Find Intruder Application for Smartphone

Dr. N. Usha Rani[1]

C.Srinivasulu[2], M.GowthamKumar[3], G. Reethu Royal[4]

[1]Assistant Professor, Department of CSE, S V U College of Engineering, Tirupati, AP, India.

[2, 3, 4] BTech Student, Department of CSE, S V U College of Engineering, Tirupati, AP,India.

Abstract: Smartphones usage has increased a lot with the advancement in technology coupled with an increase in their computing power. Smart phones are used by many people to store personal data such as images, files, contacts, videos and official data like confidential documents. They are also used to maintain accounts like Gmail, Facebook, Twitteretc. So the security of smart phones is very important in order to restrict unauthorized access. This application mainly helps to enhance the security of smartphones. It provides real time acknowledgement to the user by sending an SMS and email to the registered mobile number and email id, when someone tries to unlock the mobile. It also provides the image of the person trying to access the mobile along with the location details.

Keywords: *Android Operating System, Device Administration API, Find Intruder Application.*

*****

I. INTRODUCTION

The mobile phone is one of the quickest to be adopted technologies in human history. There has been a rapid shift in how mobile phones are perceived: from simple communication devices to general purpose mobile computers. Smartphones are used by people to store data, maintain accounts, mobile banking etc. hence their security is of major concern. Smartphone users want to know who are trying to access their mobile in their absence. They also want to know the location of the mobile when someone steals the mobile. This Find Intruder application (app) provides those features for the users. When the intruder tries to unlock the mobile, this application sends an SMS to the registered mobile number with the location details and also sends an email to the registered email id with the location details and captured image of the intruder.

II. SOME RELATED APPLICATIONS

Smartphones provide flexibility for the users to store data and access accounts. So securing those data from intruders is crucial now a days. So an application is needed to provide security. Applications can be easily downloaded and run in smartphones. Some of the smartphone applications that deals with the security of smartphones are given below.

A.Anti-Theft Mobile Tracker:

This application provides the security feature which sends the lost or stolen mobile location information to recipient mobile phone. It gives user the power of controlling their data and location information in case of any theft. It also provides the remote locking of the mobile [1].

B. Leo Privacy Guard:

It provides lock feature for apps installed in the mobile. When anyone tries to open the application with wrong pattern or pin it captures the image of the person and saves it in the application's internal storage [2].

C. Anti-Theft and Find My Phone:

This is a security application that tracks the location of the mobile and by just sending a text your phone will be automatically locked. In case of no recovery, all the data on SD card will get erased and the contacts will be send to mail [3].

D. Comodo Anti-Theft:

This application controls all your lost devices through a single web interface. It also allows the user to remotely send commands like locate,lock,erase the data and also gets the image of the person [4].

E.Anti-Theft GPS:

It is useful to retrieve the mobile. The main features are tracking the location, remotecontrol, owner can also monitor any SIM card changes and a ringing alarm [5].

F. An Intelligent Anti-Theft Android Application:

This application overcomes the issue of sending the unwanted notification for the SIM card changes made by the real owner of the android phone by providing the safe and alert modes. It is embedded with features to remotely wipe the content of the memory card, detect the SIM card changes, track the location of the phone and change the target phone to send the notification messages at any point of time. This application uses GPS or global system for

mobile (GSM) network to track a mobile device [6].

III. ANDROID OPERATING SYSTEM

Android is an open source operating system for mobile devices. Android was initially developed by Android Inc., and sold to Google in 2005. On November 2007, the Open Handset Alliance (OHA) was announced amongst a consortium of several top companies. The goal was to develop an open mobile platform every developer to contribute towards improving the performance and features of the product. Android is built on top of Linux kernel and GNU software. Software stack of the Android runs Java applications using Java core libraries [7]. Each instance of Java application runs on its own Virtual Machine (VM) called Dalvik. Well as for Dalvik VM, it has its own Java Byte code and is designed to be to be optimal on memory and processor usage [8]. The VM executes Dalvik Executable with (.dex) extension. Among the various tools built in the Android, 'dx' tool is used to generate the executable that converts the Java classes into .dex format. Android relies on the Linux kernel to perform system level functions such as memory management and threading and even the more dependent on it for hardware interactions and power management [9].

Developers can build applications using the Software Development Kit (SDK) developed by Google. It consists of Application Programming Interface (API) used to develop robust Java applications. These API's facilitate to access the contents on the phone such as contacts and calendar information and also integrate them with external web service in order to provide online services.

