**EVENT-TRIGGERED ANTI-THEFT MOBILE SECURITY APPLICATION**

**PROJECT SUBMITTED BY**

OTIENO BEN ODOYO

AND

OTIENO CANTON WEKE

A project submitted to the school of informatics and innovative system in partial fulfillment of the requirements for the award for a BSc in Computer Security and Forensics at.

Jaramogi Oginga Odinga University of science and technology

November 25th 2021

## **DECLARATION**

I Otieno Ben and Otieno Canton do hereby declare that this Project progress Report is original and has not been published or submitted for any other degree award to any other University before.

Signed…OTIENO BEN ODOYO………………………………………………. Date… October 20, 2021………………………….

Otieno Ben Odoyo

I132/1585/2017

Signed…OTIENO CANTON WEKE…...

Date…………October 20, 2021………………………………….

Otieno Canton Weke

I132/0418/2017

**Supervisor**

This project has been submitted for examination with the approval of the following supervisor.

Signed…………………………………… Date…………………………….

Project supervisor

Dr. Richard Omollo.

# **DEDICATION**

This project is dedicated to our families who have seen us through our academic journey tirelessly, offering us both financial and moral support. Especially to our parents, who have been our greatest inspiration since we were young up to this far. To all our lecturers at Jaramogi University who have imparted to us both technical and soft skills that will see us carry out this project successfully. Also to our fellow students, all our classmates, and every single person who has a passion for solving problems and making the world a better place using technology.

## **ACKNOWLEDGMENTS**

We would like to acknowledge the contributions of several people to this research; without whose help it would have not been possible for us to carry out this research. First and foremost, we would like to thank our heavenly father who has kept us in good health all throughout the course of this project and reminded us of the principle of living a day at a time. Would also like to thank Dr Richard Omollo our project supervisor for guidance and support he gave during the project development period and Dr. Solomon Ogara at the School of Informatics and Innovative System at Jaramogi Oginga Odinga University of Science and Technology for the leadership he continues to render to the center. Finally yet importantly, we would like to thank our beautiful parents and beautiful Grandmothers Mrs. Elsa Obaria and Helen Dula Olielo for the financial and spiritual support they continue to render, without them not all, this would be possible.

Again, we would also like to thank Jaramogi University for having us all these four years and giving us the chance and good learning environment to study at the university. Most importantly, the lecturers having imparted us with a massive amount of knowledge both academic and social. Much thanks especially to our proposal supervisor Dr. Newton for guiding us through this project proposal, without him this project would be a failure. May God grant him long life and health.

Lastly, we would like to thank all our friends and relatives for their sincere feedback during the execution of this project; their feedback has been instrumental in helping us evaluate critically every step during this project proposal.

# **ABSTRACT**

The project course at the Department of Computing and Information Technology at Jaramogi University done during the final year is an essential unit for the student of the department. This course is designed to test both the practical skills the student has gathered throughout his life at the university. The course tests the student skills in requirement collection, analyzing them, designing a prototype of the system, and implementing the system. During this project, the student gets the chance to exhibit his skills and gets to learn additional skills such as project management and teamwork.

This project is about mobile-based application aiming at eradicating the constant and rampant theft of phones going through the school hostels. The system employs features such as GPS tracking, sensor mechanism, and phone application group to solve this problem. The system is developed to be a free distributed application that will help subside phone theft among students in hostels and even around the school.

Table of Content

[**DECLARATION** i](#_heading=h.gjdgxs)

[**DEDICATION** ii](#_heading=h.30j0zll)

[**ACKNOWLEDGMENTS** iii](#_heading=h.1fob9te)

[**ABSTRACT** iv](#_heading=h.3znysh7)

[**LIST OF FIGURES** viii](#_heading=h.2et92p0)

[**ACRONYM** x](#_heading=h.tyjcwt)

[**CHAPTER 1** 1](#_heading=h.1t3h5sf)

[**INTRODUCTION** 1](#_heading=h.4d34og8)

[**1.1**](#_heading=h.2s8eyo1) **BACKGROUND OF THE STUDY** 1

[**1.2**](#_heading=h.3rdcrjn) **PROBLEM STATEMENT** 2

[**1.3**](#_heading=h.26in1rg) **OBJECTIVES** 2

[**1.4 SCOPE AND LIMITATION OF THE PROJECT** 3](#_heading=h.35nkun2)

[**1.4.1 SCOPE** 3](#_heading=h.1ksv4uv)

[**1.4.2 LIMITATIONS** 3](#_heading=h.44sinio)

[**1.5 PROJECT JUSTIFICATION** 3](#_heading=h.2jxsxqh)

[**CHAPTER 2** 5](#_heading=h.3j2qqm3)

[**LITERATURE REVIEW AND CONCEPTUAL/THEORETICAL FRAMEWORK** 5](#_heading=h.1y810tw)

[**2.1 LITERATURE OVERVIEW** 5](#_heading=h.4i7ojhp)

[**2.2 CASE STUDY 1. SMARTPHONE TRACKING APPLICATION USING SHORT MESSAGE SERVICE** 5](#_heading=h.2xcytpi)

[**2.3 CASE STUDY 2. FINDING LOST ANDROID DEVICES USING MMS TECHNOLOGY** 6](#_heading=h.1ci93xb)

[**2.4 CASE STUDY 3. MOBILE THEFT TRACKING APPLICATION USING MMS AND SMS TECHNOLOGY.** 7](#_heading=h.3whwml4)

[**2.5 CONCLUSION** 8](#_heading=h.2bn6wsx)

[**CHAPTER 3** 9](#_heading=h.3as4poj)

[**METHODOLOGY** 9](#_heading=h.1pxezwc)

[**3.1 DESIGN METHODOLOGY** 9](#_heading=h.49x2ik5)

[**3.2 STAGES OF DEVELOPMENT** 9](#_heading=h.3o7alnk)

[3.2.1 Feasibility Study - Stage 0**.** 9](#_heading=h.23ckvvd)

[3.2.2 Requirement Analysis - Stage 1&2**.** 9](#_heading=h.ihv636)

[3.2.3 Requirements Specification - Stage 3. 9](#_heading=h.32hioqz)

[3.2.4 Logical System Specification – Stage 4&5. 9](#_heading=h.1hmsyys)

[3.2.5 Physical Design – Stage 6. 10](#_heading=h.2grqrue)

[***Reasons for choosing SSADM*** 10](#_heading=h.3fwokq0)

[**3.3 COMPARISON OF SSADM WITH OTHER METHODOLOGIES** 11](#_heading=h.1v1yuxt)

[**CHAPTER 4** 13](#_heading=h.2u6wntf)

[**SYSTEM ANALYSIS AND REQUIREMENT DEFINITION** 13](#_heading=h.19c6y18)

[**4.1 INTRODUCTION** 13](#_heading=h.3tbugp1)

[**4.2 CURRENT STRUCTURE OF THE MOBILE THEFT APPLICATION** 13](#_heading=h.28h4qwu)

[**4.2.1 USER SIGN UP** 13](#_heading=h.nmf14n)

[**4.2.1 USER LOGIN** 14](#_heading=h.46r0co2)

[**4.2.2 TRACK PHONE AND UPDATE OWNER** 15](#_heading=h.2lwamvv)

[**4.2.1 USER PROFILE** 15](#_heading=h.111kx3o)

[**4.3 REQUIREMENT ELICITATION METHODS** 15](#_heading=h.3l18frh)

[**4.3.1 INTERVIEWS** 15](#_heading=h.206ipza)

[**4.3.2 OBSERVATIONS** 16](#_heading=h.4k668n3)

[**4.4 PROPOSED SYSTEM** 16](#_heading=h.2zbgiuw)

[**4.5 USER REQUIREMENTS** 16](#_heading=h.1egqt2p)

[**4.6 FUNCTIONAL REQUIREMENTS** 17](#_heading=h.3ygebqi)

[**4.7 NON-FUNCTIONAL REQUIREMENTS** 17](#_heading=h.2dlolyb)

[**4.8 FEASIBILITY STUDY** 17](#_heading=h.sqyw64)

[**4.8.1 Economic Feasibility** 17](#_heading=h.3cqmetx)

[**4.8.2 Technical Feasibility** 18](#_heading=h.1rvwp1q)

[**Tools for Design, Development, and Testing** 18](#_heading=h.4bvk7pj)

[**4.8.3 Design and analysis tools** 18](#_heading=h.2r0uhxc)

[**4.8.4 Development and testing tool** 19](#_heading=h.1664s55)

[**4.8.5 Schedule Feasibility** 19](#_heading=h.3q5sasy)

[**CHAPTER 5** 20](#_heading=h.kgcv8k)

[**SYSTEM DESIGN** 20](#_heading=h.34g0dwd)

[**5.1 Introduction** 20](#_heading=h.1jlao46)

[**5.2. Architecture Design** 20](#_heading=h.43ky6rz)

[**5.3 System Design** 21](#_heading=h.3hv69ve)

[**5.3.1 Use case diagram** 21](#_heading=h.2w5ecyt)

[**5.3.2 Dataflow diagram** 23](#_heading=h.2afmg28)

[**5.4 Database design** 25](#_heading=h.1opuj5n)

[**5.4.1 Entities** 26](#_heading=h.48pi1tg)

[**5.4.2 Conceptual database design** 26](#_heading=h.2nusc19)

[**5.4.3 Physical design tables** 27](#_heading=h.1302m92)

[**5.5 Activities diagram** 29](#_heading=h.40ew0vw)

[**CHAPTER 6** 32](#_heading=h.3ep43zb)

[**SYSTEM IMPLEMENTATION** 32](#_heading=h.1tuee74)

[**6.1 Introduction** 32](#_heading=h.4du1wux)

[**6.2 Tools for Development** 32](#_heading=h.2szc72q)

[**6.2.1 Software Tools for Development** 32](#_heading=h.184mhaj)

[**6.2.2 Hardware Tools for Development** 34](#_heading=h.279ka65)

[**6.3 Tools for Testing** 34](#_heading=h.meukdy)

[**6.3.1 Software Tools for Testing** 34](#_heading=h.36ei31r)

[**6.3.2**](#_heading=h.1ljsd9k) **Hardware Tools for Testing** 34

[**CHAPTER 7** 40](#_heading=h.1qoc8b1)

[**TESTING PROCESS** 40](#_heading=h.4anzqyu)

[**7.1 Unit Testing** 40](#_heading=h.2pta16n)

[**7.2 Functional Testing** 40](#_heading=h.14ykbeg)

[**6.3 Performance Testing** 41](#_heading=h.3oy7u29)

[**7.4 Stress Testing** 41](#_heading=h.j8sehv)

[**7.5 Proposed Changeover Techniques** 44](#_heading=h.2hio093)

[**7.6 Ethical Considerations** 44](#_heading=h.wnyagw)

[**7.7 Mobile Security Risk assessment and risk mitigation** 44](#_heading=h.3gnlt4p)

[**7.7.1 Risk** 44](#_heading=h.1vsw3ci)

[**CHAPTER 8** 46](#_heading=h.2uxtw84)

[**LIMITATIONS, RECOMMENDATIONS, AND CONCLUSIONS** 46](#_heading=h.1a346fx)

[8.1 **Limitations** 46](#_heading=h.3u2rp3q)

[**8.2 Recommendations** 46](#_heading=h.2981zbj)

[**8.3 Conclusion** 46](#_heading=h.odc9jc)

[**REFERENCES** 47](#_heading=h.38czs75)

[A Simple Flutter Android App that displays Sensor Data. (2019, March 3). Retrieved from 47](#_heading=h.1nia2ey)

[Thiran, T. (2018, Aug 4). How to send a screenshot attachment in Mail using Flutter. 48](#_heading=h.47hxl2r)

[**APPENDICES** 51](#_heading=h.2mn7vak)

[**APPENDIX A** 51](#_heading=h.11si5id)

[SYSTEM CODES 51](#_heading=h.3ls5o66)

[User authentication 51](#_heading=h.20xfydz)

[Database service sample codes 53](#_heading=h.4kx3h1s)

[Location services codes 54](#_heading=h.302dr9l)

[Security codes 55](#_heading=h.1f7o1he)

[APPENDIX B 57](#_heading=h.3z7bk57)

[**System User’s Manual** 57](#_heading=h.2eclud0)

[**1 General Information** 57](#_heading=h.thw4kt)

[**System** **Overview** 57](#_heading=h.3dhjn8m)

[**1.1 System Configuration** 57](#_heading=h.1smtxgf)

[**1.2 User Access Levels** 57](#_heading=h.4cmhg48)

[**Contingencies** 57](#_heading=h.2rrrqc1)

[**2 Getting started** 58](#_heading=h.16x20ju)

[**TIME SCHEDULE AND PROJECT COST** 62](#_heading=h.3qwpj7n)

[Schedule 62](#_heading=h.261ztfg)

## **LIST OF FIGURES**

[Figure 3. 1 Development Stages 10](#_heading=h.vx1227)

[Figure 4. 1 Current system use case Diagram 13](#_heading=h.37m2jsg)

[Figure 4. 2 Current System DFD Diagram 14](#_heading=h.1mrcu09)

[Figure 5. 1 Architecture Design 19](#_heading=h.1kc7wiv)

[Figure 5. 2 Use case diagram for user 20](#_heading=h.1baon6m)

[Figure 5. 3 use case diagram for both admin and user 21](#_heading=h.3vac5uf)

[Figure 5. 4 Context diagram for the system 22](#_heading=h.pkwqa1)

[Figure 5. 5 Full DFD diagram for entire system 23](#_heading=h.39kk8xu)

[Figure 5. 6 Entity relation diagram. 27](#_heading=h.1gf8i83)

[Figure 5. 7 the system design flowchart is as follows 28](#_heading=h.44bvf6o)

[Figure 5. 8 the profile management flowchart is as follows 29](#_heading=h.1x0gk37)

[Figure 5. 9 Proposed System Securing Phone Flowchart 30](#_heading=h.4h042r0)

[Figure 6. 1 Signup page 34](#_heading=h.2koq656)

[Figure 6. 2 Login interface 34](#_heading=h.zu0gcz)

[Figure 6. 3 The navigation bar of the system 35](#_heading=h.3jtnz0s)

[Figure 6. 4 Main design user interface 35](#_heading=h.1yyy98l)

[Figure 6. 5 setting profile window 36](#_heading=h.4iylrwe)

[Figure 6. 6 joining group and viewing the location of your member’s page 36](#_heading=h.2y3w247)

[Figure 6. 7 Firebase database 37](#_heading=h.1d96cc0)

[Figure 6. 8 Authentication, showing users that have sign in the application 38](#_heading=h.rjefff)

[Figure 6. 9 Cloud\_firestore 38](#_heading=h.3bj1y38)

[Figure 7. 1 Showing location ben 40](#_heading=h.338fx5o)

[Figure 7. 2 Tracking bens position 41](#_heading=h.1idq7dh)

[Figure 7. 3 Showing how the system run in background 42](#_heading=h.42ddq1a)

**List of Tables**

[Table 1 Members 27](#_heading=h.3mzq4wv)

[Table 2 Image 27](#_heading=h.2250f4o)

[Table 3 Groups 27](#_heading=h.haapch)

[Table 4 Group occurrence (location) 27](#_heading=h.319y80a)

## **ACRONYM**

GPS- global position system

SIM- subscriber identity module

MMS-multimedia message services

SMS- short message services

IMEI-international mobile equipment identity

GSM-global system for mobile communication

SSADM-structured system analysis and design method

JSON- JavaScript on Notation

PHP- hypertext preprocessor

MYSQL-structured query language

UI-user interface

IDE-integrated development environment

API- application programming interface

ERD-Entity Relation Diagra

# **CHAPTER 1**

# **INTRODUCTION**

The spread of computers and smart phones to ordinary people has made information security to become increasingly important. User authentication is one of the most important technologies for computer security. Although passwords are used in phones and personal computers in securing them, they are known to sometimes have problems and cannot be able to safeguard these devices from being stolen as mobile devices faces many challenges. (Martinez, 2012).

The project will try to look into event-triggered Anti-theft mobile security applications and how it will help in minimizing theft of mobile devices within the university hostels among the students. The introduction part has been divided into various parts as follows, the background of the study, problem statement, object, and then research scope.

