Design and Implementation of Android Security App Against Mobile Theft Using GPS and SMS

Abdelmalik Yousif Abdallah
R-Soft Global Information Technology
Software Development Section
Riyadh, KSA
abdelmalik19930@gmail.com

Ibrahim Fadul Ibrahim
College of Ahfad for Women
Ahfad University
Omdurman, Sudan
ibrahimhassaboon@gmail.com

Yasir Abdelgadir Mohamed
Faculty of Computer Science & IT
Karary University
Omdurman, Sudan
yasir_eym@yahoo.com

Abstract—**Physical security is one of the biggest challenges to the designers of mobile phones and their applications. Mobile phones are lost or stolen. When a mobile device is lost or stolen, the real concern is not about the cost of the mobile but the amount of sensitive data that is present on that mobile. Imagine that the personal phone which is provided by your employer for enterprise activities falls into the hands of the wrong person then what could happen.**

In this research, an Android Smartphone-based application presented to safeguard against mobile phone theft security. The application design depends primarily on the android platform features like GPS (Global Positioning System) to get the current location of the mobile phone on theft, and SMS (Short Messaging Service) to make notifications and inform the user about his mobile phone location. Also, the application provides other features such as photo capture, contacts backup and data deletion.

Keywords—informationsecurity; confidentiality; integrity; availability.

1. INTRODUCTION

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Mobile security or mobile phone security has become increasingly important in mobile computing. Of particular concern is the security of personal and business information now stored on smartphones. More and more users and businesses employ smartphones as communication tools, but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks.

Physical security is one of the biggest challenges to the designers of mobile phones and their applications. The real concern is not about the cost of the mobile but the amount of sensitive data that is present on that mobile. In the past these devices were primarily used to call and send text messages. In addition, an address book. There is a new generation of mobile devices that come with Internet access, built-in video cameras and the ability to install additional software. These phones contain a lot of private data and, unfortunately, a phone can be lost easily.

The address book might be of special interest: it can be used just to gain knowledge of network or for further social engineering. As a minimum safety measure should always enable some kind of password protection on the phone, but this will never enable to get back data again, so this research is going to introduce a mechanism to enable us to get access and prevent mobile phones data from disclosure.

2. BACKGROUND

A. Android

Android is a mobile phone platform. It is produced by Google, Inc., and its first release was presented in 2007 [1]. Android is installed on many different mobile devices and its users can download Android apps and other content through Google Play service, which replaced old Android Market [2].

This thesis discusses technologies incorporated in Android application development and how they apply to the research problem. As the official Android website describes this platform, “Android is a software stack for mobile devices that includes operating system, middleware and key applications” [3]. Android provides “core set of applications including an email client, SMS program, calendar, maps, browser, contacts, and others” [3]. While additional applications can be downloaded through Google Play service [2].

Google claims that “Android powers millions of phones, tablets and other devices.” Phones and tablets are mobile devices that can have Android applications installed on them. These applications are written in Java programming language and they are called mobile device applications or apps [3]. Development techniques for apps are structured sets of Java code focused on implementing particular task that provides content for a mobile device application. Although Java programming language includes a broad variety of topics. This section will discuss about android background and literature review.

This section provides the information necessary for a reader to become familiar with an Android application environment in order to follow solutions given in the subsequent chapters. It outlines the steps needed to set up an environment, explains the fundamental concepts of Android application development.

“Android is a software stack for mobile devices that includes an operating system, middleware and key

applications. The Android SDK provides the tools and APIs necessary to begin developing applications on the Android platform using the Java programming language". Android features, an application framework, Dalvik virtual machine, integrated browser, optimized graphics, SQLite, Media support, GSM Telephony, Bluetooth, EDGE, 3G, Wi-Fi, Camera, GPS, compass, accelerometer, rich development environment. Bluetooth, EDGE, 3G, Wi-Fi, GSM Telephony, Camera, GPS, compass, and accelerometer are all hardware dependent. Below is a diagram showing the major components of the Android operating system [4].

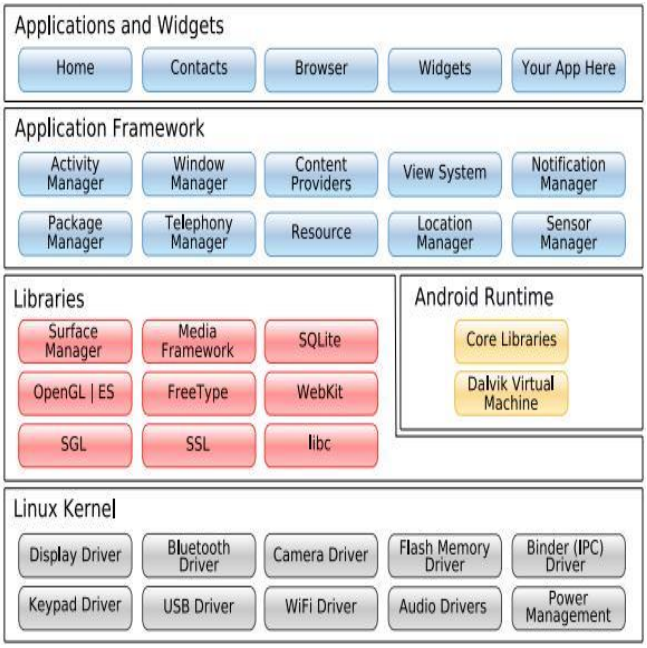

Figure (2.1): *Android OS Architecture.*

B. Activities

Activities are classes within packages that interact with the user [13]. These classes extend an "Activity" type and thus inherit methods and other related information needed for successful Android app implementation. Table (2.1) presents states that an activity can be in, depending on the user's interaction with it. Figure (2.2) describes the state paths an activity can take. According to the official Android Developers website, in this figure "square rectangles represent call back methods you can implement to perform operations when the Activity moves between states [13]. The colored ovals are major states the Activity can be in steps to initialize Activities are described below.

