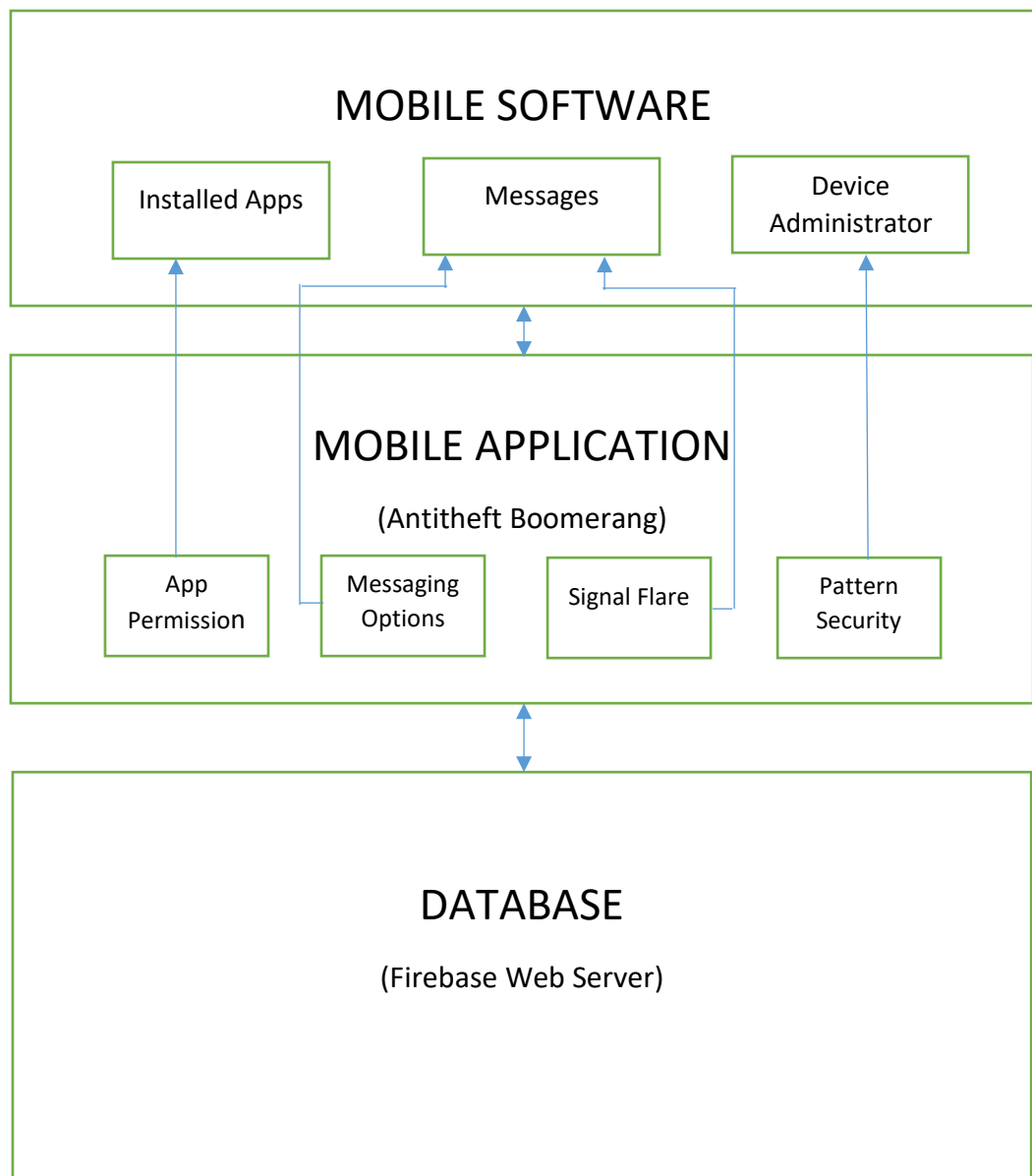

Fig 4.4.2 Block Diagram
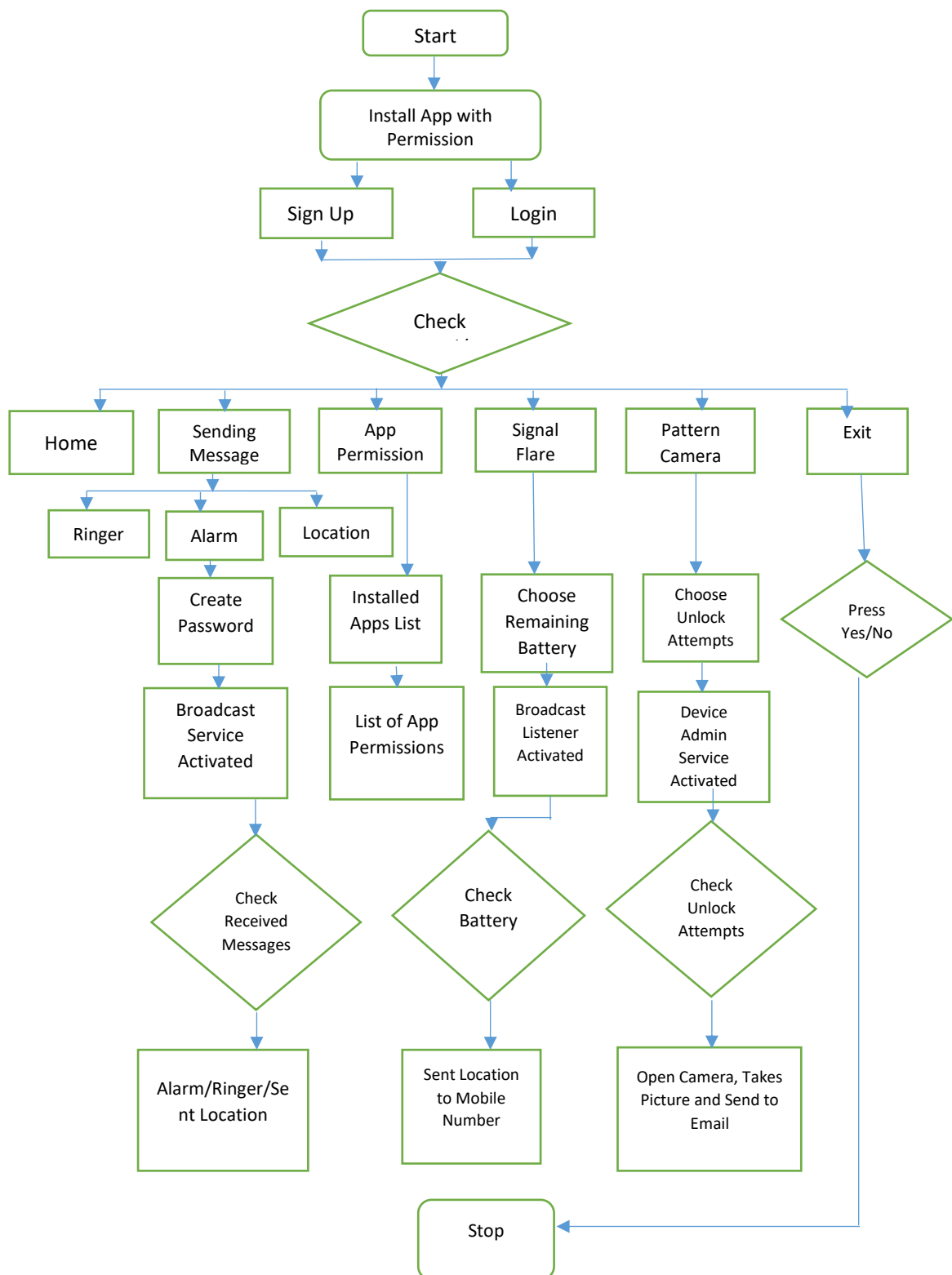
4.4.3 Activity Diagram

Fig 4.4.2 Activity Diagram

5   Testing Report

Testing is the process carried out on software to detect the differences between its behaviour and the desired behaviour as stipulated by the requirements specifications.

5.1 Testing

Testing is advantageous in several ways. Firstly, the defects found help in the process of making the software reliable. Secondly, even if the defects found are not corrected, testing gives an idea as to how reliable the software is. Thirdly, over time, the record of defects found reveals the most common kinds of defects, which can be used for developing appropriate preventive measures such as training, proper design and reviewing.