## **BACKGROUND OF THE STUDY**

The introduction of smartphones in universities brings a tremendous change in helping streamline the education process between students and Lecturers (Baron, 2011). These mobile phones have many features, and applications that are very useful to the students e.g. they are majorly used to pass communication about lectures and sharing of study materials. Unfortunately, over the years, the students have experienced a major problem of theft, as these mobile phones have long been prone to theft, especially among students living in the hostels. This act of theft usually occurs at night without the owner's consent and even more importantly, the owners lack a means of tracking their phones.

The event-triggered anti-theft mobile security application is a mobile application that solves this theft problem by combining several features to come up with an elaborate solution. These features include the mobile camera, the alarm system, and the use of a satellite-based navigation system by google (Lu et al., 2010). All these features are combined to enable the owner to be alerted in case of theft, and track his/her phone in case of a successful theft or incase of the phone cannot access photo or take photo the user will use group join during the time of registration to track his or her phone.

## **PROBLEM STATEMENT**

According to (Kibona & Mgaya, 2015). The constant need for the use of mobile phones especially among students in the universities has made these phones vulnerable to theft. Many of the students, especially those that live within school, experience loss of phone from time to time, which majorly occurs at night while the owners are sound asleep, though sometimes it does occur in the daytime. This theft case occurs mainly without the owner's consent since he/she is sleeping, and even when the phone is stolen the owner always lacks a way to locate his/her phone and identifying the culprit and locate the phone, thus in case of theft the owner finds it hard to access study materials, contact friends, family, and lecturers due to loss contacts, receive notifications and messages for lessons schedule and even fail to access money stored in the phone. An event-triggered anti-theft mobile security application will enable the phone's owner to identify the thief through an alarm clock, camera phone, and even be able to track the lost phone as such recovering the lost phone and important materials stored on the phone.

## **OBJECTIVES**

Our objective covered the main objective and specific objective.

**Main objective**

1. To develop an event triggered anti-theft mobile security application, capable of alerting the owner during a theft case, identify the culprit in case of theft, and easily track the lost mobile phone by initiating a tracking process through someone with the same application in his/her mobile phone.

**Other specific objectives**

1. Analyze related case studies and come up with a literature review that conceptualizes the project.
2. To test if the develop application will be able track a lost phone
3. To review the develop application if it can work with existing one.

## **1.4 SCOPE AND LIMITATION OF THE PROJECT**

### **1.4.1 SCOPE**

This project involves a mobile application that utilizes the phone sensor mechanism, camera, alarm, emails, groups joined by the user of the application, and tracking mechanism, by use of GPS (Global Positioning System). The application will alert the owner with an alarm in case of an ongoing theft case by utilizing the sensor mechanism and the alarm, if the phone’s camera is sensitive enough and well integrated, it might capture the culprit photo and sent it to the owner through an email system, and locate the phone in case of theft by utilizing the GPS (Global Positioning System).

### **1.4.2 LIMITATIONS**

* The project does not consider overall theft cases.
* The project does not investigate more sophisticated technological features that can make the application more efficient such as binding the application to the firmware hence making it a permanent mobile application.
* Culprit photo might not work sometimes, failing to identify the thief correctly
* The tracking functionality of the application requires the use of the internet.

## **1.5 PROJECT JUSTIFICATION**

The project involves the development of a mobile application to combat mobile theft cases (Arikpo & Osuobiem, (2020). Unlike nearly all the current mobile theft applications that require the thief to change the SIM card to alert the owner, with this application one can track his/her lost phone by simply using the phone of another person who has the same application. This application also provides a protection mechanism for the phone by alerting the owner in case of theft and can help know the thief by capturing the phone's IMEI and sending the information to the owner's email. One can use this IMEI number and track the location of the phone.

This project will help provide insight into mobile theft cases by mainly applying different data collection techniques such as interviews, questionnaires, and observation to collect relevant information from the victims. Data collected through this project has the potential to be used to raise awareness of security measures among students living in the universities. This data will help in providing information to use to create or improve prevention plans for mobile theft. In so doing students will have clear knowledge of how different implementations could potentially help prevent mobile theft cases. Furthermore, the project result of developing a technological solution will provide the students with ideas on how to apply technology in improving security.

# **CHAPTER 2**

# **LITERATURE REVIEW AND CONCEPTUAL/THEORETICAL FRAMEWORK**

## **2.1 LITERATURE OVERVIEW**

(Shedg, Dhatrak & Ugal, 2017) argue that a smartphone is a mobile phone, which offers advanced technologies with functionality similar to a personal computer. With the growing speed of technological advancement, smartphones have become an essential component of our daily performance. Faster networking systems, attractive and powerful applications, and technology literate users are making these smartphones very powerful these days. Smartphones have also become very instrumental in streamlining the learning process in higher institutions by facilitating research and the passing of information (Handoyono, 2020). However, due to this wonderful processing power of the phone, they also become vulnerable to theft, hence protecting a mobile phone from theft and tracking a lost mobile phone is an important factor to consider at this age. The goal of this literature review is to compare case studies that provide a solution to mobile theft and come up with a more elaborate solution.

## **2.2 CASE STUDY 1. SMARTPHONE TRACKING APPLICATION USING SHORT MESSAGE SERVICE**

(Zahira Jahan & Vinodhini, 2016) aim at providing a solution by majorly focusing on the manipulation of short message services that can be implemented by using two mechanisms. First, using the GPS (Global Positioning System) to identify the location of the stolen phone, send an email to the owner, and update the owner in case the phone's location is changed in 10 minutes. Secondly, it involves notifying the owner of the thief's mobile number by utilizing the SIM card serial number mechanism. This relies on automatic registration of the SIM card serial number during the installation of the application which is unique for every SIM card, and in case of phone theft and there be a change of the SIM, a mismatch of the SIM card serial number is detected, and the owner is notified about thief's mobile number via SMS messages sent on alternative mobile numbers configured with the application. In the application, one must insert an alternative phone number during the installation of the application to be notified of the stolen mobile **(S**rilekha1 & Dhanakoti, 2016).

According to (Kumar et al., 2015). One can locate his /her phone in case of theft by receiving an instant message from the phone upon change of the phone's SIM card. However, this implies also that if the thief does not change the sim card one will not be able to locate his/her phone, the thief can change the sim card in a far location from the user, and even after the user tracks the phone it might take a lot of time to reach the phone's location. Upon using the GPS, it relies on the change of location to alert the owner of the thief's location, this approach causes a delay in locating a stolen phone since without a change of location the owner will not be notified.

This case study does not provide a protection mechanism like sensors to help prevent phone theft beforehand. Also, an expert thief may change the version or format of the smartphone, then the installed apps will be deleted and can't send any SMS, also during the development of such application include one must have a smartphone, and a proficient developer is needed, and necessary applications are required for complete realization of such a project. (Zahira, Jahan & Vinodhini, 2016).

## **2.3 CASE STUDY 2. FINDING LOST ANDROID DEVICES USING MMS TECHNOLOGY**

(Dhalpe et al., 2016) developed an application that solved the problem of mobile theft by improving on the old simple messaging system that is by applying the use of multimedia messaging such as cameras and videos. The scheme proposed in this system is very dependent on the hardware of your smartphones like the camera (front-back) and support for multimedia messages. Once this software is installed in a device, it works in the background, stores the user's current SIM number in a variable database and keeps checking continuously for SIM card change, whenever SIM card gets changed from mobile, it will start working in the background and take snapshots and record a video in the background i.e. without taking user permission it will take snapshots, record video and then it will send an MMS and number of snapshots to an alternate mobile number, chat messenger and an email id, which was provided by the user during installation. This application majorly relies on MMS (multimedia messaging service) technology, where you can send video and snapshots to any other chat messengers on a mobile phone i.e., WhatsApp, unlike SMS that provides only text information. It gives information about the location of the thief by sending the current location using latitude and longitude coordinates to an alternate email address, which helps us to recognize the thief (Adam et al., 2019).

This application far surpasses one using SMS, since one Implements background features such as running in the background without the thief's consent and sends key information to the owner's email such as thief's pictures, videos, etc. two it provides accurate device information that is the specific longitude and latitudes. Three Easy to manipulate( **S**rilekha1& Dhanakoti 2016) According to this case study, one can locate his/her phone in case of theft by receiving an instant multimedia message from the phone upon change of the phone's SIM card. However this implies also that if the thief does not change the sim card one will not able to locate his/her phone, The thief can change the sim card in a far location from the user, and even after the user tracks the phone it might take a lot of time to reach the location of the phone, one must provide an email or messaging app info to receive messages in case of theft and does not provide a protection mechanism to protect the phone storage beforehand and also one must have a smartphone to implement this application (Fawaz & Shin, 2014).

## **2.4 CASE STUDY 3. MOBILE THEFT TRACKING APPLICATION USING MMS AND SMS TECHNOLOGY.**

(Shedge, Dhatrak & Ugale, 2017) state that one can find the smartphone with the help of the IMEI (International Mobile Equipment Identity) numbering system, which is a 15-digit unique code that is used to identify a phone by use of GSM (Global System for Mobile Communication) protocol. This application also uses the latest technology like SMS (Short Message Services), and MMS technology. Utilizing these features, one can send a thief's picture that will be captured using the front camera and the current location of the IMEI number. It gives the exact details about the thief and his/her last location. If the SIM is changed then the location will be sent to the email id or the alternative number of the user that is given by the user at the time of installation of this application.

This application uses a SIM card unique number for the identification of the authorized user. SIM card's unique number is nothing but the sequence of ten-digit numbers. Every SIM card has its unique number. When the phone is stolen the thief will replace the SIM card with its SIM card then so the new SIM card number will not match with the previous SIM card number, this will have sent an alert message to the alternative number that is registered at the time of installation of the application. With the help of this new number, we can easily find out the location of the smartphone, besides one can track the stolen phone using the IMEI number since every phone has a unique IMEI number. Tracking a phone using an IMEI number can be done using a GPS that can locate the phone IMEI number (Subha & Sujatha, 2016).

According to this application, one can get the current location of the thief by using an alternative phone number to receive an SMS from the stolen phone, and if the SIM card is changed one can get the picture of the thief. However, for all this functionality to occur one must be connected to the internet, his or her phone must support a global positioning system (Bao & LI, 2006).

This application also delays tracking time, as it is dependent on the thief replacing the SIM card that might take considerably a very long time. It does not guarantee permanency upon phone rooting or flashing of the phone and does consider alerting owners in case of theft without the owner's consent. (Adam et al., 2019)

## **2.5 CONCLUSION**

About the case studies above, mobile phone theft is prevalent, and more elaborate solutions that are elaborate are needed to eliminate this problem. These case studies majorly provide a solution by relying on detecting SIM card removal to send a message to the owner alerting him of the thief's location. However though this solution might seem awesome, it is dependent on the removal of the SIM card by the thief which may influence the time of tracking the phone in case it is stolen due to delay in changing the SIM card, influence the tracking distance if the culprit happens to remove the SIM card from a very far location and hence delaying the process of catching the thief, also this solutions particularly do not provide a protection mechanism to secure the phone beforehand, as such it is crucial to work on the improvement of this security applications by providing protection mechanisms and ways to locate a stolen mobile phone right away in case of a theft case with ease.

The event triggered anti-theft security mobile application improves this solution by, providing a phone protection mechanism through alerting the owner with an alarm in case of an ongoing theft case, providing a mechanism to immediately locate a phone in case of theft by using another phone with the application to locate the stolen phone

# 

# **CHAPTER 3**

# **METHODOLOGY**

## **3.1 DESIGN METHODOLOGY**

Structured systems analysis and design method (SSADM) was used to analyze and design the application. (Kendall, 1988) states that: SSADM methodology involves users during the first phases of development that is the most critical and intense stage in the development process. Other than this, it is similar to the waterfall model in the terms of development stages or processes. It breaks down development into stages, modules, steps, and tasks. The first model it develops is the data model. Techniques used are:

1. Logical data modeling - the process of identifying, modeling, and documenting data as a part of system requirements gathering. Data is then classified into entities and relationships.
2. Data Flow Modelling. – involves tracking the data flow in an information system. Analyzes the processes, data stores, external entities, and data movement.
3. Entity Behavior Modeling- involves identifying and documenting the events influencing each entity and the sequence in which these events happen.

## **3.2 STAGES OF DEVELOPMENT**

### 3.2.1 Feasibility Study - Stage 0**.**

It aims at establishing whether the direction and requirements of the project are feasible economically, technically, and operationally.

### 3.2.2 Requirement Analysis - Stage 1&2**.**

This stage involves investigating the current environment and identifying problems and areas that need improvements. The second state involves developing a range of options that meet the defined requirements and picking one that is most suitable to the requirement.

### 3.2.3 Requirements Specification - Stage 3.

This stage aims at determining the desired system data, functions, and events.

### 3.2.4 Logical System Specification – Stage 4&5.

These stages aim at assessing the technical system operations and the logical design.

### 3.2.5 Physical Design – Stage 6.

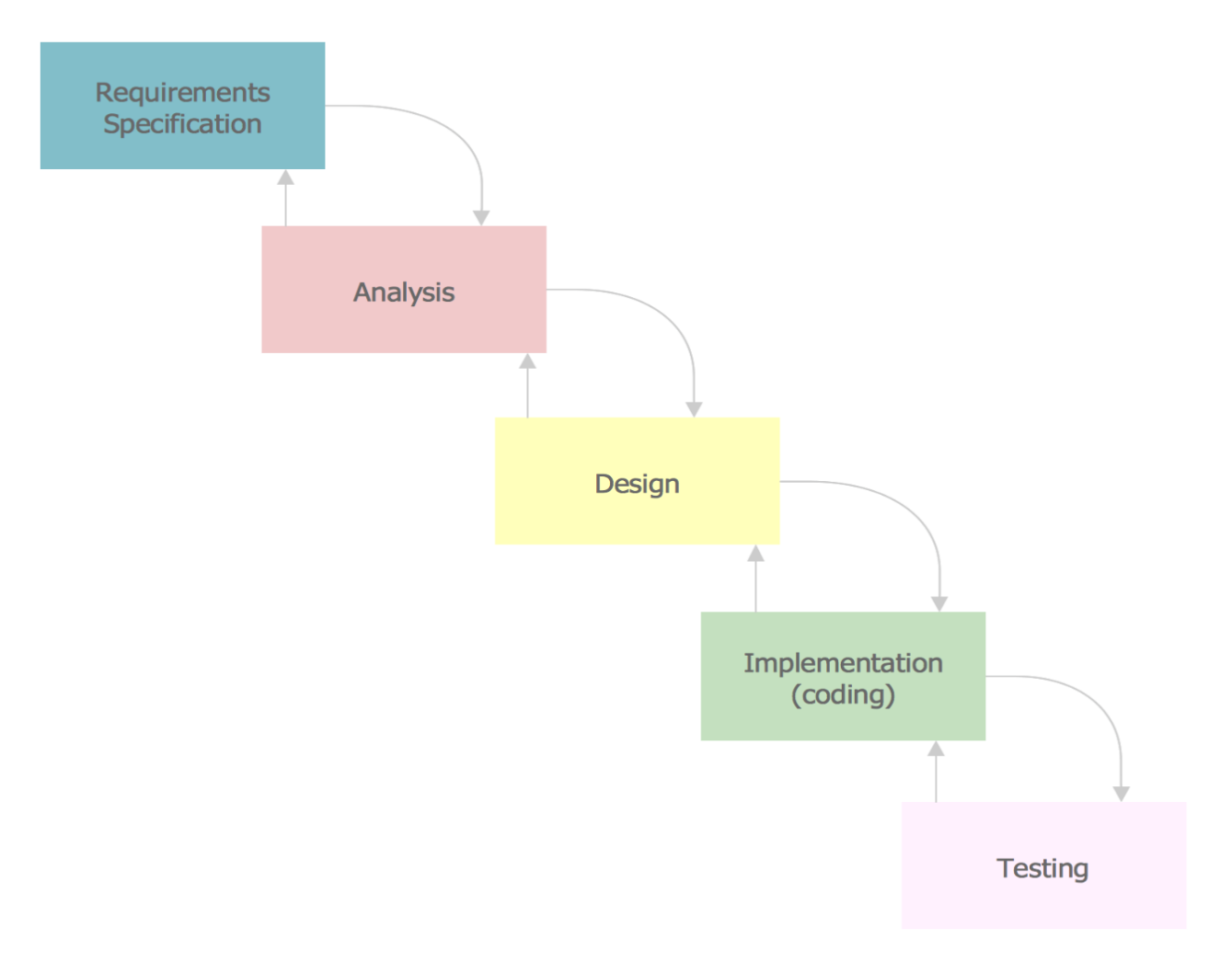
The physical environment in which the system will run is considered.