Table (2.1): *Activity States.*

State	Description
1	If an activity in the foreground of the screen (at the top of the stack), it is active or running.
2	If an activity has lost focus but is still visible (that is, a new non-full-sized or transparent activity has focus on top of your activity), it is paused. A paused activity is completely alive (it maintains all state and member information and remains attached to the window manager), but can be killed by the system in extreme low memory situations.
3	If an activity is completely obscured by another activity, it is stopped. It still retains all state and member information, however, it is no longer visible to the user so its window is hidden and it will often be killed by the system when memory is needed elsewhere.
4	If an activity is paused or stopped, the system can drop the activity from memory by either asking it to finish, or simply killing its process. When it is displayed again to the user, it must be completely restarted and restored to its previous state.

Activity Lifecycle

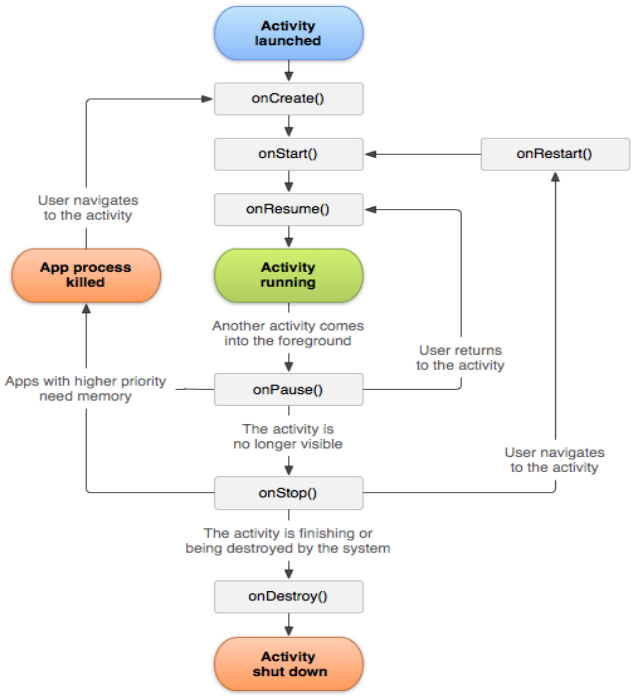

Figure (2.2): *Activity Lifecycle.*

C. Location Based Services in Android:

Android's Network Location Provider determines user location using cell tower and Wi-Fi signals, providing location information in a way that works indoor and outdoor, responds faster, and uses less battery power. The purpose of location-based services is to find the Physical location of the device. Access to the location-based services is handled by the LocationManager system Service. To access the Location Manager, request an instance of the LOCATION_SERVICE using the get System Service() method. Current Location can be fetched using two ways:

1. GPS (Global Positioning System).
2. Network Service Location.

❖ **GPS (Global Positioning System)**

The Global Positioning System (GPS) uses a constellation of 24 satellites orbiting the earth. GPS finds the user position by calculating differences in the times the signals, from

different satellites, take to reach the receiver. GPS signals are decoded, so the smart phone must have in-built GPS receiver.

To get access to GPS hardware of android we request using following statement LocationManager.GPS_PROVIDER.

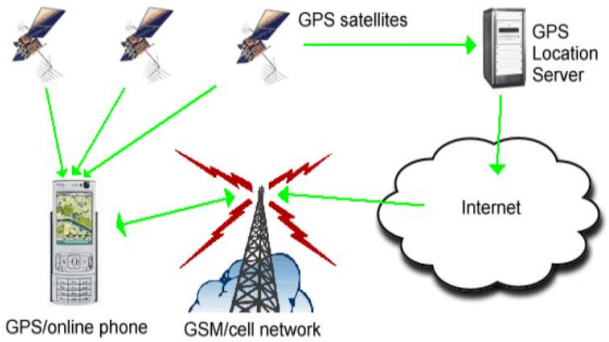

Figure (2.3): *Architecture of a GPS System.*

❖ **Network Service Location**

The current cell ID is used to locate the Base Transceiver Station (BTS) that the mobile phone is interacting with and the location of that BTS. It is the most basic and cheapest method for this purpose as it uses the location of the radio base station that the cell phone is connected to. A GSM cell may be anywhere from 2 to 20 kilometers in diameter. Other approaches used along with cell ID can achieve location granularity within 150 meters. The granularity of location information is poor due to Wide Cell Range. The advantage is that no additional cost is attached to the handset or to the network to enable this service.

To get access to Network Provider android we request using following statement:

LocationManager.NETWORK_PROVIDER.

