



OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

ANTI-THEFT MOBILE TRACKING APPLICATION

Abhinav Srivastava¹, Manasi Thakkar², Rahul Verma³, Uday Rote⁴

Student, Department of Information Technology, KJ Somaiya Institute of Engineering & IT, Sion, Mumbai-400022, India^{1,2,3}

Professor, Department of Information Technology, KJ Somaiya Institute of Engineering & IT, Sion, Mumbai-400022, India⁴

abhinav.js@somaiya.edu¹, manasi.t@somaiya.edu², rahul.iv@somaiya.edu³, udayrote@somaiya.edu⁴

Abstract: Mobile phones have brought a new revolution in today’s world and majority of people might have experienced misplacing or losing their mobile phones. Hence, it has become compelling to develop an android application to protect the smart phones. This paper describes the application, which is embedded with lot of features such as location tracking, capturing images and videos and sending messages along with automatic data backing up of data. The application starts running in background as soon as the SIM card is changed. It will track the location of the stolen phone and send it to alternate mobile number and registered email address. As the phone moves from one place to another the value of latitude and longitude will be sent to email address and registered mobile number. The application will also capture images and videos using the front and rear camera without alarming the thief. Also as soon as the SIM is changed by the thief, automatic user’s data backup will start on the server so that there is no data loss and user can access his/her confidential data. This proposed application runs in the background using “service” thus providing safety and distinguishing it from other existing mobile tracking applications.

Keywords: - Smartphones, SIM, Google Maps, GPS, GCM, Data Backup.

I INTRODUCTION

Smart phones have become a major part in today’s world. Smartphones are like computers capable of storing information, documents, video-conferencing, email, sharing files over internet, etc. Due to its small size, it can be stolen easily and data inside it can be easily hampered.

This paper puts forward a technique through which thief can be identified easily. This application include use of technologies like Google Maps and Mail services using which you can send images to registered number and Email address. When the SIM (Subscribers Identity Module) card is changed, the application starts running in the background, fetches the location and send it via SMS. There are many problems faced by android users. One of the biggest problem is that the mobile gets stolen easily and hence security of the confidential and personal data is hampered.

According to a survey, we came to know that the number of android users are more as compared to others. For 2016, the number of smartphone users is forecast to reach 2.1 billion. The number of mobile phone users in the world is expected to pass the five billion mark by 2019[6], so it is

necessary to protect android smart phones from being stolen. Since 2013, 9053156308 mobile theft cases were registered. Out of these stolen mobiles only 4% of phones had advanced security to prevent mobile theft. As 4% is a very small percent of recovered phones there is a need of security application [8]. If the phone is lost the user has to manually report to the customer care to track the location of the smartphone and find the thief.

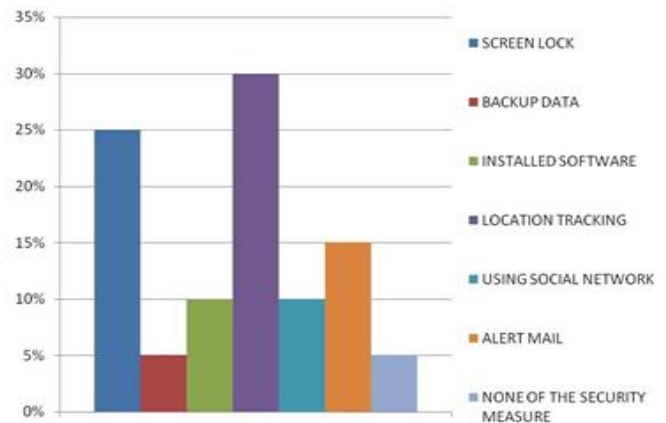


Figure 1:- Percentage of users securing their smart phones

Services and Activities

A service is an application component that can perform long running operations in background and does provide user interface. Another application component can start a service, and it continues to run in the background even if the user switches to another application. Additionally, a component can bind to a service to interact with it and even perform inter process communication (IPC). For example, a service can handle network transactions, play music, perform file I/O, or interact with a content provider, all from the background. There are three different types of services:-

- Foreground: A foreground service performs some operation that users can notice. Foreground services must display a notification.
- Background: A background service performs an operation that isn't directly noticed by the user.
- Bound: A service is *bound* when an application component binds to it by calling `bindService()`. A bound service offers a client-server interface that allows components to interact with the service, send requests, receive results, and even do so across processes with inter process communication (IPC).