Figure 3. 1 Development Stages

### ***Reasons for choosing SSADM***

SSADM combines three methods, complementing each other within a systems development cycle that includes:

* Logical Data Modelling
* Data Flow Modelling
* Entity Event Modelling.

Its main benefits are over the other methodologies include:

* Improvement of quality
* Detailed documentation of the development stages
* Reusability for similar projects that follow.

Because of this rigorous analysis of the information system, this methodology reduces the chances of misunderstandings of the information in the project life cycle thus the reason for its selection for this project.

## **3.3 COMPARISON OF SSADM WITH OTHER METHODOLOGIES**

Other software development methodologies that have been studied and not considered for this project include:

1. **Waterfall Model**

This is a sequential design process in which progress is seen as flowing steadily downwards like a waterfall through the phases of:

* Conception
* Initiation
* Analysis
* Design
* Construction
* Testing
* Implementation and maintenance

All these phases are cascaded into each other in which progress is seen as flowing steadily like a waterfall.

*Advantages of Waterfall*

1. It is easy to manage as each stage is rigid and has specific deliverables and a review process.
2. Phases are processed and completed one at a time thus there is no overlapping.

*Disadvantages of waterfall*

1. Difficult to estimate the time and cost for each phase of development
2. Not a good model for complex and object-oriented projects.
3. Not suitable for projects whose requirements may change.

*SSADM vs Waterfall*

The two many times look similar but there is a slight difference that makes SSADM preferable to Waterfall. This is the fact that SSADM allows for the review of the previous stages/phases even after passing them unlike the traditional Waterfall that is rigid and once a phase is done it cannot be reviewed.

1. **Iterative Model**

This is a particular implementation of a software development life cycle that focuses on an initial simplified implementation that then progressively gains complexity and a broader feature set until the final set is complete. After the initial planning phase, a small handful of stages are repeated with each completion of the cycle incrementally improving and iterating on the software. The small phases include:

* Planning and requirements
* Analysis and design
* Implementation (coding)
* Testing
* Evaluation

*Advantages of iterative model*

1. Easy adaptability to the ever-changing needs of the system.
2. Each stage can be slimmed into smaller periods to fit the needs of the project or organization.

*Disadvantages of iterative model*

1. Increased pressure on user engagement.
2. Users experience the change in each iteration and thus there is a risk of feature/requirements creep.

# **CHAPTER 4**

# **SYSTEM ANALYSIS AND REQUIREMENT DEFINITION**

## **4.1 INTRODUCTION**

This chapter involves observing how the current system functions and interpreting the observations to outline its purposes and discover ways of accomplishing them most efficiently thus helps to ensure that all aspects of the system are captured in its design forming a blueprint of the development process.

## **4.2 CURRENT STRUCTURE OF THE MOBILE THEFT APPLICATION**

The following modules consist of the current structure of a mobile theft application:

* User Sign Up
* User Login
* Track Phone and Update Owner
* User Profile
* Alert user during theft case

## **4.2.1 USER SIGN UP**

If the user is new, he/she needs to sign up to be able to login in to access the tracking services provided by the application.

**Use case diagram for the current mobile application**

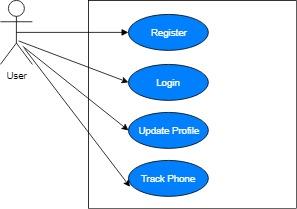


Figure 4. 1 Current system use case Diagram

**Data flow for the current mobile application**

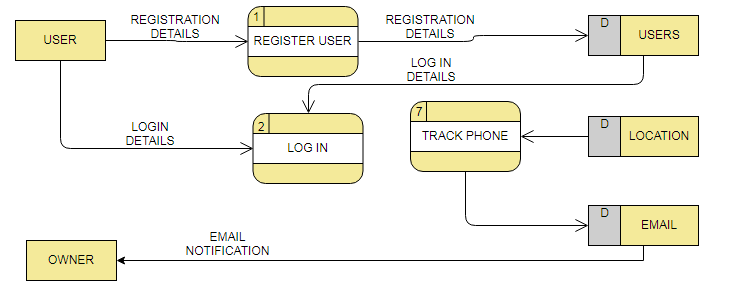


Figure 4. 2 Current System DFD Diagram

## **4.2.1 USER LOGIN**

This process allows only authenticated users to access the application services thus preventing unauthorized access to the application. Only registered users will be able to access the application services.

## **4.2.2 TRACK PHONE AND UPDATE OWNER**

If a mobile phone is stolen and the culprit happens to change the phones SIM card or access the phone like touching the phone without owners consent, an action will be detected and the phone's location and the thief's multimedia information is sent to the owner through an optional phone number and email that he/she entered during the installation of the application. If the event does not alert the victim immediately when the phone is stolen or is misplaced, he/she can go to another person's phone provided they registered under one group with the same application, and use group information to search for his lost phone by viewing location.

## **4.2.1 USER PROFILE**

This defines the user/owner information that he/she has been registered with and it majorly includes the Name, Email, and a Cover Photo

## **4.3 REQUIREMENT ELICITATION METHODS**

### **4.3.1 INTERVIEWS**

Requirements for the system were obtained through interviews of various stakeholders, observations of day-to-day activities of various stakeholders, and analysis of documents.

Interviews against various stakeholders were conducted. These stakeholders included some students, some housekeepers, and security personnel.

The following were the findings during the interviews:

Lack of a well-defined mechanism to track a lost phone

Loss of important material such as study material, phone numbers for friends and family in case of a mobile theft case.

Lack of a mechanism to alert the owner during a theft scenario, which usually occurs at night.

Lack of a mechanism to identify the culprit in a theft case.

### **4.3.2 OBSERVATIONS**

Observations against the day-to-day activities of various stakeholders were done, these stakeholders also included some students, some housekeepers, and security personnel.

## **4.4 PROPOSED SYSTEM**

The main objective of the system was to eventually come up with a mobile phone application capable of alerting the owner during a theft case, identify the culprit in case of theft, and easily track the lost mobile phone by initiating a tracking process through someone with the same application in his/her mobile phone.

## **4.5 USER REQUIREMENTS**

The following are user requirements for each stakeholder that will be involved in using the system:

***Mobile phone user***

* Register
* Log into account.
* View personal information i.e., name, email, profile avatar.
* Edit Profile
* Create groups and add members whom he/she can share location information with members
* Locate a lost mobile phone.

***Admin***

* Send Notifications to users.
* Update the application functions

## **4.6 FUNCTIONAL REQUIREMENTS**

The following are Functional requirements for each stakeholder that will be involved in using the system:

***Mobile Phone***

* Alert the phone owner in case of a theft
* Track another lost phone with the application
* Capture the thief's photo and notify the owner.
* Notify users in case of updates
* Share IMEI number to preferred email address for tracking of your phone.

## **4.7 NON-FUNCTIONAL REQUIREMENTS**

The following are non-functional requirements of the proposed system, which are meant to reinforce functional requirements:

* Appealing graphical user interface.
* The application should be user-friendly and easy to use**.**
* The system should be always available.

## **4.8 FEASIBILITY STUDY**

A feasibility study was carried out to evaluate the project’s potential for success. The following are the types of the feasibility study that was carried out to determine if the project would be reasonable:

* Economic feasibility
* Technical feasibility
* Schedule feasibility

### **4.8.1 Economic Feasibility**

Economic feasibility was carried out to determine whether it is logical and possible to complete by analyzing the project's costs and revenues and comparing it to its benefits.

### **4.8.2 Technical Feasibility**

Technical feasibility was carried out to specify if the project could be delivered with the available technology, techniques, skills, and resources. The laptop is installed with Visual studio code and Sublime Text editors used to code the application and backend respectively. As for skills, the developers we were competent with the following development skills:

* Flutter Framework - Its purpose is to create a powerful UI for the system. Additionally, it helps speed up coding.

Dart Programming Language – was essential in writing the backend side of the application, which helped speed up running the application at run time.

* Firebase Database Service - Its purpose is to allow the application to store real-time data for efficient access to required information
* PHP – Its purpose was to code backend API on the server side since it’s easy to use and will speed development time
* Chrome Dev Tools – This was required for testing the application
* Google Play Store Services-This would be required for Deploying the services
* Git-help in version control of the application.

Seeing the technology, techniques, and skills available, the project is deemed technically feasible.

## **Tools for Design, Development, and Testing**

### **4.8.3 Design and analysis tools**

* Flowchart Diagrams
* Use case Diagrams
* Data Flow Diagrams

### **4.8.4 Development and testing tool**

* Sublime, Visual Studio Code, and IntelliJ Text Editors (as the code editors).
* PHP, MYSQL (handle the application logic and the application database)
* GitHub (for version control), Chrome DevTools, and Real Mobile Phones (for Testing)
* JSON and FIREBASE for creating API and host real-time data.
* Flutter Framework for Developing the application
* Dart Programming Language for front design
* A laptop and Operating system

### **4.8.5 Schedule Feasibility**

Typically, this means estimating how long the application will take to develop, and if it can be completed in a given time period using some methods like payback period. Schedule feasibility is a measure of how reasonable the project timetable is.

# **CHAPTER 5**

# **SYSTEM DESIGN**

## **5.1 Introduction**

This chapter involved creating a blueprint of the proposed system using the requirements defined in the previous chapter.

## **5.2. Architecture Design**

The most suitable architecture design to be used is three-tiered client-server architecture due to its simplistic nature, which allows the three tiers, which include the presentation tier, application tier, and data tier to work as separate modules hence making tiers to be developed separately which can drastically reduce development time faster.

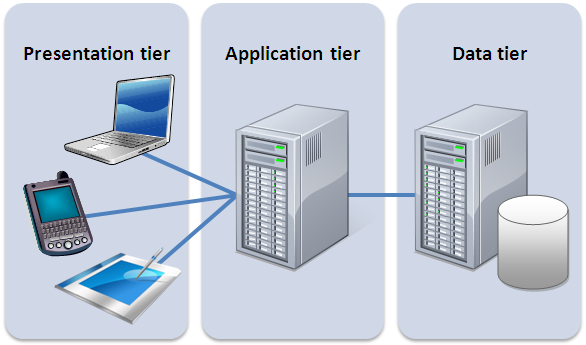
Three-Tiered Client-Server Architecture

Figure 5. 1 Architecture Design

**Presentation tier** – This involves the user interface design i.e., input and output design

**Application tier** – This involves the server API backend design.

**Data-tier –** This involves the database design.

## **5.3 System Design**

The system consist of the following modules, registration, and login, profile management, Phone securing management,

**Proposed system design flow chart.**

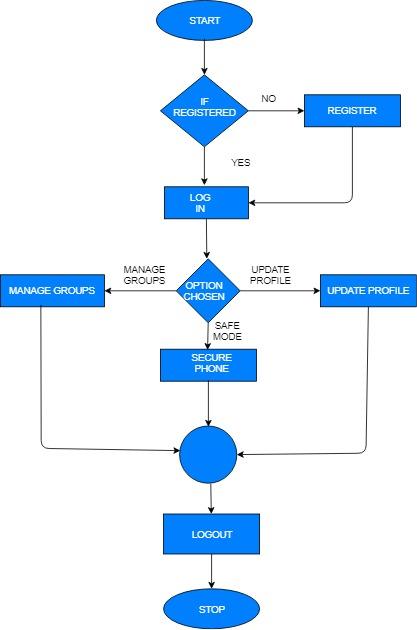


Figure 5. 2 The system design flowchart is as follows.

**The profile management flowchart is as follows**

Diagram

Description automatically generated

Figure 5. 3 The profile management flowchart is as follows

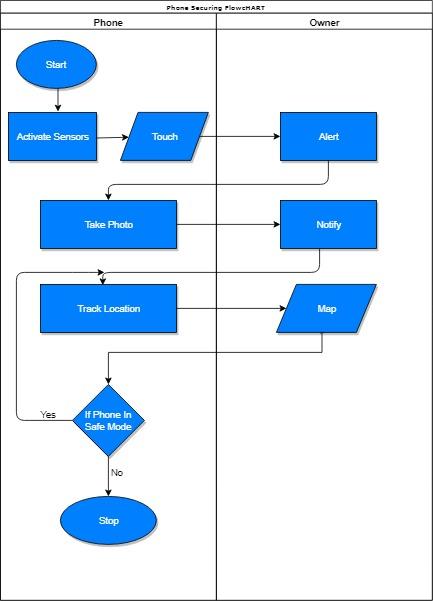
**The phone securing management is as follow**

Figure 5. 4 Proposed System Securing Phone Flowchart

### **5.3.1 Use case diagram**

This diagram shows the interactions between users and the system .It shows the relationships between users and different use cases involved in the system.

**A use case diagram for the current mobile application**

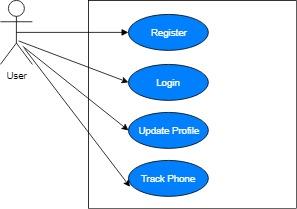


Figure 5. 5 Use case diagram for user

**The use case diagram of both admin and the user is as follow**

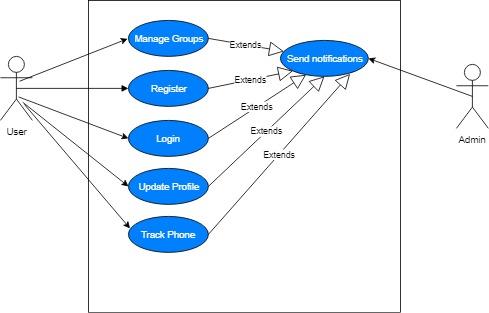


Figure 5. 6 use case diagram for both admin and user

### **5.3.2 Data Flow diagram**

This is a graphical representation of the flow of data within the system. It shows what kind of information will be input to, output from the system, where data will come from, go to, and where it will be stored

**Context diagram**

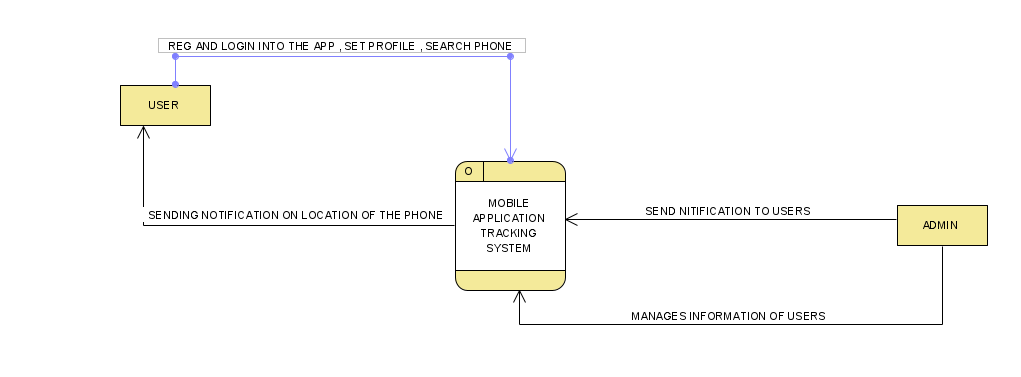
****

Figure 5. 7 Context diagram for the system

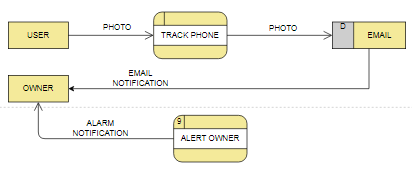
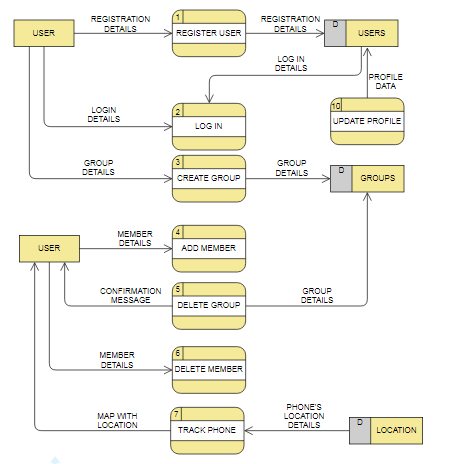
**Data flow for the current mobile application**

Figure 5. 8 Full DFD diagram for entire system

## **5.4 Database design**

In this section, the various entities and their corresponding attributes and data types, as well as the relationships among them were defined based on the user requirements. It also involves the construction of a suitable data model for the system. The design of the database was based on the information that was collected or had been collected in the past. The data are stored in NoSQL firebase server FCM backend provided by Google. Access to the data will be through a web interface running on a cloud fire store server. This design is to allow easy data entry access and querying to users.