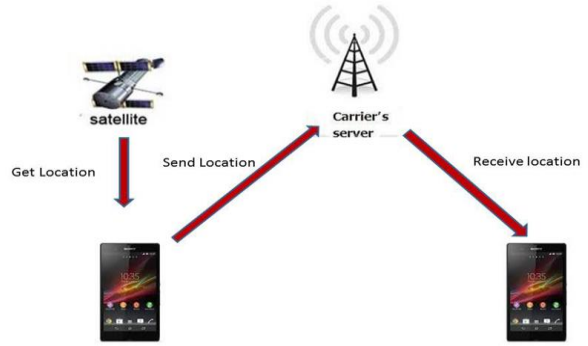

Figure (2.4): *Showing network services.*

D. Related Work

The paper [17] developed "anti-theft" mechanisms for android mobile phones against theft. The main mitigation against unauthorised data access on stolen devices is provided by "anti-theft" apps; that is, with "remote wipe" and "remote lock" functions. The methodology they used divide the app into two: android app and web application to enable users to sign in after theft occurred to trigger remote actions on their phones. Such as wipe data and remote unlock.

One anti-theft option for users to protect their data on stolen devices is to remotely lock the screen, generally through a web page provided by MAVs. In the following sections, we assume that the Android Debug Bridge (a db.) is disabled or protected in the device Settings (if not, then a thief can get an interactive shell and access user data as described in Section II-C). As users may have improperly configured their MAV, we study outcomes whether it runs as admin or not. The following sections present the many attack vectors we discovered during our study.

Researchers in [18] developed an application Vehicle Tracking System aims at determining the location of a vehicle using different methods like GPS and GSM systems operating through satellites and ground-based stations. Vehicle information like location details, speed, distance travelled etc. can be viewed on a Google map with the help of APIs via Internet.

This system is an important tool for tracking registered vehicles at any given period of time and is now becoming increasingly popular as a theft prevention and retrieval device. The vehicle tracking system installed within the vehicle sends an SMS containing the GPS coordinates to the user, using which he tracks the vehicle on Google Earth. The user can forward the SMS containing the GPS coordinates to his close friends and relatives if he wishes to, so that they can also track the vehicle using Google Earth.

Shweta and other in [19] aim to improve anti-theft for android based mobile phones by using different services like MMS instead of SMS. The scenario proposed in this project is totally dependent on the hardware of your smart phone like front camera, back camera and support for multimedia messages. Once the installation of this software is complete, it will work in the background.

The developed anti-theft app will enable user to use his android-based smartphone with freedom of getting stolen. It will enhance the security of the android-based smartphone.

Paper [20] developed a Personal Tracking Systems are the tracking devices specially built up for personal information. The person takes it with him and the information of where he is presently is provided. The same system has been implemented in this mobile tracking application i.e., Track Me App but various extended features that the existing system does not have. This system is GPS enabled android mobile phone whose location is tracked. Our application provides the functionality of defining the geo-fence areas as safe, risky and highly risky.

Jiang in [21] proposed a system for early diagnosis of hypertension and other chronic diseases. The proposed design consists of three main parts: a wrist Blood Pressure (BP) measurement unit, a server unit and a terminal unit. Blood Pressure is detected using data acquired by sensors intelligently using DSP microchip. The data is then transmitted to the remote server unit located at Community Healthcare Centers/Points (CHC/P) by using Short Messaging Service (SMS), and notification information is sent to the terminal unit to inform users if patient's BP is abnormal.

The researcher in [22] developed a system composed of server which interfaces several video surveillance cameras including several microphones for audio surveillance. This server captures video and audio streams from the video cameras and microphones and operates on these streams

according to the configuration of the local control software module. This module can store the video and audio streams on local hard-disks, index video and audio captures by time and place, retrieve images and sound based on user specified time intervals and deliver them to the user via Internet, or deliver (streaming) live images and sounds from a predefined camera. The system is connected to the building power supply and can be connected to the Internet via several communication solutions based on their availability. In case of power grid failure the system is provided with a secondary power supply based on rechargeable batteries which can keep the system functional for several hours. The main weaknesses of this system are the power supply and the Internet connection. To improve the reliability of this system, an autonomous diagnosis system has been added to the main monitoring server. The system will detect any change in the functioning state of the main system, like communication link failure, power grid failure or internal power source depletion and will report these events by sending a short message (SMS).

3. THE METHODOLOGY

The proposed methodology which should be followed in this research combine between the GPS (Global Positioning System) and SMS messages (Short message Service) android features in one App to protect against mobile theft security. Firstly, the user should register his data such as email address to send the thief picture as an attachment, and alternative phone number to notify the user if his SIM card changed and also send the thief location, and template messages which tell the app to take specific action like take thief image and location and send them to the registered email address and as SMS message, or delete user contacts, accounts and data after backing up the contacts to the registered email address.