To create a service, you must create a subclass of `Service` or use one of its existing subclasses. These are the most important callback methods that you should override:

- `onStart ()`: The system invokes this method by calling `startService ()` when another component (such as an activity) requests that the service be started. When this method executes, the service is started and can run in the background indefinitely. If you implement this, it is your responsibility to stop the service when its work is complete by calling `stopSelf ()` or `stopService ()`.
- `onBind ()`: The system invokes this method by calling `bindService ()` when another component wants to bind with the service.
- `onCreate ()`: The system invokes this method to perform one-time setup procedures when the service is initially created.
- `onDestroy ()`: The system invokes this method when the service is no longer used and is being destroyed. Your service should implement this to clean up any resources such as threads, registered listeners, or receivers.[9]

Declaring services in manifest:-

```
<manifest ...>
...
<application ...>
    <service android: name="".ExampleService"/>
    ...
</application>
```

</manifest>

An Activity represents a single screen with a user interface just like window or frame of java. Android activity is subclass of `ContextThemeWrapper` class. Android system initiates its program within an activity starting with a call on `onCreate ()` callback method. There is a sequence of callback methods that start up an activity and a sequence of callback methods that tear down an activity. Activities are fundamental building blocks on android applications. When one application invokes another, the calling application invokes an activity in other application, rather than application as an atomic level. Most application contains multiple screens that is they contain multiple activities. The first screen to appear when the application is launched by the user is the Main Activity. Each activity can then start another activity to perform different actions. [10]

Declaring activities: - To declare an activity, open manifest and add `<activity>` element as a child of `<application>` element.

```
<manifest ...>
<application ...>
    <activity android: name="".ExampleActivity"/>
    ...
</application...>
</manifest>
```

II LITERATURE SURVEY

[1] **“I-Lock: Immediate and Automatic Locking of Mobile Devices against Data Theft”** describes a smart application which provides secure and usable defence against mobile theft. Mobile phones have become very important for everyone and almost all the sensitive and confidential data are stored in their mobiles. Hence it is necessary to protect the data theft from thieves. I-Lock quickly and accurately recognizes the user’s physical separation from his/her mobile by detecting changes in wireless signals. Once this separation is detected, this application quickly locks the stolen phone so that the thief cannot access the confidential data, even if successful in stealing the mobile. I-Lock uses acoustic signals and requires at least one speaker and microphone that are available on most of the mobile devices.

[2] **“Smart Phone Anti-theft Solution Based on Locking Card of Mobile Phone”** describes an android application which provides anti-theft solution based on SIM card locking. The solution proposed mainly includes software components, and accordingly hardware needs to be chosen. This application is based on SIM locking. Mobile Phone just identifies one or two locking SIM card belonged to user. Even if thief steals the phone, the mobile owner can telephone the service operators that he lost SIM will be invalid. The thief cannot start the mobile, exchanging for other SIM. Even if the thief is successful in stealing the

phone he cannot use it or sell it. In this application the function of SIM locking is realized by using software algorithm.

[3] **“I Guard: A Real-Time Anti-Theft System for Smartphones”** describes a real-time anti-theft system for smartphones. I Guard utilize only the inertial sensing data from the smartphone. The basic idea behind I Guard is to distinguish different people holding a smartphone, by identifying the order of the motions during the ‘take-out’ behavior and how each motion is performed. It uses a motion segmentation algorithm to detect the transition between two motions from the noisy sensing data. This algorithm checks that the motion is performed by smartphone owner itself. I guard instantly alarms once the tracked data deviate from the phone’s original user’s habit. The advantage of this system is, it is able to identify instantly whether the user is himself/herself taking out the smartphone, by exploiting the built-in inertial sensors on smartphone. However if the mobile is switched off this system is of no use.

[4] **“Smart Dog: Real-time Detection of Smartphone Theft”** is a real time smartphone anti-theft scheme for keeping mobiles safe. With embedded motion sensors, it can easily capture the owner’s behavior of how they pick up their mobiles from pocket or their bags. If a thief makes an attempt to steal the mobile from pocket or bag, the application will detect the thief’s unusual motion. Even if the thief knows the owner’s style of picking up his/her mobile from pocket or a bag, the thief can hardly reproduce the same behavior of picking up the mobile. Through an intensive trace-driven simulation with “picking up” samples from 20 volunteers, collected over 2 weeks, this system achieved 10.2% average false positive and 5.5% average false negative error rates.[4] The advantage of this system is it can easily detect the thief’s unusual motion of stealing the mobiles by triggering an alarm. However this system is of no use if the mobile owner come to know about his/her phone theft after long interval of time.