The driving philosophy behind the database design was to have an efficient, normalized database that would be easy to maintain and expand, as well as allow easy data entry and access. (Bahmani, Naghibzadeh, & Bahmani, 2008)

The first step in the database design was to analyze the data that would be collected and determine the expected uses of the data. For consistency, each data group is defined as a group of related data tables. Data from one or more surveys may be included in a Group. Analysis of the datasheets and data collection methods identified several different data entities. (Teorey, 1990).

Once the groups were identified, the commonalities between the datasheets within each group were identified. These commonalities would be in one table, to which all of the other tables in the group would be linked. This would provide a connection between the various tables within a group and entities.

To aid in the management of the data and tables, each table would have at least one field that contained a unique identifier for that record, a field to identify who was doing the data entry, and another field to track when the data is entered. In most cases, these fields are hidden from the user and are updated automatically by the system. This information is accessible by the administrator for troubleshooting purposes (Shasha & Bonnet, 2002). .

### **5.4.1 Entities**

* Members (users)
* Images
* Locations (group occurrence)
* Groups

### **5.4.2 Conceptual database design**

This involves a comprehensive conceptual schema for the system that is best represented by an entity relationship diagram describing how entities relate to each other within the system .Below is a list of the entities in this system and their respective attributes

#### **5.4.2.1 Entities and Attributes tables**

| **Entity** | **Attributes** | **Description** |
| --- | --- | --- |
| Member | Full Name | User first name |
|  | Phone Number | User mobile number |
|  | Email | Email Address |
|  | User Name | Account user name |
|  | Password | User password |
|  | Image | Members image |

| Entity | Attribute | Description |
| --- | --- | --- |
| Groups | group number | Group ID |
|  | group name | Members Group name |

| Entity | Attribute | Description |
| --- | --- | --- |
| Image | Image No | Image ID number |
|  | Image name | User image name |
|  | Image url | Image location |

| Entity | Attribute | Description |
| --- | --- | --- |
| Group occurrence(location) | Group No | Group ID number |
|  | Members id | Member id |

### **5.4.3 Physical design tables**

Table 5. 1 Members

| Field Name | Field Type | Field Size | Description |
| --- | --- | --- | --- |
| Full Name | Text | 100 | User full name |
| Phone Number | Number | 45 | User mobile number |
| Email | Varchar | 50 | Email Address |
| Username | Varchar | 50 | Account Username |
| Password | Varchar | 60 | User Password |

Table 5. 2 Image

| Field name | Field type | Field size |
| --- | --- | --- |
| Image name | varchar | 200 |
| Image id number | int | 11 |
| Image url | varchar | 200 |

Table 5. 3 Groups

| Field name | Field type | Field size |
| --- | --- | --- |
| Group name | varchar | 100 |
| Group id number | varchar | 100 |

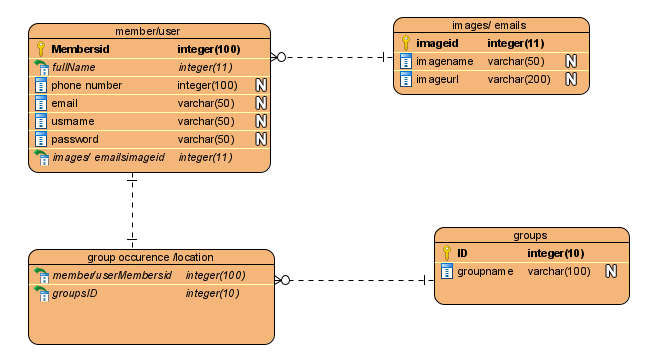
Table 5. 4 Group occurrence (location)

| Field name | Field type | Field size |
| --- | --- | --- |
| Group id | varchar | 200 |
| Members id | varchar | 200 |

**The database design of the system is as follows and the entity relation diagram.**Graphical user interface, text, application, chat or text message

Description automatically generated

Figure 5. 9 Entity relation diagram.



Entity relationship models incorporate some of the important semantic information about the real world. A special diagrammatic technique is introduced as a tool for database design. An example of database design and description using the model and the diagrammatic technique is given (Chen, 2002)

System design covers the recommendation and the suggested guidelines on implementing an event triggered anti-theft mobile security application.

## **5.5 class diagram**

 Class diagram in the [Unified Modeling Language (UML)](https://en.wikipedia.org/wiki/Unified_Modeling_Language) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects (Visual paradigm, 2021).

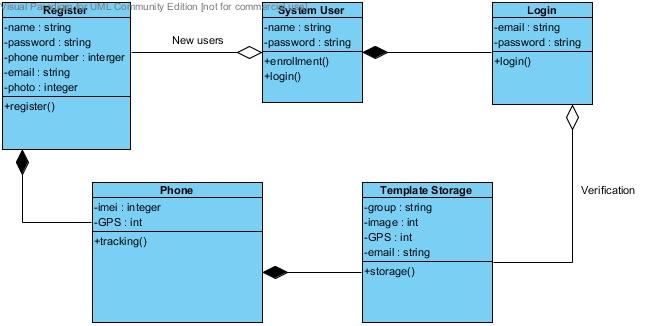


Figure 5. 10 Class diagram

# **CHAPTER 6**

# **SYSTEM IMPLEMENTATION**

## **6.1 Introduction**

This chapter covers the various tools that we have used for coding and testing the developed system and how testing was done to ensure the system is bug-free. Furthermore, it covered the various changes over techniques that a user would use to shift to adapt the use with ease.

## **6.2 Tools for Development**

Tools that were used to develop the system comprise both software and hardware.

### **6.2.1 Software Tools for Development**

As per software. The following tools were used in developing the system

* IntelliJ – IDE used to develop different applications for different platforms e.g., mobile applications, web applications, desktop applications, etc. It majorly employs programming languages such as Java, kotlin, Dart, and Swift. Furthermore, it employs platforms such as Flutter, Android, etc.

**Why Use IntelliJ IDE**

* Using the Flutter framework, we were able to easily create cross-platform applications.
* Using the Flutter framework, one can create rich and powerful user interfaces, which require few lines of code to achieve reducing development time.
* Sublime Text – IDE is used to develop a Backend API for the developed application.

**Why Use Sublime IDE**

* Allows one to code APIs with ease by providing suggestions speeding up the development process.
* Color variations of different code types make it easy to identify syntax errors and correct them easily.
* Firebase Database – A Cloud Database by Google. for hosting real-time data

**Why Use Firebase**

* Easy to set up the Databases
* Support scalability with ease.
* Better performance in terms of speed and handling errors.

**Procedure for setting up firebase database to work with the application**

The Firebase Real-time Database is a cloud-hosted NoSQL database that lets one store and sync data between users in real-time. The goodness with firebase is that one only signs in to the firebase services by the email address then he/she registers his/her application under console, where it provides with all the services required for the storage of information for the application.

* We downloaded the Firebase Android **config file**google-services.json and added it under **android/app**, in android studio.

Navigate to the **android/build.gradle** and add the google maven repository and the google-services class path

Then inside the android\app\build.gradle, we added the following:

* apply plugin: 'com.android.application'
* apply plugin: 'kotlin-android'
* apply plugin: 'com.google.gms.google-services'

Therefore, inside pubspec.yaml we added the following:

Dependencies:

* cupertino\_icons:
* firebase core:
* firebase database:

### **6.2.2 Hardware Tools for Development**

As per software, we used the following tools in developing the system

* Mobile phones with an Android operating system
* Up to date laptop running Windows Operating System

## **6.3 Tools for Testing**

After the development of the proposed system, the system went through various tests to check for various aspects of the system. The tools, which were used to achieve this, were both hardware and software as shown below.

### **6.3.1 Software Tools for Testing**

As per software, the following tools were used in testing the system

* Android Emulator – To allow testing in the android environment.
* Mobile phone
* IntelliJ In-Built Application Debugger – To allow testing and analysis of code performance on various platforms.

### **Hardware Tools for Testing**

* Mobile Phone Running android operating system – To allow testing in a real-world environment
* Laptop – To create and run test scripts.