Application components are the essential building blocks of an Android application. These components are loosely coupled by the application manifest file AndroidManifest.xml that describes each component of the application and how they interact. Every application must have an AndroidManifest.xml file (with precisely that name) in its root directory. The four main components that can be used within an Android application are [10]:

1. **Activities:** They dictate the UI and handle the user interaction to the smart phone screen.
2. **Services:** They handle background processing associated with an application.
3. **Broadcast Receivers:** They handle communication between Android OS and applications.
4. **Content Providers:** They handle data and database management issues.

IV. DEVELOPMENT OF ANDROID APPLICATION

Step 1: Set-up Java Development Kit (JDK)

One can download the latest version of Java JDK from Oracle's Java site – http://www.oracle.com/technetwork/java/javase/downloads/index.html. Instructions for installing JDK will be found in downloaded files, follow the given instructions to install and configure the setup. Finally set PATH and JAVA_HOME environment variables to refer to the directory that contains java and javac, typically java_install_dir/bin and java_install_dir respectively [12].

Step 2: Downloading Android Studio

Android Studio is the official IDE for android application development. It works based on **IntelliJ IDEA**. It provides the fastest tools for building apps on every type of Android device. World-class code editing, debugging, performance tooling, a flexible build system, and an instant build/deploy system all allow you to focus on building unique and high quality apps. Download the latest version of android studio from https://developer.android.com/studio/index.html

Step 3: Installing Android Studio

Once the file is downloaded on windows machine launch Android Studio.exe. Once Android Studio is launched, it's time to mention JDK path in android studio installer. Then need to check the components, which are required to create applications and specify the location of local machine path for Android studio and Android SDK.Need to specify the ram space for Android emulator by default it would take 512MB of local machine RAM. At final stage, it would extract SDK packages into the local machine.

Step 4: Creating new Android Studio Project

Start application development by calling start a new android studio project. In a new installation frame should ask Application name, package information and location of the project. After entered application name, it going to be called select the form factors that the application runs on, here need to specify Minimum SDK.The next level of installation should contain selecting the activity to mobile, it specifies the default layout for Applications.At the final stage it going to be open development tool to write the application code.

Step 5: Create Android Virtual Device

To test Android applications, a virtual Android device is needed. So before start of writing the code, create an Android virtual device. Launch Android AVD Manager Clicking AVD_Manager icon.After Click on a virtual device icon, it going to be shown by default virtual devices which

are present on your SDK, or else need to create a virtual device by clicking Create new Virtual device button [13].

V. FIND INTRUDER APPLICATION

Android operating system provides lock screen features such as pattern, password, pin etc. in order to provide security to the mobile [11]. This application works on this screen lock feature to enhance the security. Basically an intruder tries to unlock the mobile with maximum possible attempts so this application listens for all those wrong attempts and keep counting them. When the count reaches five the application captures the image of the intruder with the front facing camera and tracks the location details of the mobile and send them to the registered user details. Thus the user can know who is trying to unlock the mobile in his absence. Another usage of this application is that when the mobile is lost or someone has stolen the mobile and when he tries to unlock the mobile the user can get the image and location details so that these details may help him to findthe mobile. Thus it not only enhances the security of the mobile but also helps to get back the mobile.

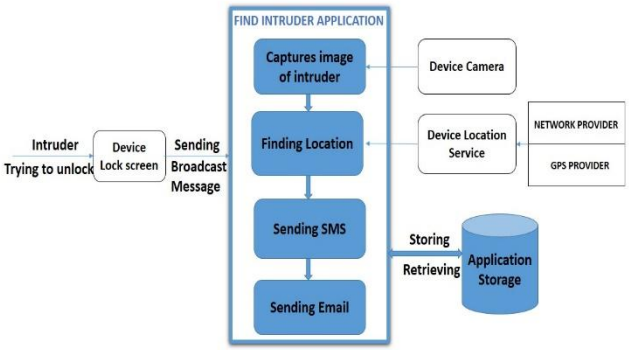

Fig.1. Block diagram of Find Intruder Application

TheBlock diagramof Find Intruder application is shown in Fig.1. Device Lock screen is linked with the application using Android Device Administration API and hence any action performed on the lock screen such as drawing wrong pattern, entering wrong pin or password,will send a broadcast message to the application by android operating system. On receiving broadcast message the application performs different set of tasks. Device Camera, captures image of the intruder for the application. Device Location Service, finds the location details of the mobile either by using Network Provider or GPS Provider based on availability. Then the application retrieves the registered mobile number from Application storage and sends an acknowledgement with the location details to the user as an SMS as shown in Fig.2.It then retrieves registered email id from Application storage and uses JavaMail API in order to send an email to the user along with the location details and also the captured image of the intruder as shown in Fig.3. So the user can login to his email account and can find who is trying to unlock his mobile or who has stolen his mobile.