A. Flowchart

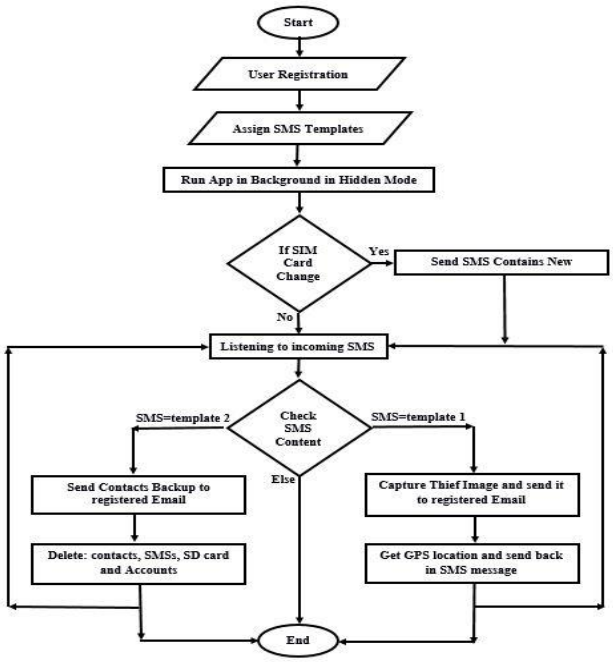

Figure (3.1): *Flowchart Diagram*

- **Step 1:** Start:

Initiate the application.

- **Step 2:** User Registration:

The application should be provided by initial details of the user to perform its functionality. User must enter the following at the registration phase:

1. Revocation number:
Used to launch the application by dialing this number. Because the application is running in background mode.

2. Valid E-mail address:
Used to upload thief photo and contacts backup.

3. Valid alternative phone number:
Used in case of SIM Card changed to inform the user about the new inserted number.

Notice: if the user does not provide a revocation number, the application will set (123456789) by default as a revocation number. But if the user does not provide an E-mail address and alternate number the application will never set anything as default values thus could not get neither E-mail nor SMS message notification.

- **Step 3:** Assign SMS Templates:

Two SMS messages templates should be assigned to trigger actions on the mobile phone remotely. As following:

1. Action of template 1:

- Capture thief photo and send it via email address.
- Send SMS message by the current location of the lost mobile phone.

2. Action of template 2:

- Send contact backup to the registered email address.
- Delete contacts.
- Delete SMS messages.
- Delete Accounts.
- Wipe SD Card data.

Notice: if the user does not provide templates to the application, then the application will never set default templates and user can not trigger any action on his phone after theft occurred.

- **Step 4:** Running the App:

After entering the details in step 2 and step 3, the application starts running in background mode, and has the ability to start himself at the mobile start-up.

- **Step 5:** SIM change Listener:

The application listening if the SIM card changed or not, if Yessss then:

- Send a notification SMS message to the alternative number by the new inserted number.

- Go to step 6.

If No then:

- Go to step 6.

- **Step 6:** Incoming SMS Listener:

Listening for incoming SMS messages and check each incoming message contents to take the appropriate action as mentioned above.

- **Step 7:** Check SMS contents:

If SMS message contents equals' value stored in Template 1, then go to step 8.

- **Step 8:** Template 1 action:

Trigger the front camera and take an image of the thief and send it to the registered E-mail address as an attachment, Also get the current GPS location By asking the GPS of the thief and send it back in SMS message and Go to step 6.

- **Step 9:** If SMS message contents equals value stored in Template 2, then go to step 10.

- **Step 10:** Template 2 action:

Backup contacts and send them to the registered E-mail address as an attachment, then delete all contacts, MS messages, accounts and SD card data, and Go to step 6.

- **Step 11:** End.

B. Sequence Diagram

A Sequence diagram shows how a set of objects communicate with each other to perform a task. This type of diagram allows the other developer to verify that the interaction is correct.

A Sequence diagram shows, as parallel vertical lines (lifelines), different processes or objects that live simultaneously, and as horizontal arrows, the messages exchanged between them, in the order in which they occur. This allows the specification of simple runtime scenarios in a graphical manner.

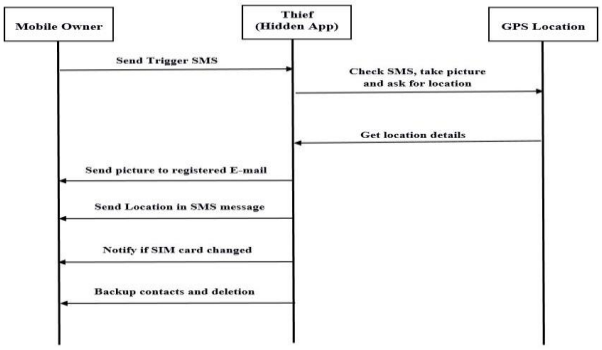

Figure (3.2): *Sequence Diagram.*

4. DESIGN AND IMPLEMENTATION

A. User Interface Design

In order for the application to satisfy the requirements and maximize the usability, much emphasis of the design is put on the user interface. Below is the detailed explanation of the application design interfaces.

Figure (4.1) shows the main screen of the application which used for app setting such as entering user email, alternative number, revocation number and assign SMS messages templates and select appropriate options to be triggered.