**Interface for user input of data to allow signing up to the application, to allow logging in.**

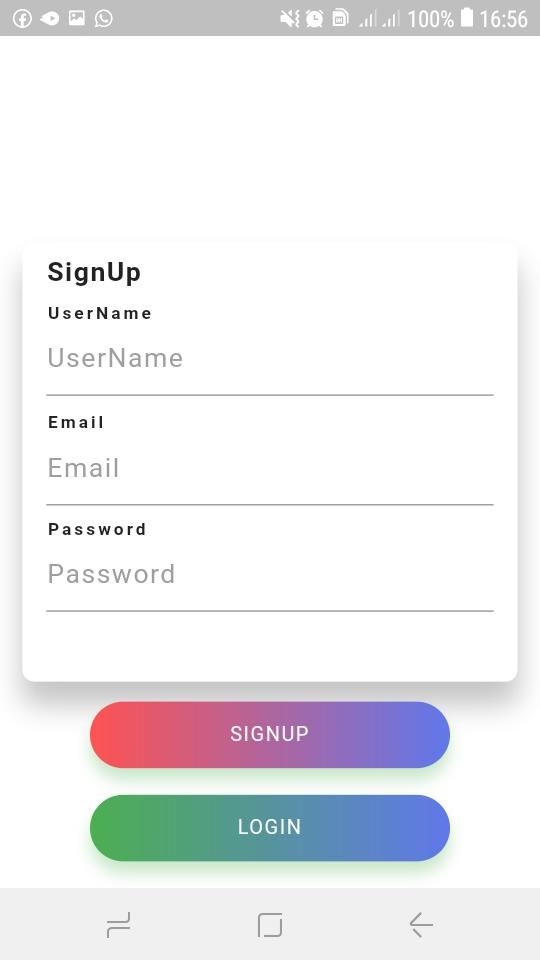
****

Figure 6. 1 Signup page

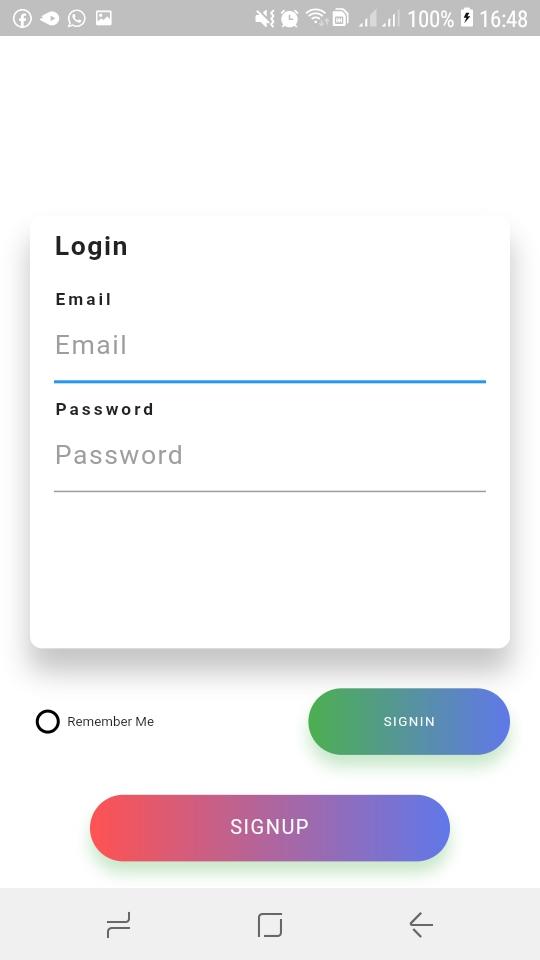
****

Figure 6. 2 Login interface

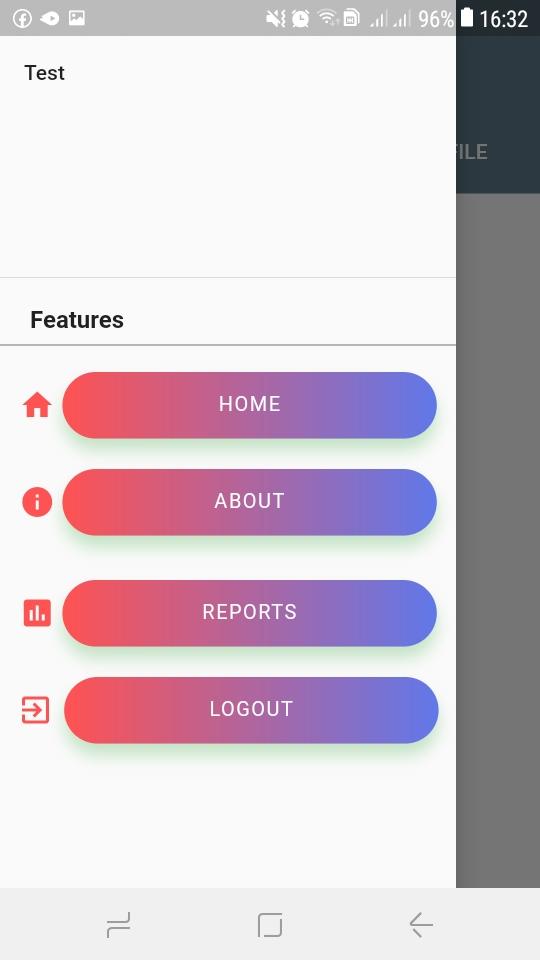
****

Figure 6. 3 The navigation bar of the system

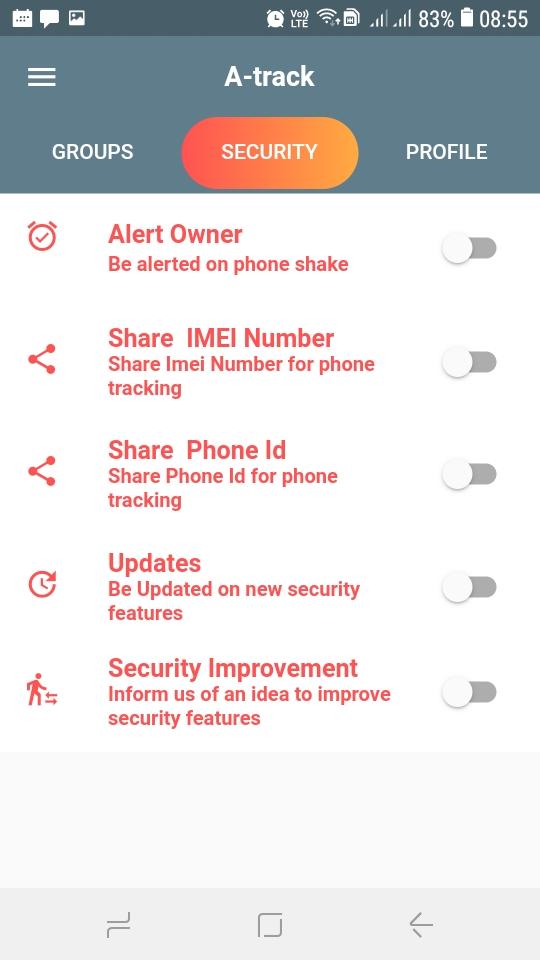
****

Figure 6. 4 Main design user interface

Setting profile page

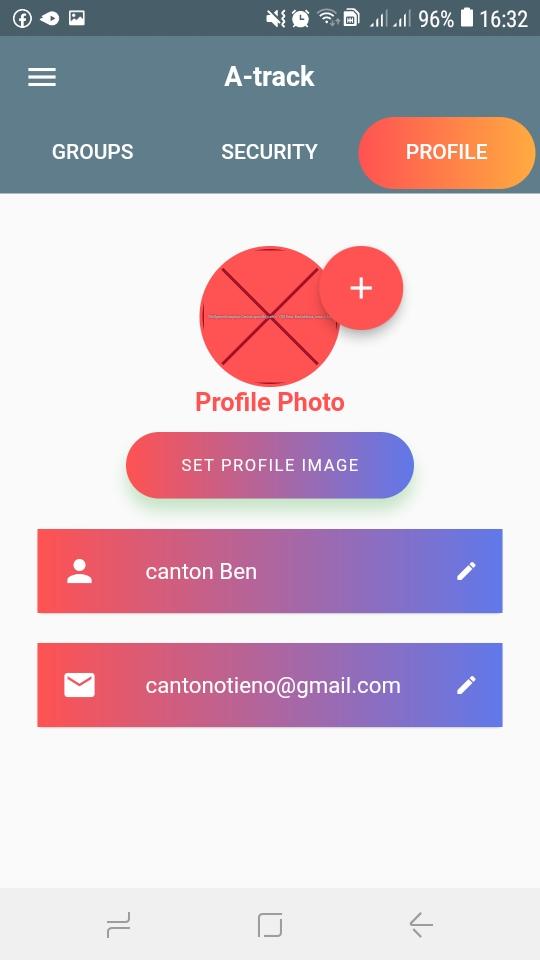


Figure 6. 5 setting profile window

Joining group page

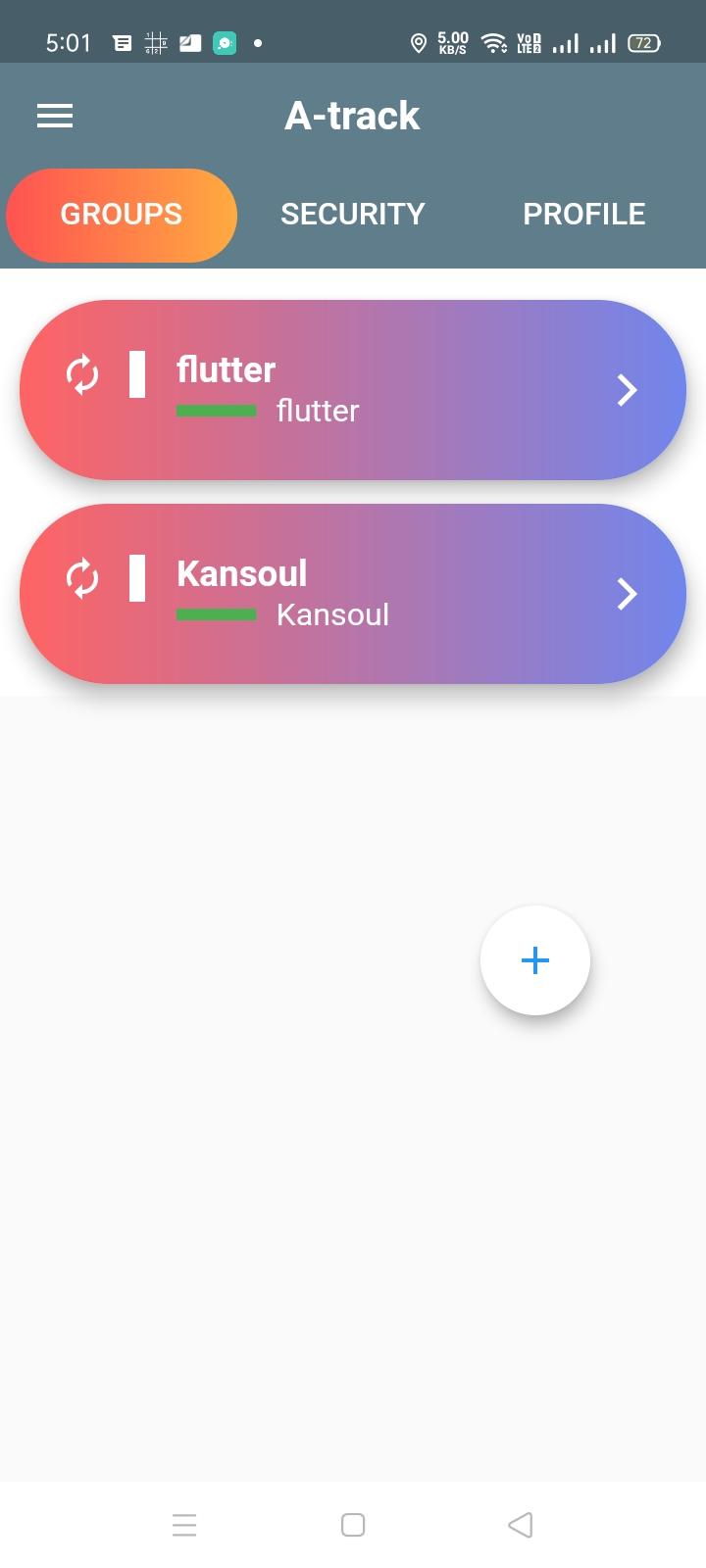


Figure 6. 6 joining group and viewing the location of your member’s page

**Snapshot of firebase database**

This is the implantation of firebase database and its features it includes user authentication, cloud\_ firestore database and the storage.

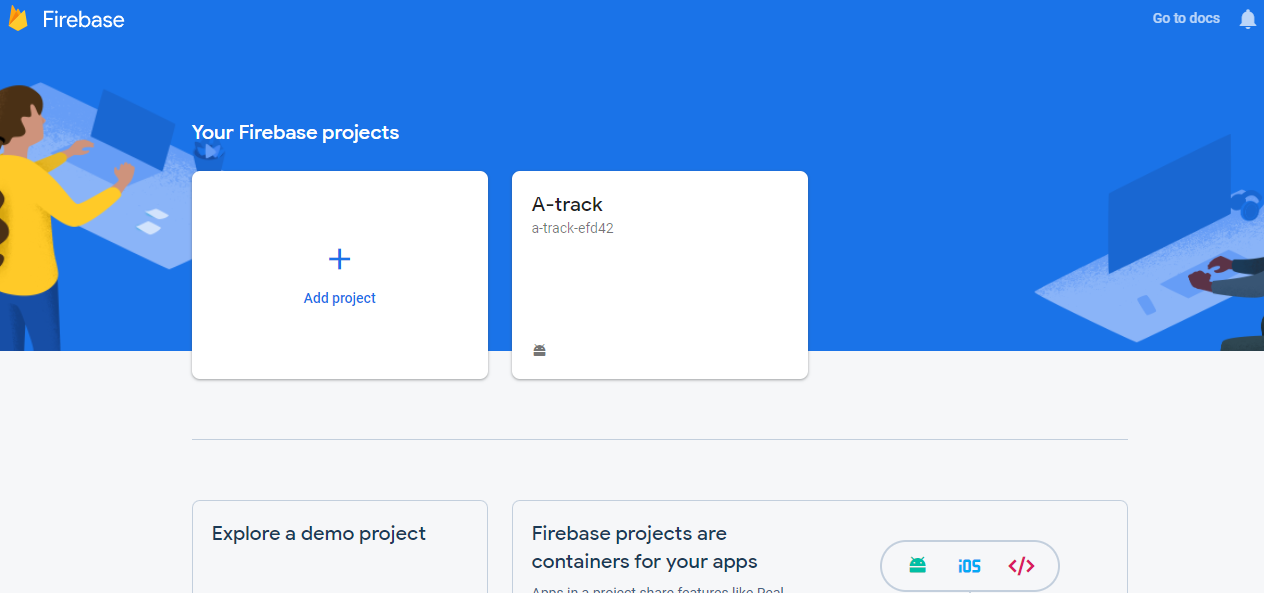
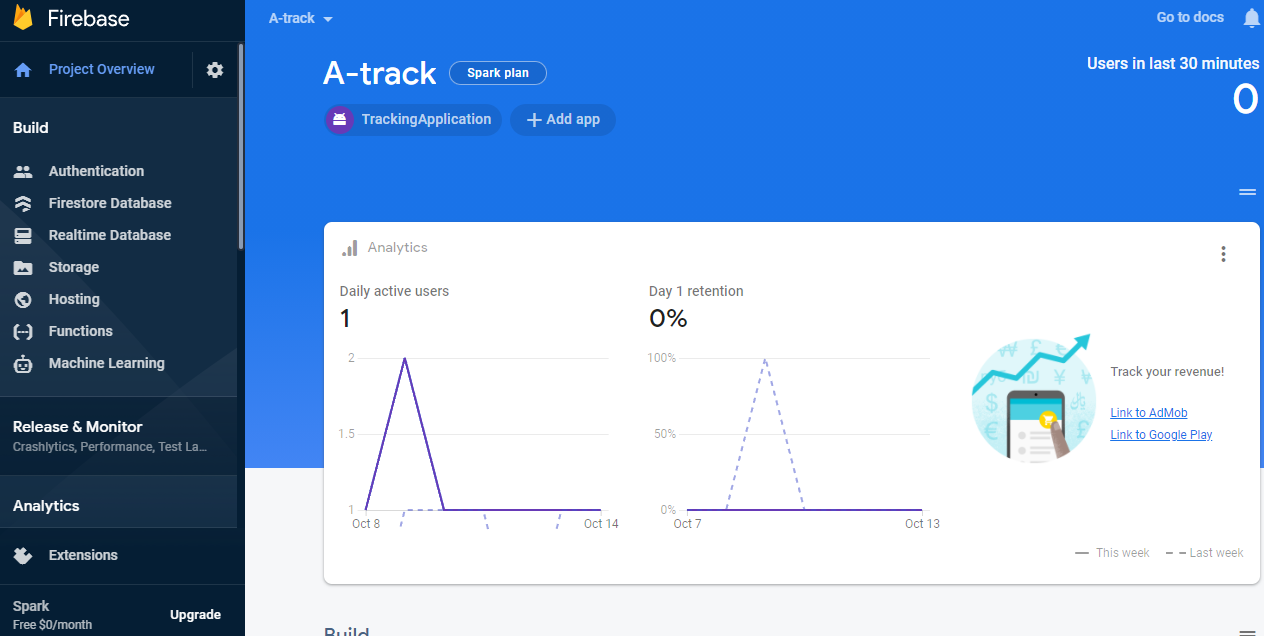
****

Figure 6. 7 Firebase database

****

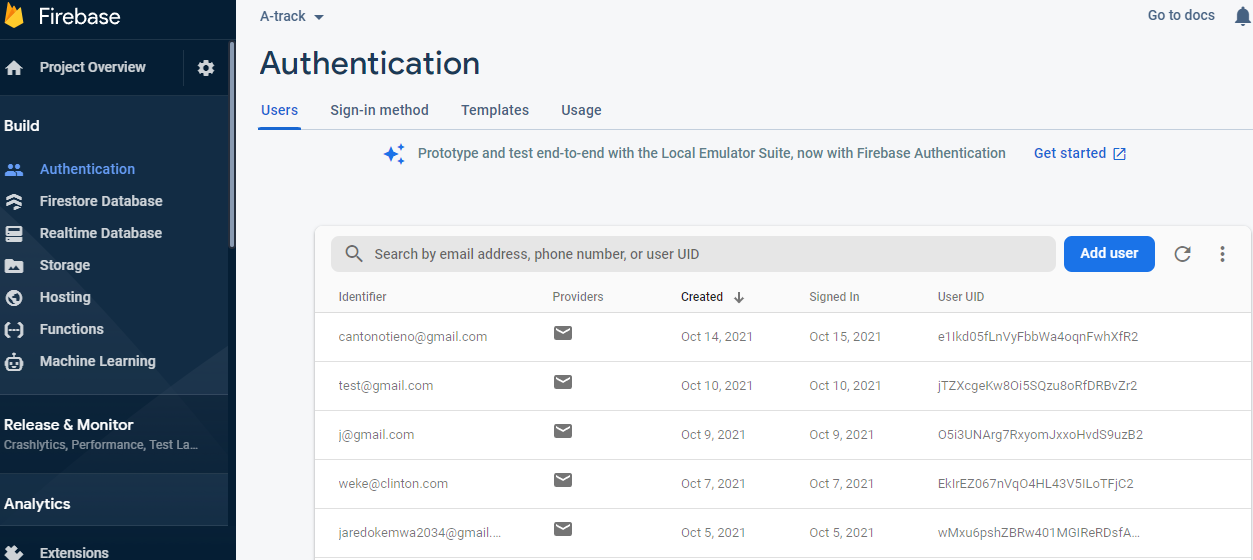
****

Figure 6. 8 Authentication, showing users that have sign in the application

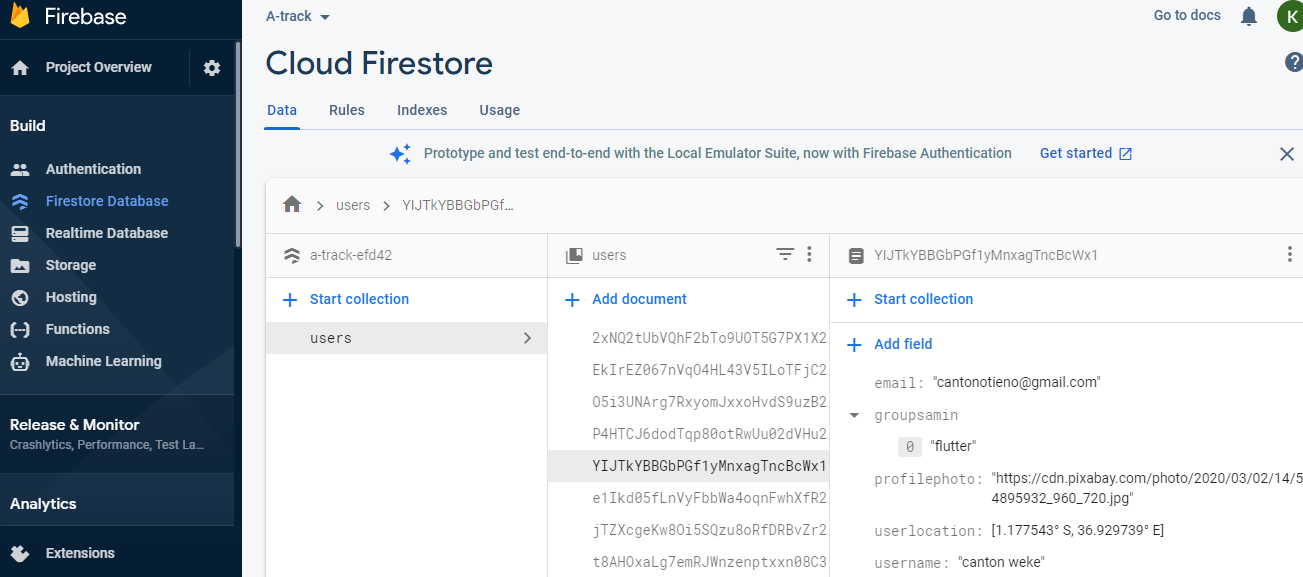
****

Figure 6. 9 Cloud\_firestore

# **CHAPTER 7**

## **TESTING PROCESS**

The Developed system went through various testing processes to ensure that the system functioning as it is supposed to. This was done before deploying the system to the real-world environment, and has the development of application is going on It mainly involve the following.

1. Unit Testing
2. Functional Testing
3. Performance Testing
4. Stress Testing

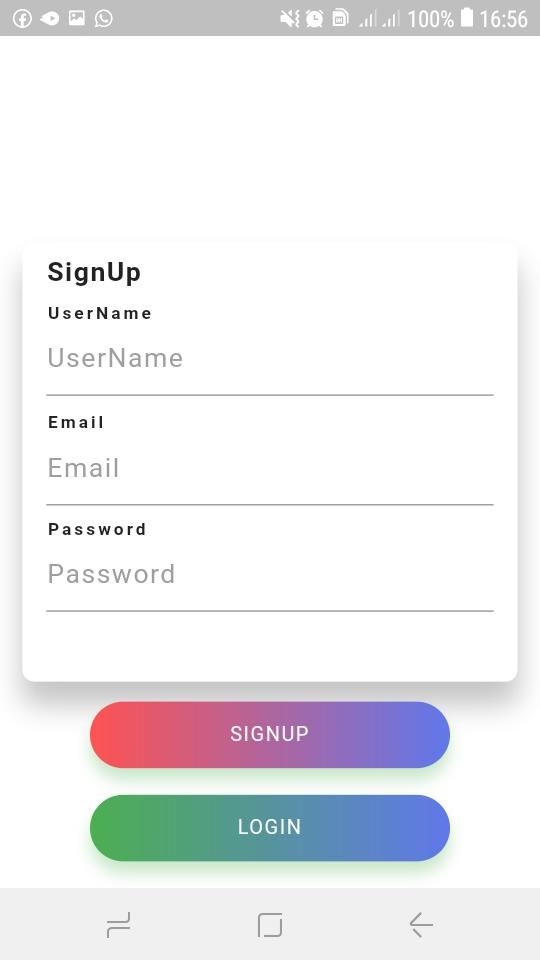
### **7.1 Unit Testing**

This involved carrying out the various test on each of the modules to ensure that they carried out their functions as expected to detect and correct errors as they arose.