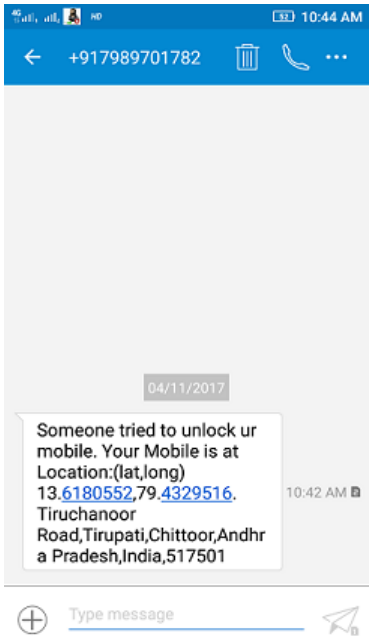

Fig.2. SMS sent by the application

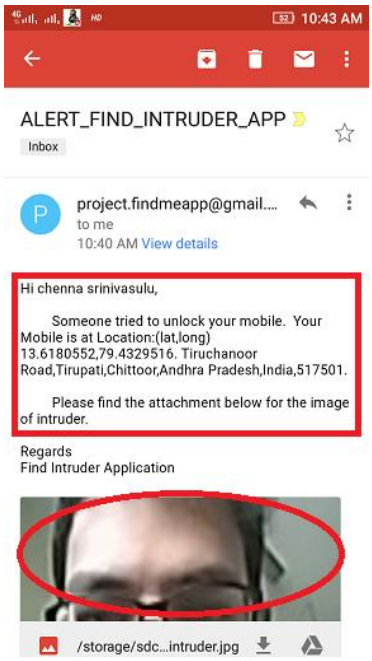

Fig.3.Email sent by the application

DEVICE ADMINISTRATION API

Android 2.2 introduces support for enterprise applications by offering the Android Device Administration API. The Device Administration API provides device administration features at the system level. These APIs allow you to create security-aware applications that are useful in enterprise settings, in which IT professionals

 ISSN: 2321-8169
297– 301

require rich control over employee devices. Such as accessing the device password, disabling the device camera, limiting the size of the password, setting the maximum failed attempt for the password, erasing all the data of the device etc. [14].

It isbasicallyimplemented with the use of three classes namely DeviceAdminReceiver, DevicePolicyManager, DeviceAdminInfo.

DeviceAdminReceiver: Create a Device Administration broadcast receiver, which gets notified of events related to the policies that have declared to support. An application can selectively override callback methods.

DevicePolicyManager: This class basically is used for managing the policies which are enforced on the device.

DeviceAdminInfo: The DeviceAdminInfo class is basically for providing the Meta data information of a device admin component.

Once the application is installed in the smartphone, it first asks the user to activate Device Administrator permissions for the application as shown in the Fig.4. After activation it the asks the user to register with the application by giving name, phone number, email id in the registration page as shown in Fig.5. After successful registration it then moves to the home page where user registered details are displayed as shown in Fig.6.