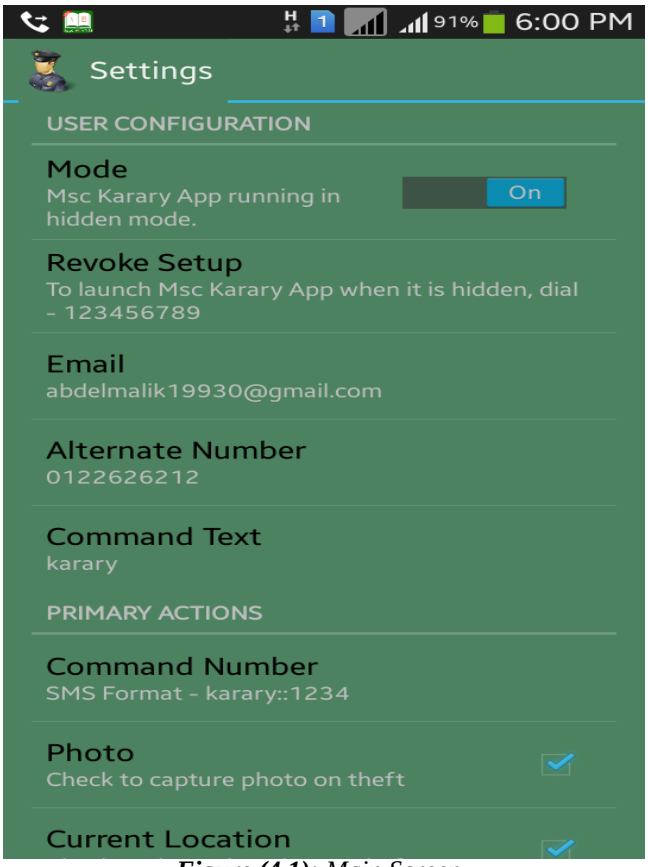

Figure (4.1): *Main Screen.*

Figure (4.2) shows the switch button is (On) which means the application is activated and running in background in a hidden mode.

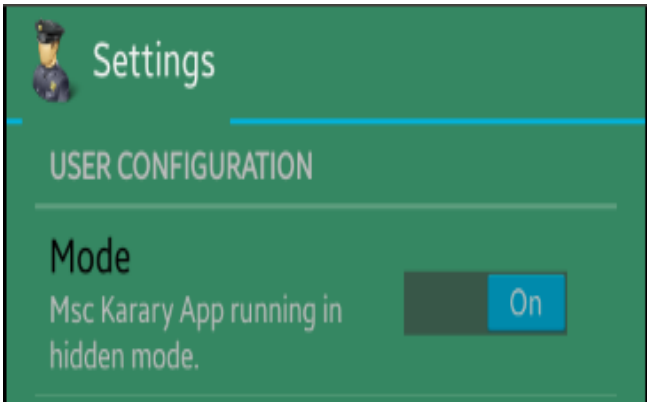

Figure (4.2): *Activation Mode.*

Figure (4.3) shows an input text to receive Revocation Number used to launch the application when it is hidden by dealing this number. Thus prevent the thief from uninstalling the application.

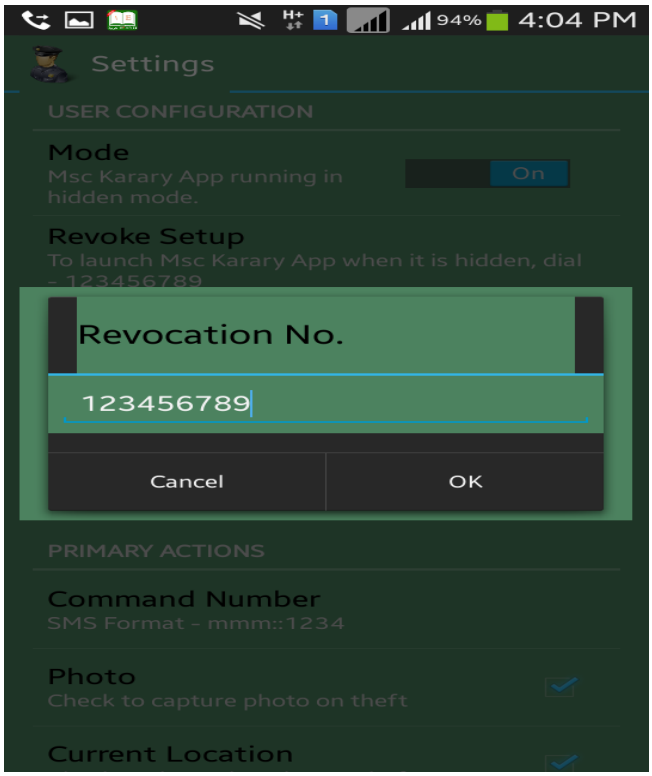

Figure (4.3): *Revocation Number.*

Figure (4.4) shows an input text to receive Email address used to send thief image and contacts backup as attachments.