[5] **“Smart Theft alert for Android Phones”** uses the concept of service. Services are one of the important Android component which runs on background without interrupting the user. The application continuously runs in the background and checks for the SIM card change. It utilizes the camera of device by running camera service in the background. As soon as the SIM is changed by the thief, the application uses front camera of the device or rear camera (if device does not have front camera), and captures the snapshots through it and send to registered e-mail id. This entire process runs in the background and thief is unaware of this. The advantages of this system are, it is easy to catch the thief through snapshots and application runs in the background. However it requires good network connection.

III EXISTING SYSTEM

There are many existing systems that provide security to the smartphone users to prevent their mobile being stolen and if in case mobile is stolen, it can be easily recovered. One of the existing system is **“Where’s my android”** which is a pure find my Android application that will assist you locating your device. When your phone gets missing, sending a particular code will make your phone ring, even if you have kept that on silent mode and then you will receive a code from phone which got GPS which will correlate you with your phone. You can control your phone with this by making it connected with the commander option. You can easily take out or seal your influential data from being misuse. The advantages of this application are it protects the confidential data and make the lost mobiles on ringer mode even if it is in silent mode. But it cannot give accurate information of the thief. Another application is **“Android Lost”** which is not only ideal for finding your missing phone but will also agony the thief. You can activate the alarm to a ring along with a flashing screen which enable GPS, Wi-Fi connection and will wipe the SD card as well and will provide you the thief’s latest call list. The advantages of this application is it provides with latest call list but if the thief formats the phone the application will also be uninstalled.

IV PROPOSED SYSTEM

The main aim of our proposed system is to track the location of the lost phone through the GPS service and capture the snapshots and videos of the thief with front and rear camera without thief’s knowledge and sending the location and images/videos to alternate contact number and email-id. We can see the location of the lost phone on actual google maps which is sent on alternate number. Once this application gets installed in your android mobile device, it will store your email id, alternate mobile number and keep running in the background by using services. Then it will keep checking for SIM number, once a user/thief changes the SIM, it will detect that SIM is changed by comparing new SIM unique number with stored one and send the signal to start services which will start capturing snapshots and videos of the thief and sending it to registered email-id with location. Also when the SIM is changed, the user’s data is automatically backed up so that the confidential data of the users are retained. In many of the existing systems, when the SIM is changed, the location is sent via SMS to alternate registered number and images/videos are sent to alternate registered email. But there is no automatic backup facility of the data and hence the user’s data is hampered by the thief. Hence in our proposed system, location is sent both as SMS and on email along with images/videos and there is automatic backup of data.

Advantages:-

- Once installed it runs in the background without thief's knowledge.
- When thief changes the SIM, the application starts its working and provides actual location of the stolen phone through google maps along with automatic data backup on the server.
- The application takes snapshots and videos of the thief with front camera without thief's knowledge and sends it to registered email-ID along with the location.

Disadvantages:-

- The location information needs to be always on.
- If the mobile is switched off after being stolen, and not switched on again, then this application will not work.
- If the thief doesn't change the SIM or remove the stolen mobile's spare parts, then this application is of no use.

Table 1: - Existing System v/s Proposed System

Existing System	Proposed System
1. In Existing system, location is sent via SMS to alternate registered contact and images/videos are sent on alternate registered email.	1. In our proposed system, the location is sent both as an SMS and on email along with images/ videos.
2. Template message corresponding to location, or image is required to be sent to the stolen phone to get respective information.	2. As soon as the SIM is changed by thief, it automatically fetches the location and images/videos and sends it to alternate mobile.
3. Here, limited push notifications can be sent.	3. Our application uses GCM through which unlimited messages can be sent.
4. There is no data backup facility in some of the systems.	4. In proposed system, when the SIM is changed, automatic data backup on the server starts.
5. Although many systems exists, the users are still unable to find the actual thief.	5. This system will help in finding actual thief of the phone by providing images/videos of the thieves.