### **7.2 Functional Testing**

This test was carried out at the end of the of the development stage. It involved verification of whether the functional requirement were all met by the system. This testing mostly involved:

1. Ensuring posting of valid inputs into the database through the implementation of various form validation techniques.

****

1. Ensuring the correct display of information from the database
2. Ensuring the various functions and procedures were being invoked and implemented correctly to ensure the output of the correct result.

### **6.3 Performance Testing**

Here the system efficiency was tested to see how the system and its infrastructure would respond in the real world environment. The system characteristics that were measured include response time, resource consumption on the serve, throughput, and processing speed.

### **7.4 Stress Testing**

As opposed to performance testing, I tested to see how the system would perform when given unfavorable conditions. These unfavorable conditions include:

1. Performing resource-intensive operations like map display.



Figure 7. 1 Showing location ben

Tracking user location

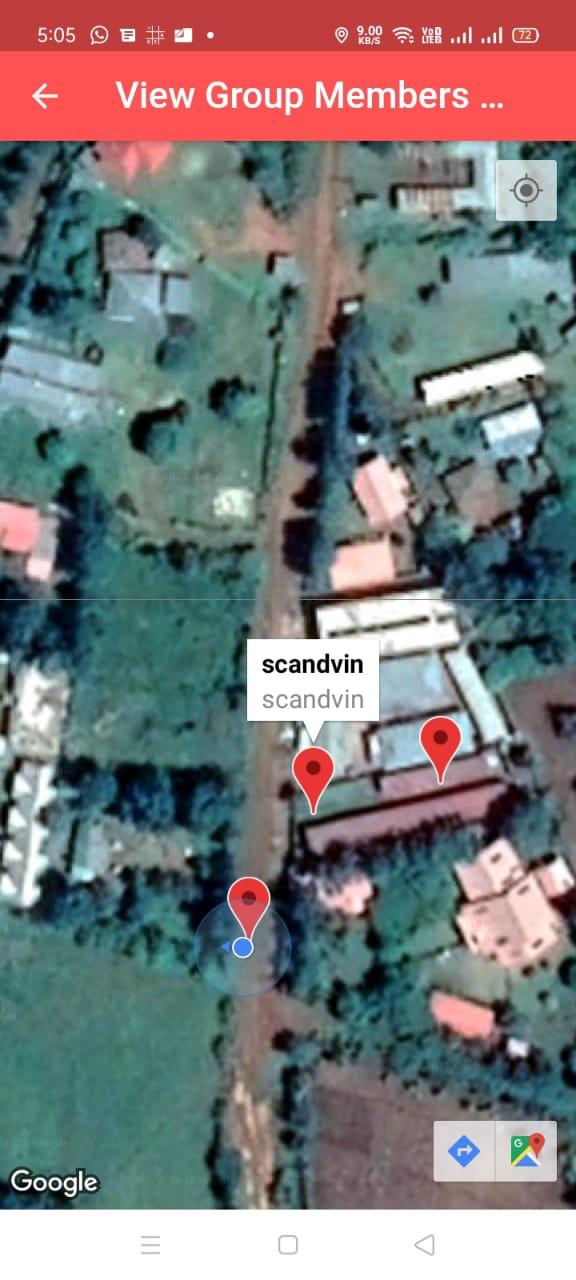


Figure 7. 2 Tracking bens position

1. Limiting the bandwidth of the test device to 2G instead of the 3G or 4G
2. Testing if the application can work on background and track user location.

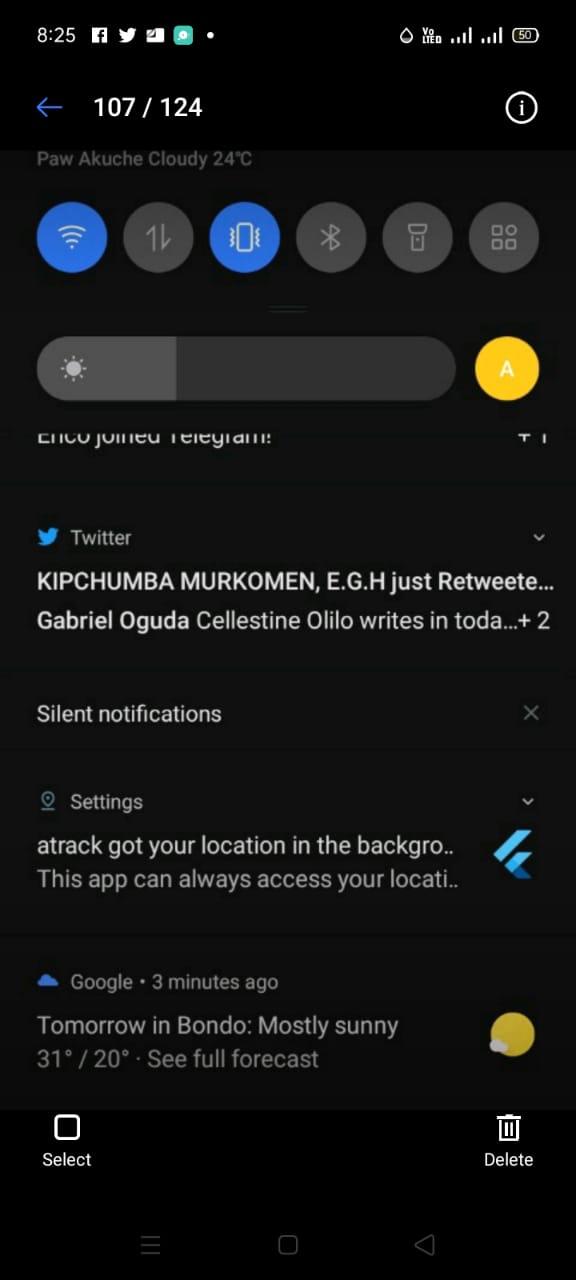


Figure 7. 3 Showing how the system run in background

## **7.5 Proposed Changeover Techniques**

This involves the techniques implemented by users to shift from the already existing system to the new system. The recommended changeover techniques that should be adopted by users is the phased over changeover techniques.

As opposed to changeover techniques, phased changeover techniques can allow various modules to be implemented at different times. This gives room to the users to be trained at a reasonable pace and familiarize themselves with the various parts of the system before the whole system is actually implemented.

## **7.6 Ethical Considerations**

During this research process of developing this application, we uphold the integrity and high moral standards. We seek permission from our fellow students and other stakeholders before distributing the questionnaires and before conducting the various interviews. We keep time, respect the respondents’ feedback and decision and treat the information given by the respondents with confidentiality so that they will not be disclosed to any third party without their consent.

## **7.7 Mobile Security Risk assessment and risk mitigation**

### **7.7.1 Risk**

Is a situation involving exposure of danger, one of the major concerns for mobile app development is the rising mobile app security risks, particularly to prevent data breaches It has been noticed that as technology advances, it has become easier to build and deploy both android and iOS apps, but also easy to crack a mobile application’s security as we developers are still writing insecure code.

**Some example of mobile security risk application**

**Insecure Communication;** Mobile developers often use SSl/TLS only during authentication but not elsewhere. This leads to an inconsistent security layer, which increases the risk of exposing sensitive data such as credentials, personal information, session IDs, and more to interception by attackers.

* **How will we mitigate this mobile security risks**

Only establish a secure connection after authenticating the identity of the endpoint server. While applying SSL/TLS to mobile application, one should make sure to implement it on the transport channels that the mobile app will use to transverse sensitive data such as session tokens and credential

**Lack of Input Validation**

When the mobile application does not validate input properly, it puts the application at risk of exposure to attackers who might be able to inject malicious data input and gain access to sensitive data in the app or breach backend data stores.

* **How it might be solve**

Minimum and maximum value range check for strings, minimum and maximum length check for dates and numerical parameters.

**Poor Encryption**

Poor encryption can lead to data loss and all of the repercussions that follow from that loss of information.

* **How it might be solve**

By implementing modern encryption algorithms that are accepted as strong by the security community. Use the encryption APIs available within your mobile platform

# **CHAPTER 8**

# **LIMITATIONS, RECOMMENDATIONS, AND CONCLUSIONS**

## 8.1 **Limitations**

The developer faced the following challenges during the development of the system

1. Internet connectivity and accessibility. Access to quality internet was a huge challenge and many times during development, the developer had to use school internet, which was hard to secure. This really slowed down the development process.\
2. Complexity of the application. Implementing the business logic of the application was due to the nature of required system functionality.

Although the system was developed successfully. There are but few challenges that could limit the system working system capabilities. This include:

1. The system requires internet access to work efficiently; therefore, the system would be down whenever there is no internet access.
2. If the thief factory resets the phone, the application would be lost.

## **8.2 Recommendations**

The system met most of the requirements as stated in the project objectives. However, given more time, further improvements could be made such as making the application a system application thus avoiding its deletion during factory reset operation and capturing culprit photos using the camera without delaying and increasing the sensitivity of the sensors in the application.

## **8.3 Conclusion**

The developed system will have the potential to prevent mobile theft among students in the hostels, as such preventing loss of important items and resources in the owners' phones. Furthermore, it will also streamline other processes such as tracking a lost phone and locating the location of different individuals, as such users are encouraged to embrace the system and give valuable feedback for a better tomorrow.

# **REFERENCES**

A Simple Flutter Android App that displays Sensor Data. (2021, July 3). Retrieved from

<https://flutterawesome.com/a-simple-flutter-android-app-which-displays-sensor-data/>

Martinez, J., H. (2012). *Mobile Device Security: Current Challenges and Existing Solutions*. Western Michigan University, USA: Western Michigan University Press

Desale, V., Dhalpe, S., Bakhale, T., Dongare, V., & Kadam, S. Finding Lost Android Devices Using Mms Technology.

Retrieved from <https://medium.com/@info_67212/how-to-send-a-screenshot-attachment-in-mail-using-flutter-703a2bba882f>

Shedge, N., K., Dhatrak, C., D., Ugale, S., K., Asmita, P., & Khade, S., A. (2017). Mobile Theft Tracking Application. *International Research Journal of Engineering and Technology, 4(1),* 620-623. Retrieved from <https://www.irjet.net/archives/V4/i1/IRJET-V4I1105.pdf>

**S**rilekha1, B., & Dhanakoti, V. (2016). Mobile Tracking Based on Phone Theft Detection. *International Journal of Advanced Research in Computer and Communication Engineering, 5(3),* 192-197. Retrieved from <https://www.ijarcce.com/upload/2016/march-16/IJARCCE%2048.pdf>

Subha, K., & Sujatha, S. (2016). Anti-Theft Tracking System for Smart Phones. *International Journal of Advanced Research in Computer Science and Software Engineering*, *6(5),* 134-138. Retrieved from <https://pdfs.semanticscholar.org/de57/341a649955fdb349f726be4253b46d0223d3.pdf>

ZahiraJahan, N., Phil, M., & Vinodhini, R. (2016). Smartphone Tracking Application Using Short Message Service. *International Journal of Computer Techniques, 3(2),* 89-94. Retrieved from <http://oaji.net/pdf.html?n=2017/1948-1513927108.pdf>

Wagh, T., Bagrecha, R., Salunke, S., Shedge, S., & Lomte, V. (2021). A Survey on Vehicle to Vehicle Communication. In *Computational Methods and Data Engineering* (pp. 163-175). Springer, Singapore.

Hammood, W. A., Abdullah, R., Hammood, O. A., Asmara, S. M., Al-Sharafi, M. A., & Hasan, A. M. (2020, February). A review of user authentication model for online banking system based on mobile IMEI number. In *IOP Conference Series: Materials Science and Engineering* (Vol. 769, No. 1, p. 012061). IOP Publishing.

Bareth, U., & Kupper, A. (2011, July). Energy-efficient position tracking in proactive location-based services for smartphone environments. In *2011 IEEE 35th Annual Computer Software and Applications Conference* (pp. 516-521). IEEE.

Fawaz, K., & Shin, K. G. (2014, November). Location privacy protection for smartphone users. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 239-250).

[Bisarahalli](https://blog.geekyants.com/@manoj_38837?source=post_page-----14b67ef17404----------------------), M. (2021, Nov 10). Flutter hands-on: Building a Live Location Sharing App. Retrieved from <https://blog.geekyants.com/flutter-hands-on-building-a-live-location-sharing-app-14b67ef17404>

# Thiran, T. (2018, Aug 4). How to send a screenshot attachment in Mail using Flutter.

Adam, I. Y., Varol, C., & Varol, A. (2019, June). Problems, Prospects of Anti-Theft, and Mobile Phone Tracking: A case in Nigeria. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

Suri, S. (2021, Aug 18). Using Camera on Flutter. Retrieved from <https://www.raywenderlich.com/4333657-using-the-camera-on-flutter>

The use of SSADM (Structured systems analysis and design methodology) as a standard methodology on information systems projects. (n.d.). GRIN - Buy academic papers and publish yours free. <https://www.grin.com/document/106034>

Kumar, K., Kaur, P., & Amritsar, G. N. D. U. (2015). Vulnerability detection of international mobile equipment identity number of smartphone and automated reporting of changed IMEI number. International Journal of Computer Science and Mobile Computing, 4(5), 527-533.

Sudiartha, I. K. G., Indrayana, I. N. E., Suasnawa, I. W., Asri, S. A., & Sunu, P. W. (2020, July). Data Structure Comparison between MySql Relational Database and Firebase Database NoSql on Mobile Based Tourist Tracking Application. In *Journal of Physics: Conference Series* (Vol. 1569, No. 3, p. 032092). IOP Publishing.

Sharman, D., & Kendall, E. J. M. (1988). A case study: Acquiring strategic knowledge for expert system development. *IEEE Intelligent Systems*, *3*(03), 32-40.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011, May). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *2011 IEEE Symposium on Security and Privacy* (pp. 96-111). IEEE.

Owusu, E., Han, J., Das, S., Perrig, A., & Zhang, J. (2012, February). Accessory: password inference using accelerometers on smartphones. In *proceedings of the twelfth workshop on mobile computing systems & applications* (pp. 1-6).

*Your server environment and FCM*. (n.d.). Firebase. <https://firebase.google.com/docs/cloud-messaging/server>.

Teorey, T. J. (1990). *Database modeling and design: The entity-relationship approach*. Morgan Kaufmann Publishers Inc.

Shasha, D., & Bonnet, P. (2002). *Database tuning: principles, experiments, and troubleshooting techniques*. Elsevier.

Chen, P. P. S. (2002). The Entity Relationship Model—Toward a Unified View of Data. In *Software Pioneers* (pp. 311-339). Springer, Berlin, Heidelberg.

Lu, H., Yang, J., Liu, Z., Lane, N. D., Choudhury, T., & Campbell, A. T. (2010, November). The jigsaw continuous sensing engine for mobile phone applications. In *Proceedings of the 8th ACM conference on embedded networked sensor systems* (pp. 71-84).

Arikpo, I. I., & Osuobiem, G. I. (2020). A SOFTWARE TOOL FOR RECOVERING LOST MOBILE PHONES USING REAL-TIME TRACKING. *International Journal of Advanced Research in Computer Science*, *11*(3).

Baron, N. S. (2011). Concerns about mobile phones: A cross-national study. *First Monday*.

Kibona, L., & Mgaya, G. (2015). Smartphones’ effects on academic performance of higher learning students. *Journal of Multidisciplinary Engineering Science and Technology*, *2*(4), 777-784.