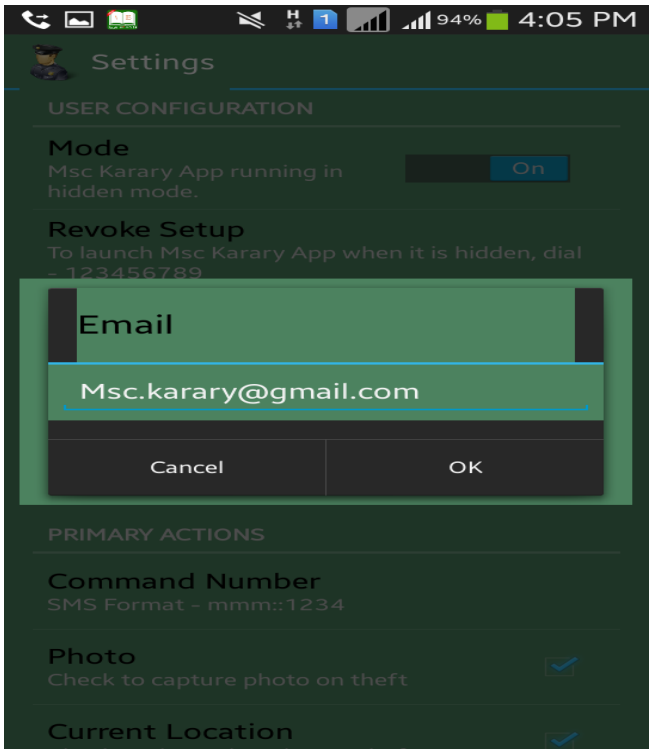

Figure (4.4): *E-mail Address.*

Figure (4.5) shows an input text to receive an alternate Number used to send SMS message containing the GPS location, mobile serial No and SIM card service provider in case of SIM card changed.

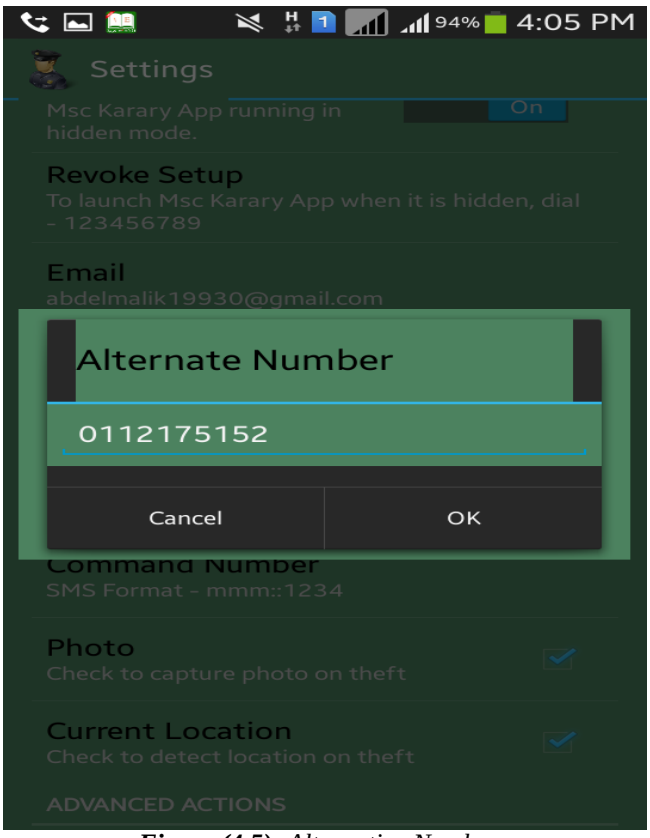

Figure (4.5): *Alternative Number.*

Figure (4.6) shows the SMS message template 1 with SMS format (karary::1234). When receiving this template, the application will capture a photo and get the current location and send them using the registered E-mail address and SMS message.

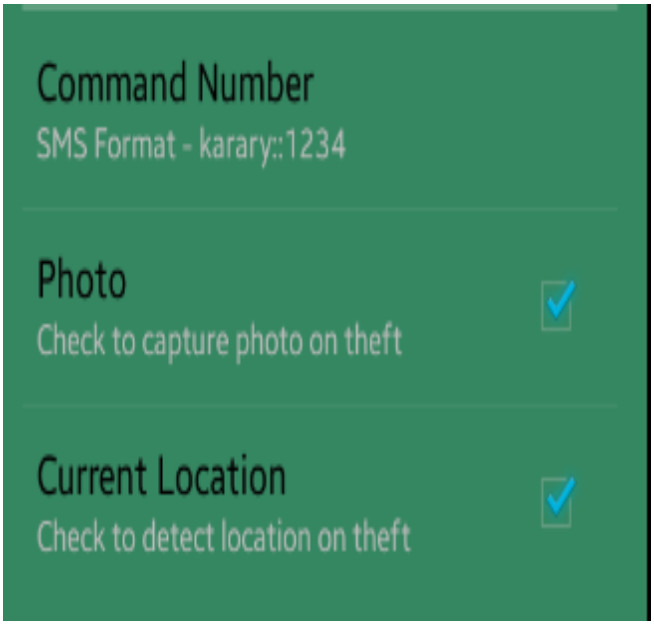

Figure (4.6): *SMS Template 1.*

Figure (4.7) shows the SMS message template 2 with SMS format (karary::4321). When receiving this template, the application will send contacts backup to the registered E-mail address as an attachment and then delete all: contacts, MS messages, SD Card data and accounts.