Flowchart of Proposed Application

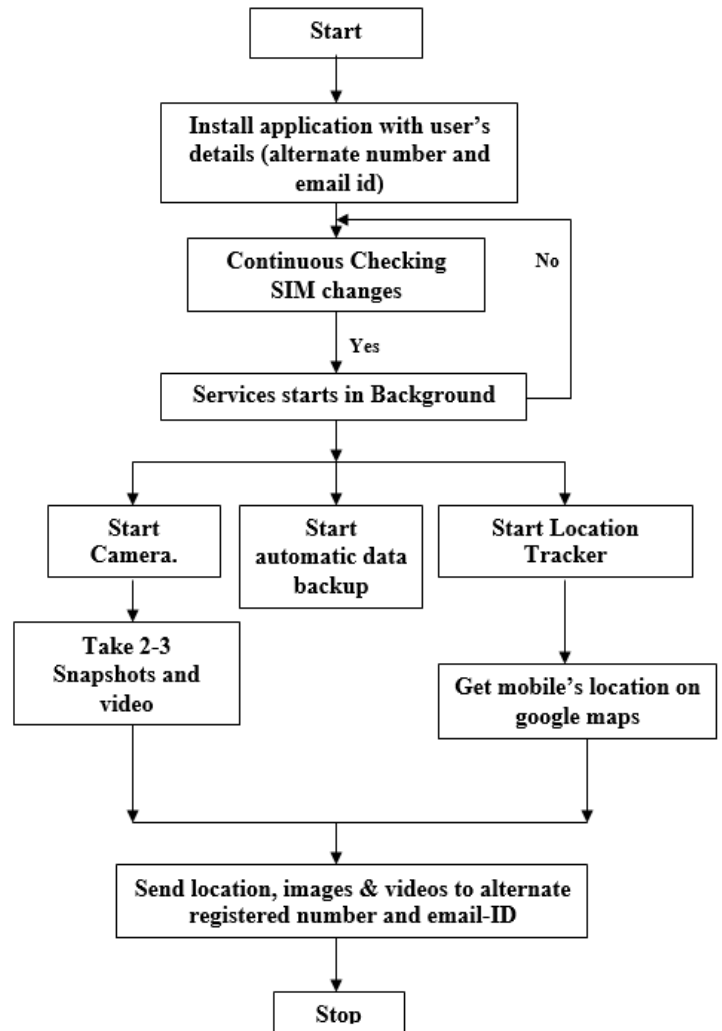


Figure 2:- Working of proposed system

V METHODOLOGY

We have proposed four methods to track location of the lost smartphone. One is the basic where we get SMS whenever SIM card is changed, second method is tracking GPS location of phone by using google maps, the third method is capturing the images and videos of thief, and the last one is automatic data backup.

1. Basic Method: - In Basic Method we use SIM unique number for identification of authorized user. A subscriber identity module or subscriber identification module (SIM) is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). SIM number is nothing but

the sequence of ten digit numbers. Every SIM has its own unique number [7]. When the phone is stolen thief will replace the SIM by its own SIM card so the new SIM number will not match with previous SIM number, this will create an alert message and will start the service in the background by sending message to alternate number. With the help of this method we can easily find out the location of the smartphone.

2. GPS Location:-In Second method we can find the location of mobile. Every mobile has unique IMEI number and we can easily track this number using GPS services. When a mobile is lost or stolen, the application will activate the GPS and mobile network. This application sends location to the user through mail in interval of one minute. The user goes to the location and catches the lost mobile.

3. Snapshot of thief:-When the phone is stolen thief will replace the SIM by its own SIM card, so the new SIM number will not match with previous SIM number, which will create an alert message and capture some of the snapshots and a video from front and rear camera and send this to registered alternate contact & email id. Using these three methods it is easy to find stolen mobile.

4. Automatic Data Backup: - When the thief steals the phone and changes the SIM, the application will automatically take the backup of the confidential data (images, videos, files, contacts) on the server, so that the user's data is safe and he/she can access it.

VI RESULTS

The Application sends the location of device to registered alternate number which can be used to get the device back. It also starts automatic data backup so that the users can access his/her data. It also provides images through camera of device, thus enabling us to recognise the thief