Kumar, K., Kaur, P., & Amritsar, G. N. D. U. (2015). Vulnerability detection of international mobile equipment identity number of smartphone and automated reporting of changed IMEI number. *International Journal of Computer Science and Mobile Computing*, *4*(5), 527-533.

Handoyono, N. A. (2020). Development of android-based learning application in EFI materials for vocational schools. In *Journal of Physics: Conference Series* (Vol. 1456, No. 1, p. 012050). IOP Publishing.

Bahmani, A. H., Naghibzadeh, M., & Bahmani, B. (2008, May). Automatic database normalization and primary key generation. In *2008 Canadian Conference on Electrical and Computer Engineering* (pp. 000011-000016). IEEE.

Visual paradigm. (2021, November 22). Retrieved November 22, 2021, from <https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-class-diagram/>

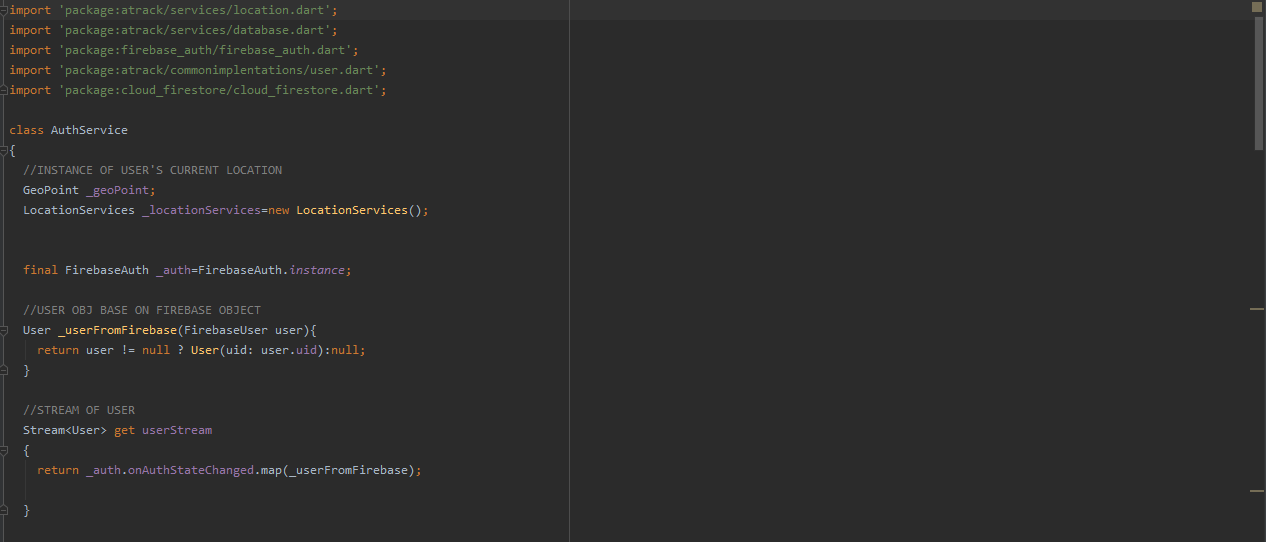
Bao, Y. M., Niu, Z., & LI, D. H. (2006). Discussion on GPS. *Technology & Economy in Areas of Communications*, *4*(36), 68-71.

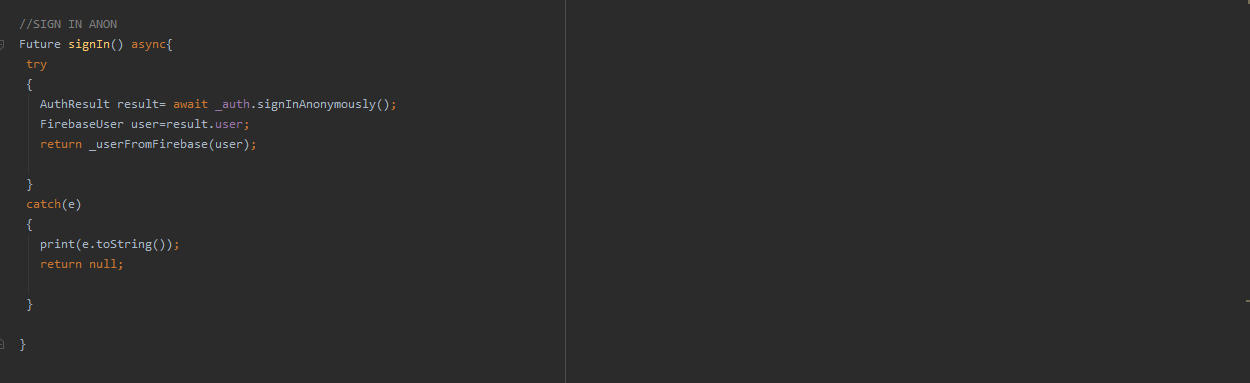
# **APPENDICES**

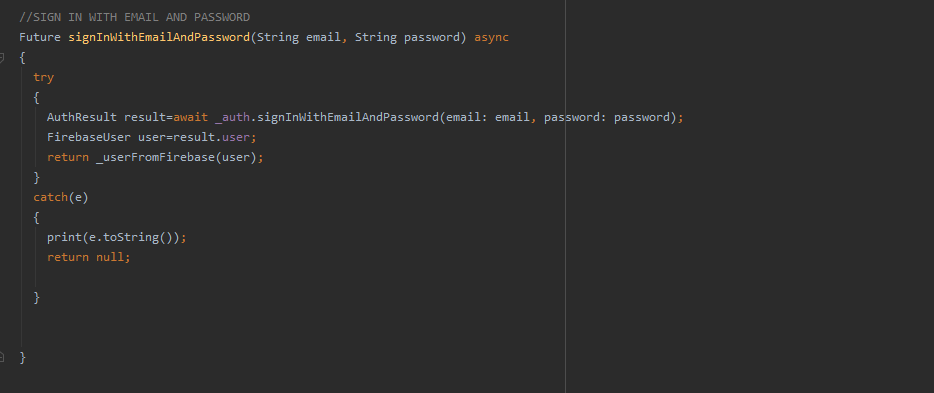
# **APPENDIX A**

## SYSTEM CODES

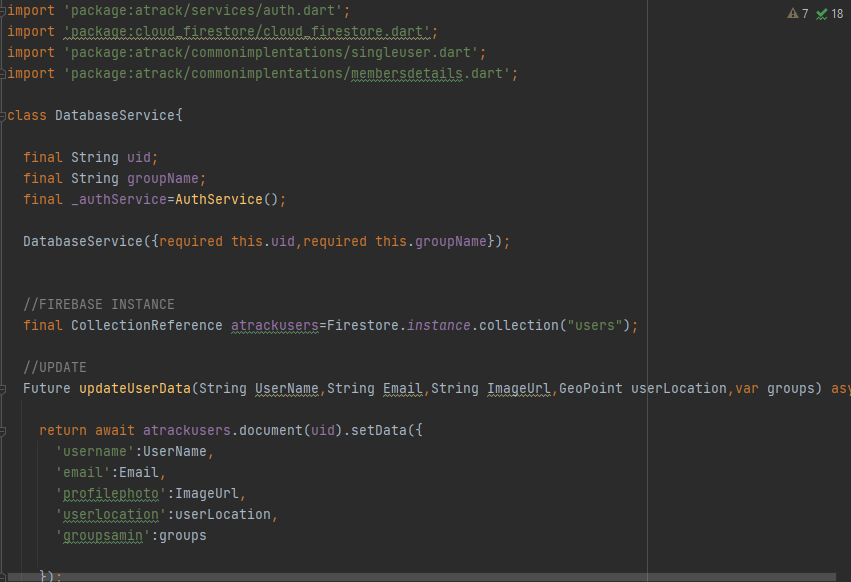
### User authentication



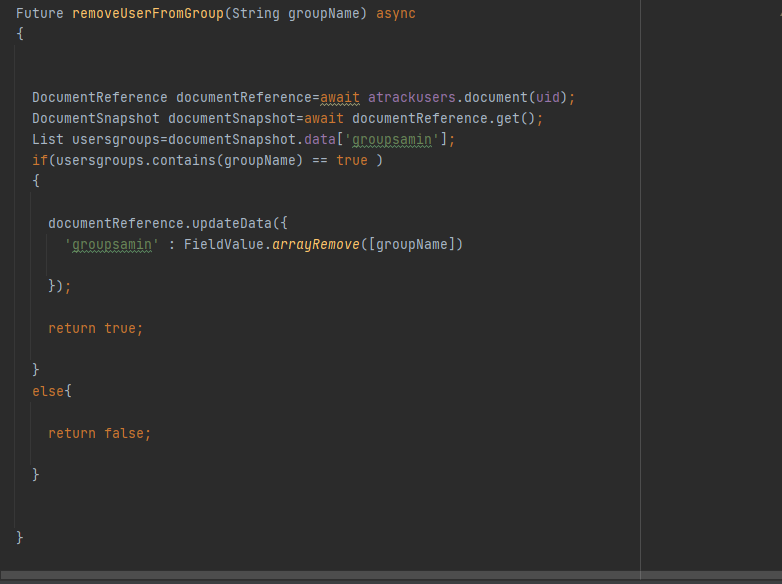




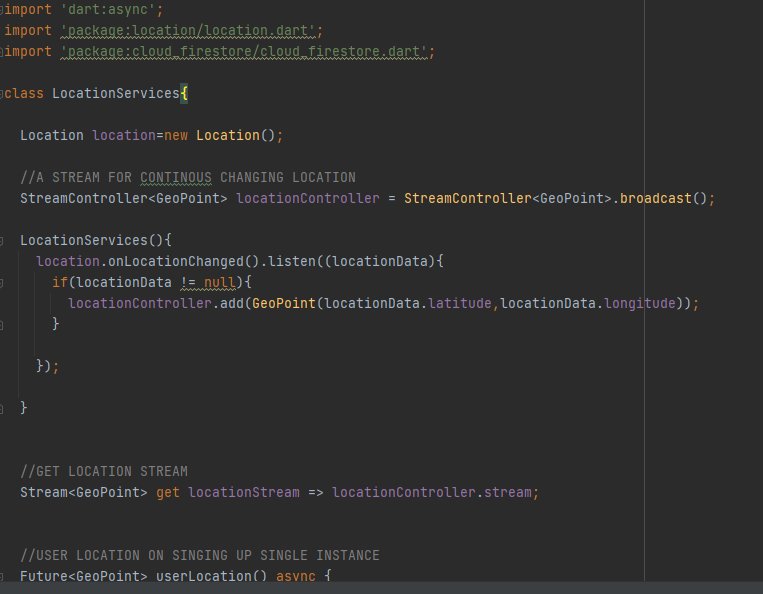
### Database service sample codes

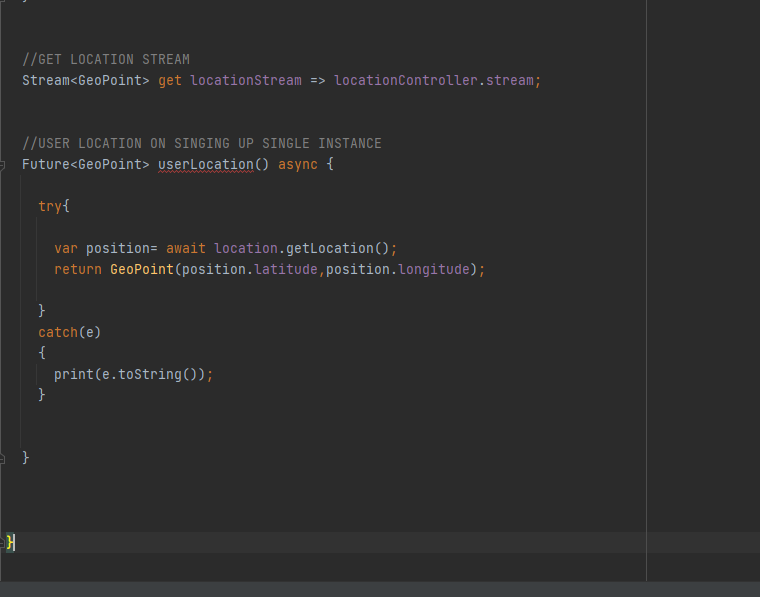




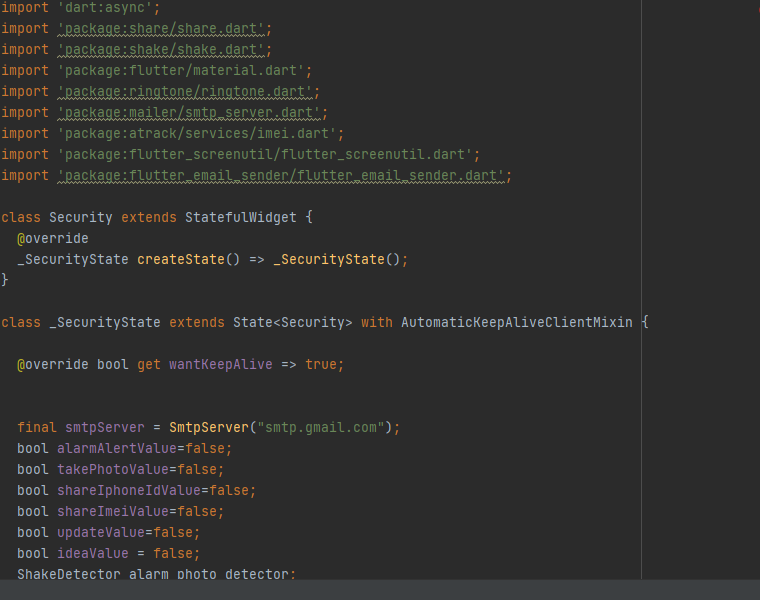


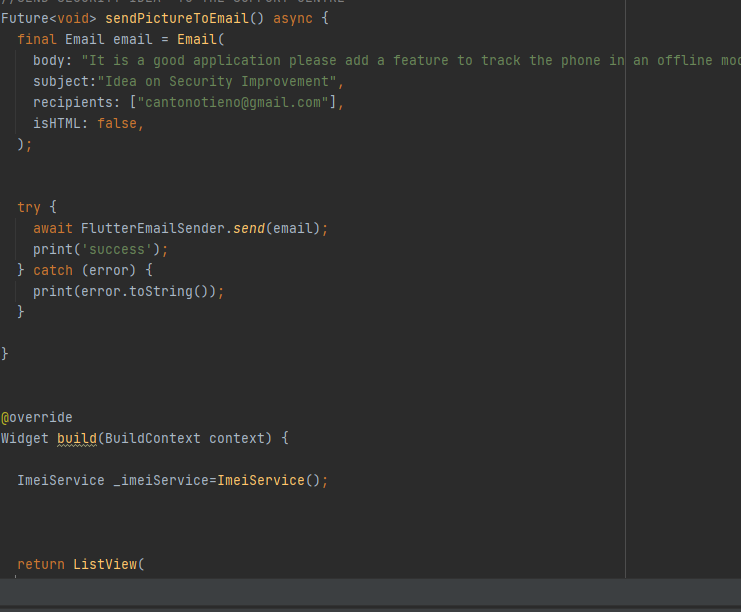
### Location services codes





### Security codes







# APPENDIX B

## **System User’s Manual**

## **1 General Information**

### **System** **Overview**

Event triggered anti-theft mobile security application is an application built to improve phone security and eradicate phone theft. It employs geospatial features for phone tracking by sharing location between different users. It also employs sensors for alerting users if the phone is in a safe mode. Furthermore, the user can be able to share phone ID and phone IMEI number to facilitate phone tracking.

### **1.1 System Configuration**

Event-triggered anti-theft mobile security application is a mobile application that can run on mobile phones. This system has a remote database system hence it requires an internet connection to save and retrieve data from the database.