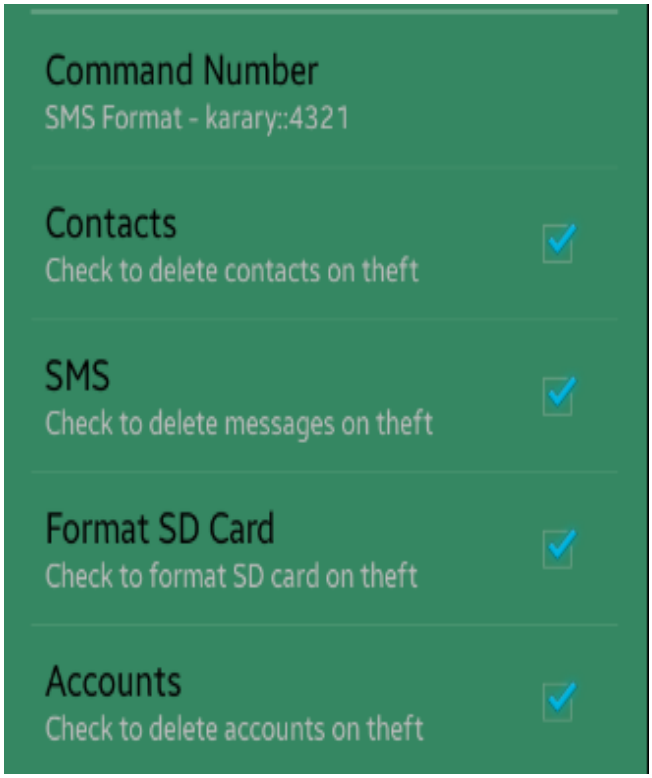

Figure (4.7): *SMS Template 2.*

B. Results

- If the application received SMS message its contents equal to the stored template (1), the application will do the following:
  i. Send back SMS contains the current GPS location, Mobile serial no and SIM Card service provider.
  ii. Capture image and attach it to the registered Email address.
- If the application received SMS message its contents equal to the stored template (2), the application will do the following:
  i. Send contacts backup to the registered E-mail address.
  ii. Delete all: contacts, MS messages, SD Card data and accounts.
- If the SIM Card changed the application automatically Send SMS message to the registered (alternative number) contains the current GPS location, Mobile serial no and SIM Card service provider.

Figure (4.8) show SMS message contains the current GPS location, Mobile serial no and SIM Card service provider. When template (1) triggered or SIM Card changed.

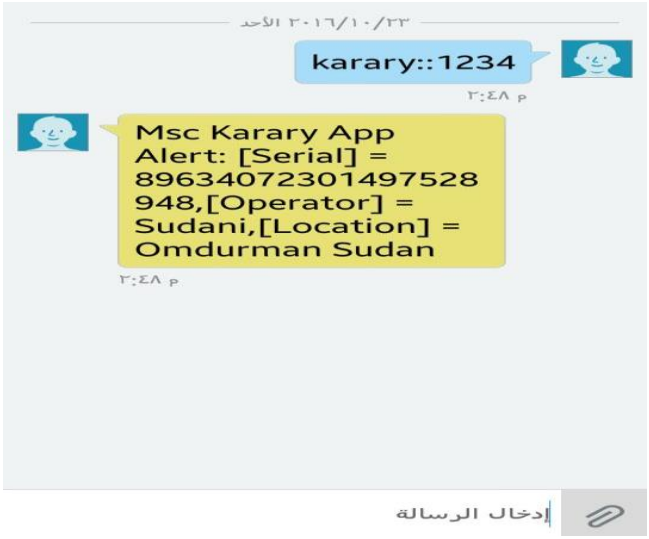

Figure (4.8): *SMS Alert by the App.*

Figure (4.9) shows E-mail message contains the captured photo as an attachment. When template (1) triggered.

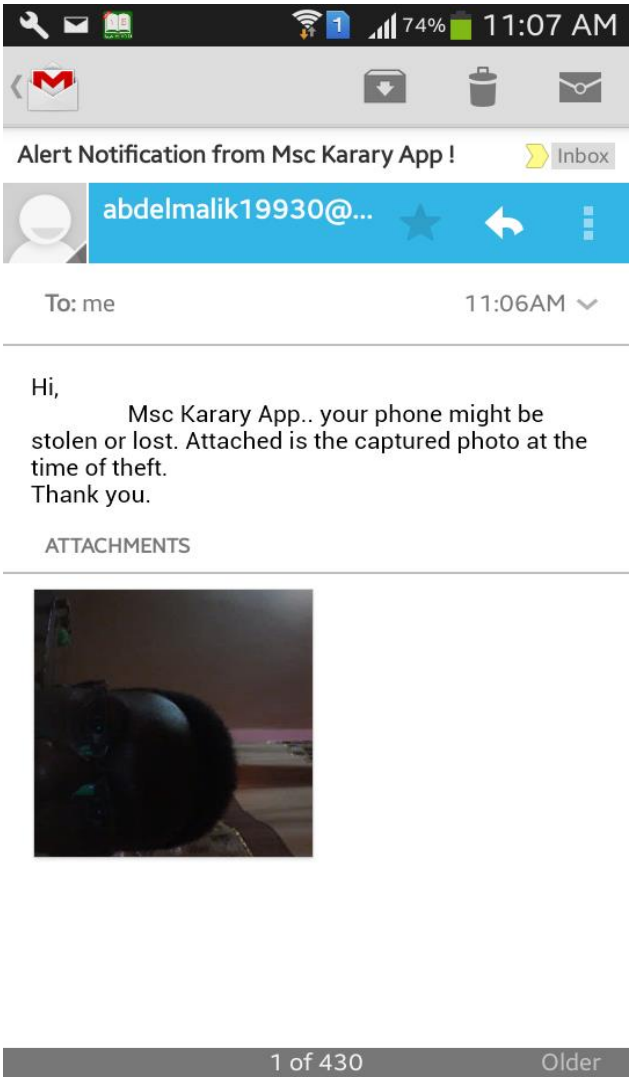

Figure (4.9): *E-mail notification with Picture attachment.*

Figure (4.10) show E-mail message contains the contacts backup as an attachment. When template (2) triggered.