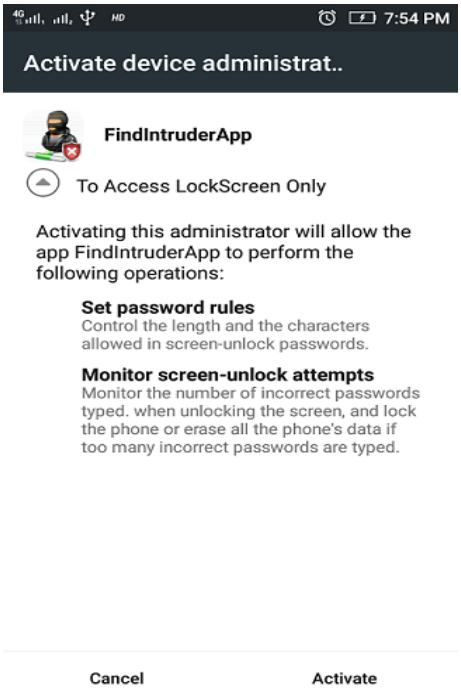

Fig.4. Activating Device Administrator permissions for application

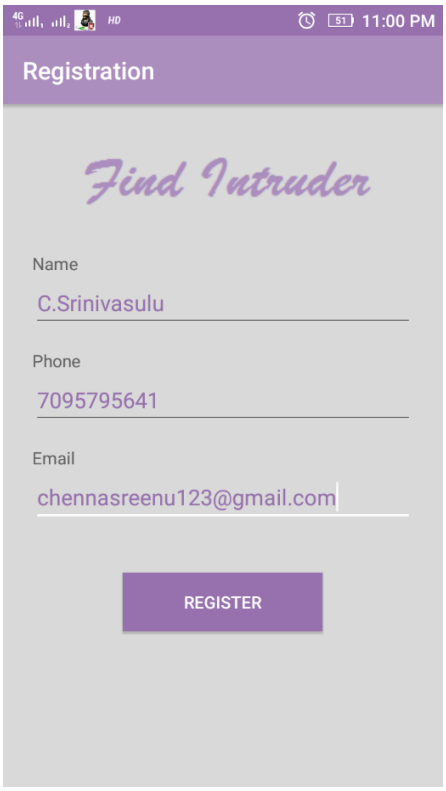

Fig.5. User Registering with the application

Fig.6. Displaying registered user details

VI. CONCLUSION

As technology is rapidly evolving, the smartphone has become the basic need of a common man. It provides flexibility to store and access various types of data at any time and place. So, maintaining security without allowing others to access theinformation is becoming a crucial thing. This application provides an efficient way to find the intruders who try to unlock phones to access the information. It enhances the security features provided by android operating system. It gives real time acknowledgment to the user. The captured image and the location which is traced helps the user to find the intruder very easily. By sending email as well as SMS, the user can access the information in either way faster.

REFERENCES

[1] https://play.google.com/store/apps/details?id=com.sim.location&hl=en
[2] http://leo-privacy-guard.en.uptodown.com/android
[3] https://play.google.com/store/apps/details?id=com.phonefindandlock&hl=en
[4] https://antitheft.comodo.com/
[5] https://play.google.com/store/apps/details?id=org.main&hl=en
[6] D. Abirami, S. Anantha Surya, S. Annapoorani, Ms. M. PadmaPriya, “AN INTELLIGENT ANTI-THEFT ANDROID APPLICATION”, International Journal of Innovative Research in Technology, ISSN: 2349-6002, Volume: 1, Issue: 10, pg:142-145, 2014.
[7] L. Ashwin Kumar, “MOBILE APPLICATION FOR NEWS AND INTERACTIVE SERVICES”,ARPN Journal of Science and Technology, VOL. 2, NO. 1, January 2012 ISSN 2225-7217.
[8] Ms.N.Usha Rani andMs.Y.Ramyakrishna “OVERVIEW OF ANDROID FOR USER APPLICATIONS”. International Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 9 October 2014.
[9] PriyaChandnani and Prof. Rajesh Wadhvani, “EVOLUTION OF ANDROID AND ITS IMPACT ON MOBILE APPLICATION DEVELOPMENT”, International Journal of Scientific Engineering and Technology, ISSN 2277-1581,Vol No.1, Issue No.3, pg:80-85 01 July 2012.
[10] SuhasHolla andMahima M Katti, “ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY”, International Journal of Science Technology & Engineering, ISSN: 2231-2803, Volume: 3, Issue: 3, pg: 486-490, 2012.
[11] Ms.R.Srilekha andMr.D.Jayakumar “A SECURE SCREEN LOCK SYSTEM FOR ANDROID SMART PHONES USING ACCELEROMETER SENSOR”. International Journal of Science Technology & Engineering Volume: 1 Issue: 10, April 2015.
[12] Ms.N.Usha Rani andMs.Y.Ramyakrishna “SMARTPHONE APPLICATION FOR HEALTH CARE”. International Journal of Scientific Engineering and Technology Research Volume: 4 Issue: 9 April 2015.
[13] https://www.tutorialspoint.com/android/android_studio.htm
[14] https://developer.android.com/guide/topics/admin/device-admin.html