5.2 Test Cases

Sr. No	Test Case Description	Expected Result	Actual Result	Remark
1	Correct Username and Password	Profile Activity should appear	Same as Expected	
2	Incorrect Username and Password	Toast Box appears indicating User registration failed	Same as Expected	
3	Email Textbox left blank	Error message appears displaying "This field cannot be blank"	Same as Expected	
4	Password Length less than 8 characters	Error message appears displaying "Password must have a minimum of 8 characters"	Same as Expected	
5	On tapping "Already Registered User" Text view	Redirects to Login Activity	Same as Expected	
6	On Clicking "Forgot Password" Text view	Redirects to Recover Password Activity	Same as Expected	
7	Submit Email in the Recovery Password Activity	Toast Box appears indicating Reset password email sent and redirects to Login Activity	Same as Expected	
8	Submitting Correct Username and Password in Login Activity	Redirects to Home Page Activity	Same as Expected	
9	Selecting App Permissions in the Navigation Drawer	List containing all the installed apps of the device appears	Same as Expected	
10	On Selecting any application in the list appeared after clicking App Permissions Option	List containing all the permissions used by the application shown	Same as Expected	

11	Selecting Messaging Options in the Navigation Drawer	Fragment appears containing Ringer, alarm and Location feature	Same as Expected	
12	On Selecting any of the feature in the Messaging options Section	Asks user to set a temporary password for the SMS feature.	Same as Expected	
13	Selecting Pattern Options from the Navigation Drawer	Fragment appears displaying feature to select minimum number of patterns to activate the feature.	Same as Expected	
14	Selecting Signal Flare from the Navigation Drawer	Fragment appears displaying feature to select minimum percentage of battery to activate the feature.	Same as Expected	
15	On Selecting Logout from the Options Menu in the top right corner	Application logs user out and redirects to Login Activity	Same as Expected	
16	On Selecting Delete Account from the Options Menu in the top right corner	User has been asked to Confirm Delete Account	Same as Expected	

Fig 5.2 Test Cases

6 Conclusion and Future Scope

As nothing is perfect, here are some of the limitations of our application that we would like to overcome in the near future.

6.1 Limitation and Conclusion

When the application is forced closed by the user by going into its settings, user manually stops all the broadcast listeners or services that an application is linked to. Hence our security application will fail to serve its purpose in that case. Another limitation is that when the user is in a zone with low connectivity, i.e., low signal strength of the operator that the user is using. In that case, the messaging feature shall suffer. Also if any user intentionally removes the battery of the device, it is switched off and there is no way to prevent that. Although, in today's scenario, most of the devices are of unibody design, i.e., they come with non-removable batteries.

To conclude, Boomerang is an application that will try its best to bring back your lost/stolen phone. It will be the only anti-theft security application that the user will ever need!

6.2 Future Enhancements

This application is an anti-theft and security application which would have to tackle all the upcoming security threats. Some of future features include the following.

Power button override: A very important aspect of an anti-theft mobile system is not to let any unauthenticated user to switch-off the device. Therefore the application will provide the feature to override the power button before the security lock, so that the device cannot be turned off.

Wipe data: With this feature the user can wipe its internal memory, to avoid any data-theft from his/her device.

Video Recording: This feature can be used to record videos from a phone and send it via email to track the location of the phone.

Further, the user shall be notified of any hot swapping of SIM in his device. The new number of the SIM card shall be sent to the user's registered mobile number and registered email id. Addition of a child lock mode, to increase security of the device. On every boot of the android device the user shall be notified of the location of the device. Using IMEI number to enhance the functionality of anti-theft tracking using government permission.

References:

1. K. Subha, Dr. S. Sujatha, "Anti-Theft Tracking System for Smart Phones", International Journal of Advanced Research in Computer Science and Software Engineering. ISSN: 2277 128X

2. Shweta Dhanu1, Afsana Shaikh2, Shweta Barshe3, "Anti-Theft Application for Android Based Devices", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016. ISSN (Online) 2278-1021 ISSN (Print) 2319 5940

3. [KMP77] D.E. Knuth, J.H. Morris and V.R. Pratt" Fast Pattern Matching in Strings" in SIAM J. Comput.6, 2 (1977) 323–350.

4. K.S. Kuppusamy1, Senthilraja.R2, G. Aghila3, MOBILE LOCATION ESTIMATION AND TRACKING FOR GSM SYSTEMS Vol. 4, Issue 5, June 2015

5. J.ManiBharathi, S.Hemalatha, V.Aishwarya, C.Meenapriya, L.Hepzibha Shekinah Grace, "Advancement in Mobile Communication using Android", International Journal of Computer Applications (0975 – 8887), Volume 1 – No. 7, 2010.

6. Chao-Lin Chen; Kai-Ten Feng; "Hybrid Location Estimation and Tracking System for Mobile Devices"