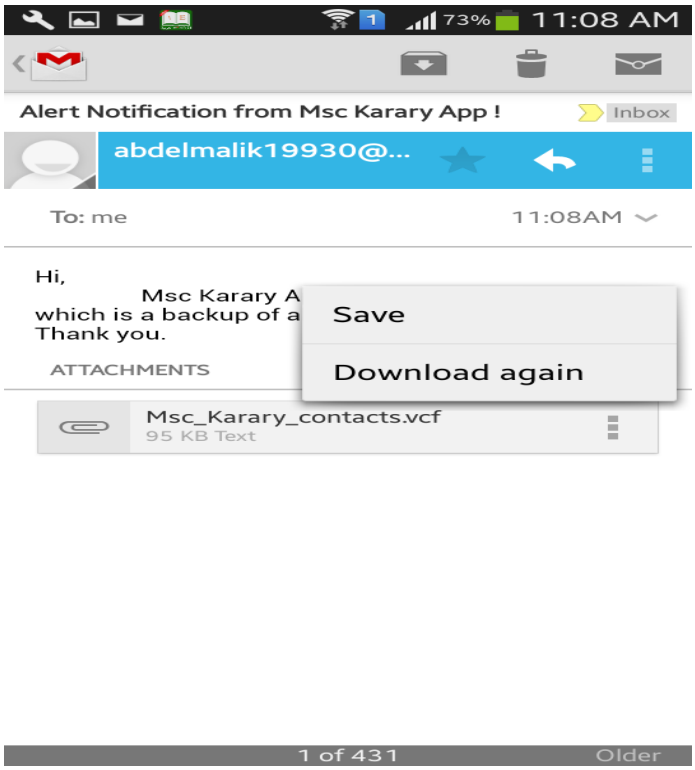

Figure (4.10): *E-mail notification with Contacts backup attachment.*

5. Conclusion

A safe (community) means that all people, regardless of gender, race, ethnicity, language, disability, age or sexual orientation, have an equal right to freedom from fear and violence. We as a community have a responsibility to address the issue of violence because it belongs to everyone.

All this application features work on GPS and SMS basis. The developed android application running in background and listening to all the incoming messages. If the SMS is meant for the application, it reads the same and performs the expected task.

This research enhanced the security of the android mobile phone tracking on theft and trigger actions remotely. This Application stands different from other systems as its not only get benefit from the GPS value but it works on text messaging services which makes application a simple and unique one.

A. Related Features

- Using GPS (Global Positioning system) to obtain the current location of the android mobile device.
- Using SMS (Short Messaging Service) to send notification message to inform the user by the mobile phone location.
- Application running in background mode.
- Using mobile hardware like camera.

B. Recommendation

Recommendations can be summarized as follows:

- Finding more convincing and unique solutions to the padding.
- Improve the rate of authentication transaction, by reducing the process time to the minimum as well as possible.
- Find appropriate ways to take advantage of the features of the Android system, (GPS, encryption, etc.), within the application to raise its efficiency to the maximum.

C. Limitations:

- If the mobile does not connected to the internet, the application could not sent neither an email notification nor current location.
- If the phone operating system software (Android) has been changed, user cannot trigger any actions on his mobile phone.

References:

[1] Whitman, M.E. and Mattord, H.J., 2011. *Principles of information security*. Cengage Learning.

[2] Friesen, J.J., 2010. Getting Started with Java. Learn Java for Android Development, pp.1-41.

[3] *Android System Development* 2004-2017, accessed 03 March 2017, <http://www. free-electrons.com/doc/training/android>.

[4] Al-Sinani, H.S. and Mitchell, C.J., 2011, June. Enhancing CardSpace Authentication Using a Mobile Device. In *DBSec* (pp. 201-216).

[5] Mustafa, A.F. and Ja'afer, A.S., 2011. An enhancement of authentication protocol and key agreement (AKA) for 3G mobile networks. *International Journal of Security (IJS)*, *5*(1), pp.35-51.

[6] Vishal, G., Ravishanker and and Ashish, Kr.L, 2016. Mobile Based Secure Authentication Using TLS and Offline OTP. *International Journal of Computer Technology and (IJCTA)*, *9*(11), pp. 5253-5262.

[7] Vishal, G., Ravishanker and and Ashish, Kr.L, 2016. Mobile Based Secure Authentication Using TLS and Offline OTP. *International Journal of Computer Technology and (IJCTA)*, *9*(11), pp. 5253-5262.

[8] Vishal, G., Ravishanker and and Ashish, Kr.L, 2016. Mobile Based Secure Authentication Using TLS and Offline OTP. *International Journal of Computer Technology and (IJCTA)*, *9*(11), pp. 5253-5262.

[9] Vishal, G., Ravishanker and and Ashish, Kr.L, 2016. Mobile Based Secure Authentication Using TLS and Offline OTP. *International Journal of Computer Technology and (IJCTA)*, *9*(11), pp. 5253-5262.