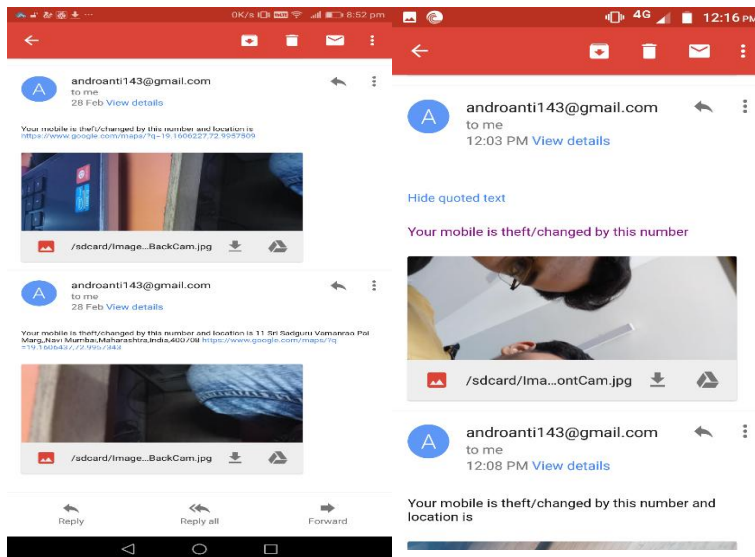


Figure 5:- Images with front Camera on registered email

Figure 5 images withback camera on registered email

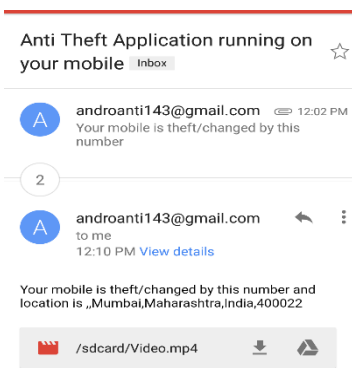


Figure 6:- video on Registered email

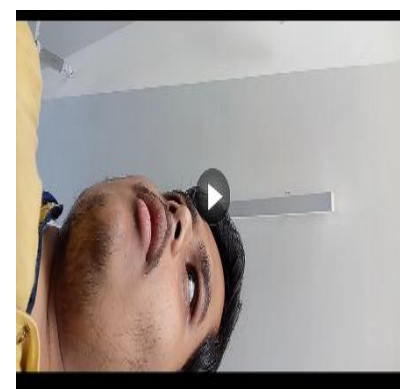


Figure 7:- Sample video

VII CONCLUSION

The application deploys a security solution that meets users immediate and long term requirements by providing the images and videos of the thief, which makes easy for the user to identify the thief and make him/her get caught and arrested. We are enhancing this application by providing the information about the location of the android based Smart phone with the help of text messages. With the advent of time, technology is evolving every day. Our application will further be developed and improved.

REFERENCES

[1] Tao Li, Yimin Chen, Jingchao Sun, Xiaocong Jin, Yanchao Zhang, "I-Lock: Immediate and Automatic Locking of Mobile Devices against Data Theft", ISBN 978-1-4503-4139-4/16/10, ACM DOI: <http://dx.doi.org/10.1145/2976749.2978294>
 [2] Gao Yongqing, Zhou Chunlai, Shang dan, "Smart Phone Anti-theft Solution Based on Locking Card of Mobile

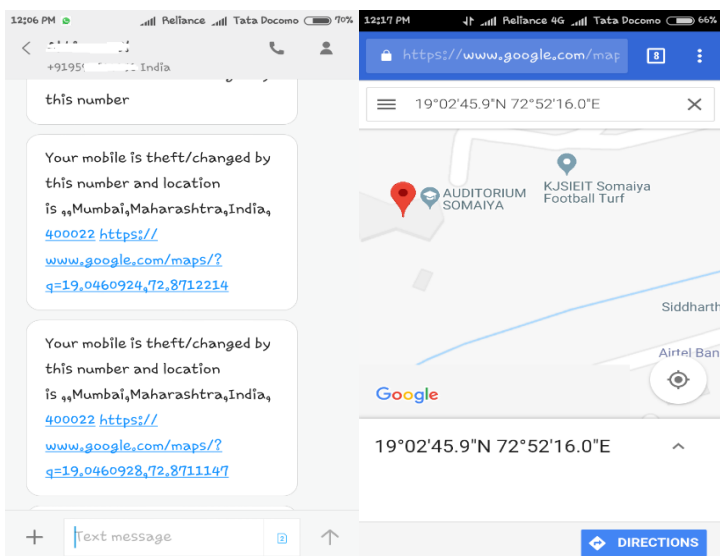


Figure3: Location SMS Figure4: Location on Google maps

Phone”, 978-0-7695-4501-1/11 2011 IEEE DOI 10.1109/ICCIS.2011.55

[3] Meng Jin, Yuan He, Dingyi Fang, Xiaojiang Chen, Xin Meng, Tianzheng Xing, “I Guard: A Real-Time Anti-Theft System for Smartphones”, DOI 10.1109/TMC.2018.2798618, IEEE Transactions on Mobile Computing

[4] Shan Chang, Ting Lu, Hui Song, “SmartDog: Real-time Detection of Smartphone Theft”, 978-1-5090-5880-8/16 \$31.00 © 2016 IEEE DOI 10.1109/iThings-GreenCom-CPSCoM-SmartData.2016.61.

[5] Sharmila K., Sivasankari A., “Smart Theft alert for Android Phones”, IJCT, Volume 3 Issue 4, July - Aug 2016.

[6]<https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>

[7] https://en.wikipedia.org/wiki/Subscriber_identity_module

[8]<https://www.businessinsider.in/People-Are-Willing-To-Go-To-Extreme-Lengths-To-Retrieve-Their-Stolen-Smartphones/articleshow/34790154.cms>

[9]<https://developer.android.com/guide/components/activities/intro-activities.html>

[10]<https://developer.android.com/guide/components/services.html>