## **1.2 User Access Levels**

Registered users can only access the system. However, the users are categorized into two roles, that is administrator and phone users/ owners

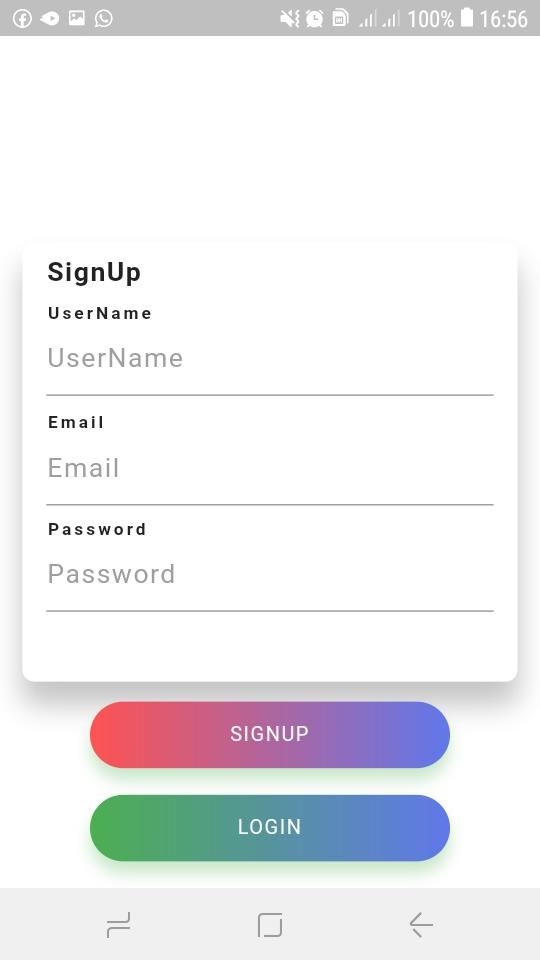
## **Contingencies**

The system requires internet connection for access and operation. In the case of power usage, data that a user was entering into the systems through the system forms, data will not be saved. In addition, the application may not capture the photo of the culprit.

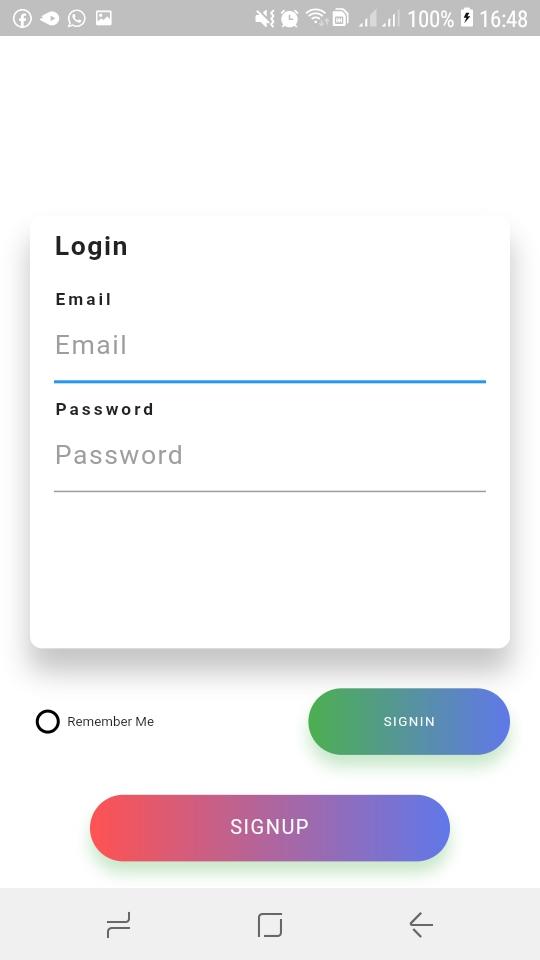
## **2 Getting started**

1. **Installation and Logging in**

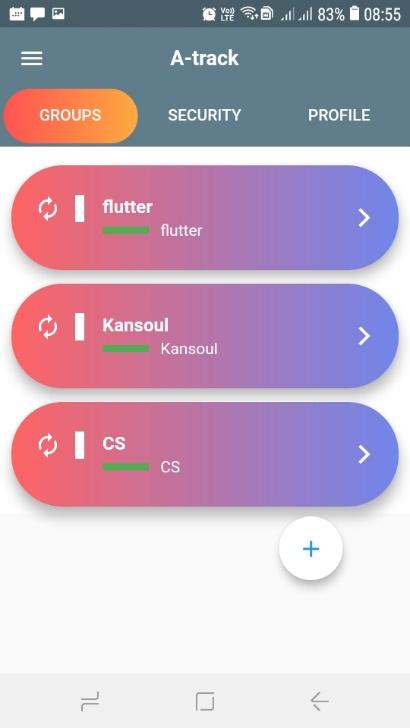
Once the user has installed the application then he or she can register as shown below

****

Once the user has successfully registered, then he or she can Log in as shown below

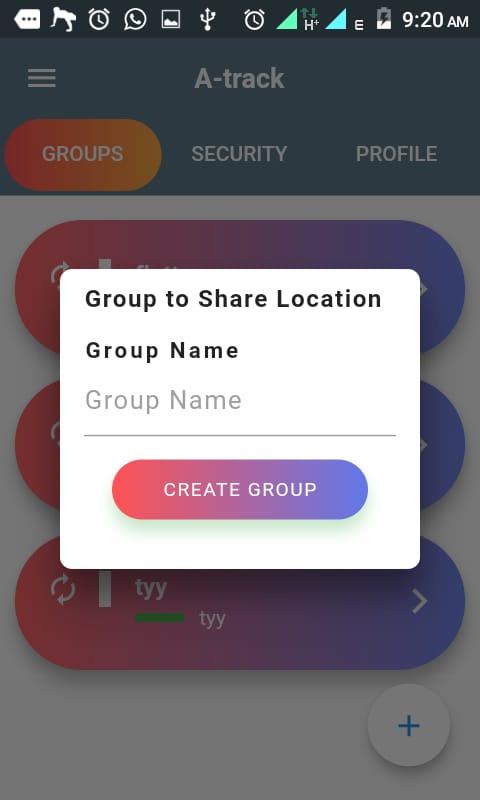
****

Once the user has successfully logged in, the main page appears as shown below

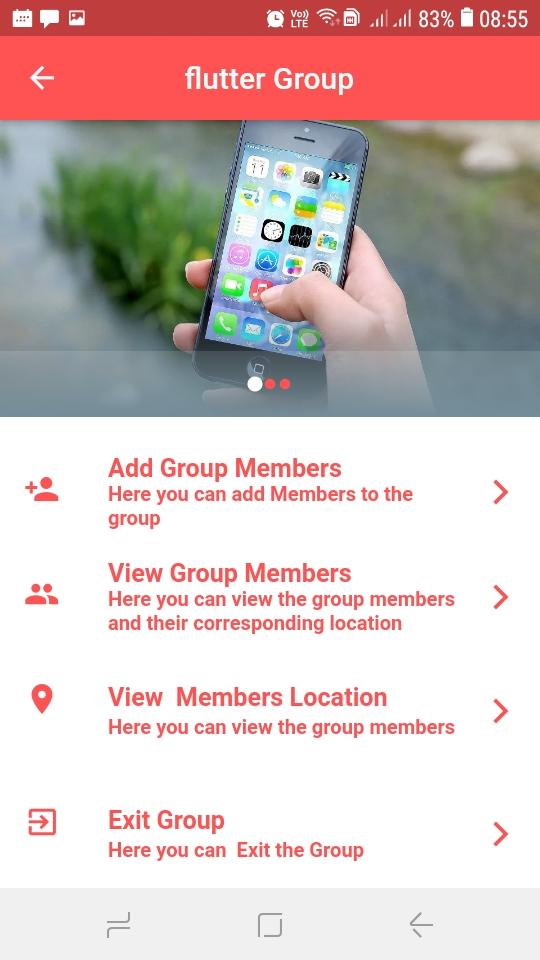


The Main page offers three major functionalities as shown

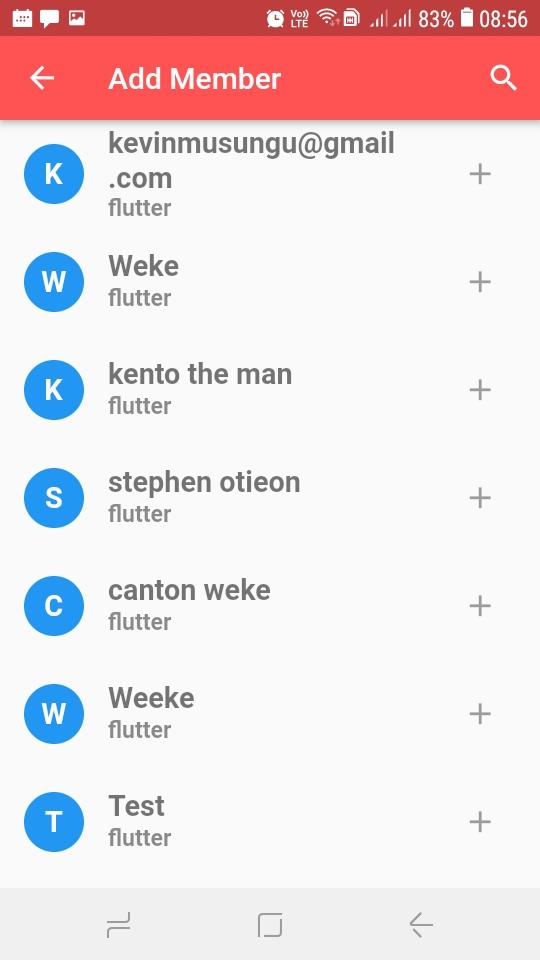
**Groups –** Herethe user can perform certain functions in reference to groups. This are

1. Create a new group for sharing location by clicking a (+) floating button at the bot.

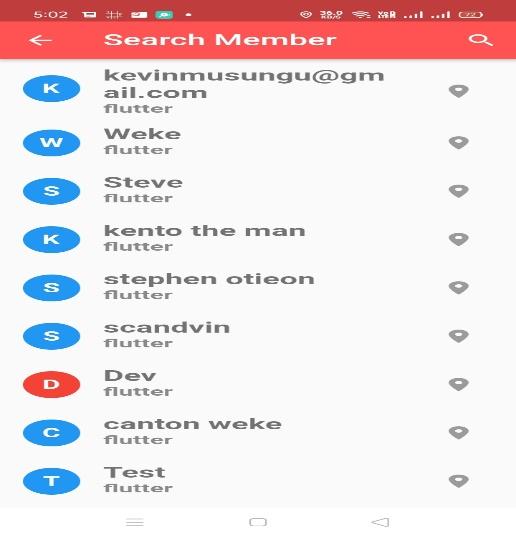
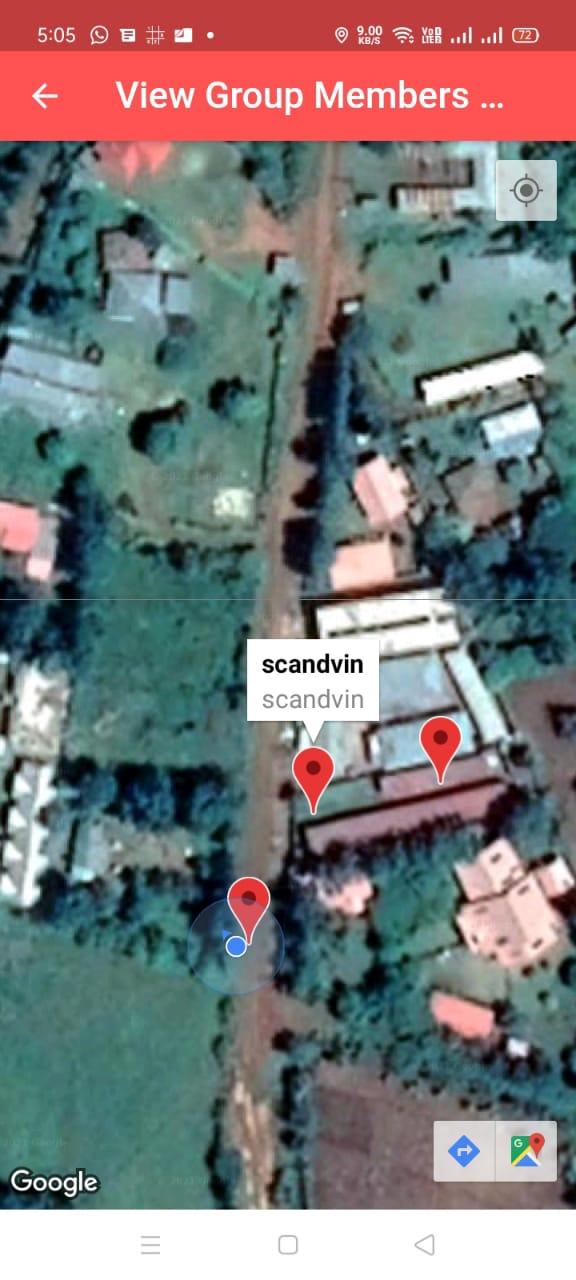
**Locations and exit a group.** Once the group has been created, on clicking on any listed group name, he or she can **Add registered** **members** to group **and view specific member location.**

****

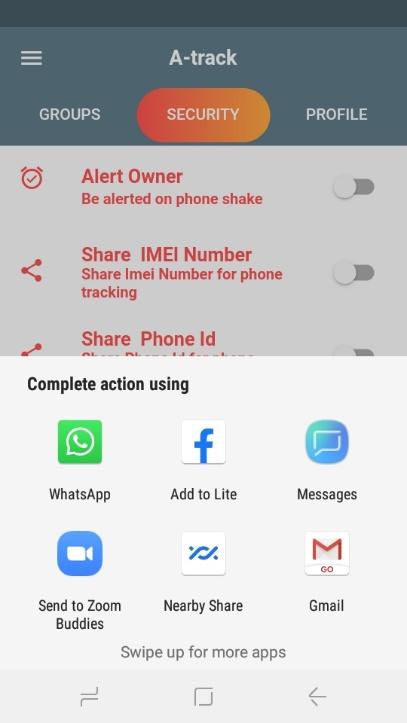
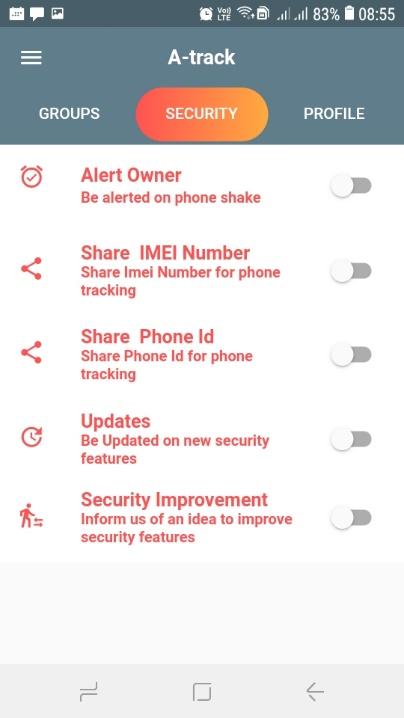
1. **Add members -** On clicking the Add members’ list tile, one can add members from a list of registered users to the specified groups; the users can even employ the search bar.



* You can view specific member location by clicking “**View Member Location”** Tile then click his or her name from the list, a map will appear that display his or her location

**Security –** Herethe user can perform certain functions in the security tab, the user can set the phone into a safe mode to be alerted on phone shake and receive the culprit photo. The user can share Phone ID and the IMEI Number for phone tracking and allow notifications for new security updates.

## **TIME SCHEDULE AND PROJECT COST**

## Schedule

The Gantt chart below shows the scheduled activities from concept paper drafting to the day the final system was implemented and documented. All this scheduled started from July and ended on November 2021.

|  | **July** | **August** | **September** | **October** | **November** |
| --- | --- | --- | --- | --- | --- |
| Project concept |  |  |  |  |  |
| Project proposal |  |  |  |  |  |
| Requirement analysis and design |  |  |  |  |  |
| Coding |  |  |  |  |  |
| System testing |  |  |  |  |  |
| Documentation |  |  |  |  |  |
| Total duration |  |  |  |  |  |

Gantt chart

Project Cost

The following table shows the estimated cost of the project during its implementation.

| ITEM | COST(KSHS) |
| --- | --- |
| Laptop | 30,000 |
| Internet services | 3,000. |
| Travel Expenses | 4,000 |
| Miscellaneous | 1,500 |
| Printing Services | 1,500 |
| **Total** | **40,000** |