Anti Theft Hybrid Solution for Tracking & Locating Mobile Devices with Data Security

Nikhil Bhomia, Kishor Kolhe

ABSTRACT--- With passage in technical and scientific knowledge, the execution and accomplishment of mobile devices is increasing. The usage of smartphones is becoming generous now a days. Since the performance and use of these smart devices is expanding to a larger extent because of their capability to reserve a vast amount of data varying from a simple multimedia file such as images, videos to those important information regarding contacts, messages etc. These smart devices are sometimes also used to store more complex information such as those important and sensitive details regarding bank accounts, passwords, ATM pins etc. Since all these information can lead to various kinds of thefts. Therefore protecting this information from unwanted theft of mobile smart devices and tracking the stolen device is a must. This paper presents an approach to an application that will help to protect the valuable data of the owner and helps to track the device when it is stolen by any unwanted means. This application will use the internal camera of the smartphones that will start capturing the activity when the application starts. The application will run in the background and will not be available in android launcher so that the one who has stolen the device will never get to know that he has been captured along with his location.

Keywords— Mobile Security, Android, Multimedia Messages, Location Tracking, Data Protection, Privacy..

I. INTRODUCTION

In today's modern world, one of the most important things a human being have is a smartphone. They have become one of the most important part of one's life. Smartphone is a vital part in day to day activities. Approximately two-thirds of the world population is connected via smartphones and these numbers will increase with upcoming generation. These devices can be used to store a huge amount of data in any form. A smartphone reduced the amount of usage for computers for daily common activities. Smart devices are also use full to accumulate some sensitive and critical data like various types of passwords for different accounts, bank account details and other critical information.

But with every advanced technology, there comes some kind of dis advantages. As the number of smartphone users is increasing rapidly, the number of thefts of these devices is also increasing. According to some sources [1], the number of smartphone devices getting lost or stolen at various places is stated below :-

- Millions of devices are stolen in an average year, out of which only 7 percent devices are found back.
- 4.3 percent devices provided by offices and various companies are stolen in an year.
- In an average year conferences lose 52 percent of smartphone devices and meetings from various offices lose 24 percent of devices.

Since the number of smartphones devices getting stolen are too huge, therefore the personal and important data of users is getting lost. But there are various applications present to protect user's data or to track the devices. Many applications provides a way to protect the data of user by deleting it from the device so the attacker will never get the access to that user data. But this approach will also has a dis advantage for the user because he/she will eventually lost the data when it gets deleted by the application in order to protect it from any unwanted usage by any unwanted person who stole the device. In some cases, the person who steals the device will change the sim card and hard reset the phone to factory restore settings which will remove and delete all the accounts along with the personal data of the user. Since this will remove the accounts from the device then it will be hard to track the device using android device manager. Even if by some means the user will able to track the device then also he will lose the data present in his device.

Such separate applications are available either to protect the user data or to track the device. But a hybrid solution is not available to protect the user data and to track the stolen device.

This paper is all about the hybrid approach to an application that will do both the task for the user at once. This application will protect the personal and important data of the user as well as track the mobile device with the help of capturing images and videos and send those captured images and videos to a preconfigured number by the user that will help the user to track the device and protect the data from any unwanted usage.

The user will need to register on this application by providing some information such as name, email id and alternate mobile number. This application will not be available in android launcher so if any time the device gets stolen then the one who has stolen it will never get to know that such an application is running in background.

This application will capture the images and videos from the device's camera and send these captured snapshots to the preconfigured number which the user has entered at the time of registering on this application. At the same time this application will also send a mail to the registered email id that will contain those videos and snapshots. With the help of those snapshots the identity of that person who has stolen the device can be traced

Revised Manuscript Received on July 10, 2019.

Nikhil Bhomia, School of Computer Science and Engineering Dr.Vishwanath Karad MIT World Peace University Pune,India. (bhomianikhil19@gmail.com)

Dr. Kishor Kolhe School of Computer Science and Engineering Dr.Vishwanath Karad MIT World Peace University Pune,India.(Kishor.kolhe@mitwpu.edu.in)

This application will run in the background without the knowledge of the person who has stolen the device & it will look for IMSI number (SIM number). Whenever this number looks different, the application will click a picture from the internal camera of the device anonymously and send that pictures to the registered email Id.

1. Tracking SIM Identity Number :-

We can get the location of our device after being stolen by using GPS technology and tracking the SIM IMSI number and IMEI number and get the captured photos of the thief as well.

2. Location Tracking via GPS:-

We can use GPS to track down the device once it gets lost or stolen by any means. The longitude and latitude will be sent to already registered number of the owner if the internet is switched off and in case of internet the exact location will be shared in a particular period of time on the app.

3. Capturing Image:-

Here the camera is inserted to capture the photographs so that unauthorized person or thief along with its surrounding is capture using this application.

On server the photograph is uploaded the server will capture the link and then the link is send in the form of alert to the original smartphone user or owner.

4. Notification Message:

In this kind of message service, the original owner will get the message on his alternate number or the number which he or she entered while registering on this application. This alert or notification message can be used to track down the device along with the person who has stolen it

II. LITERATURE SURVEY

TECHNIQUES USED FOR DETECTION AND SECURITY OF THEFT ANDROID DEVICES.

Plausible Deniable Encryption (PDE):-

This can be used to save complex data counter to strong challengers that can force operators to use different technologies to disclose their important data. Such exercise would not be muddled with encrypting technologies because it hides data on the basis of encrypted data. Various already present solutions has a provision to support encryption of full disk with plausible deniability in the released desktop operating system. True Crypt [8] is a well known system among the PDE tools. To the best of our knowledge, Mobiflage [9] is the first PDE system for android devices, and it is implemented based on a physical or emulated SD card with a FAT32 file system.

iGuard:-

iGuard is a technology that is capable in identifying instantly if the owner itself is taking the device, by manipulating only the built-in inertial sensors on the device. Unlike already present approaches for identification of the user that depends on lasting features of various users, iGuard can differentiate different users in real time, utilizing only one key behavior, namely taking out the smartphone.

Hidden volumes-based:-

Based on hidden volume approach some of the tools based on PDE are True Crypt and Free OTFE [19]. A single hidden volume enabling tool is True Crypt which is an open source project. Hidden volume can be a virtual file or any disk. It also enables plausible deniability: it allows a user to create a hidden volume inside a normal True Crypt volume's free space. Vera Crypt is a fork of the discontinued True Crypt project. Many security improvements have been implemented and issues raised by True Crypt code audits have been fixed.

Logical Volume Management (LVM):-

To avoid the modification of the file system driver a technique is implemented for linear allocation of the storage space known as logical volume management. However, such model functions on mobile devices present some mutual defects and have the same origin. 1) It is inconvenient to transfer important data to a hidden volume from a normal volume. However, TrueCrypt is the reverse and can mount the outer volume and hidden encryption volume simultaneously. 2) If we need to mount the hidden volume we need to reboot the android devices. 3) These systems present cross-border corruption and less use of space used for storage.

Typing authentication and protection (TAP):-

It is a system for smart devices that is based on virtual key concept. If we are using this technology then we can enhance the security of devices by using 2 methods, one is the login stage and another is the post login stage. Biometric Information is controlled by TAP in its first stage & also secure identity of the user by using hand morphology. With the use of virtual key, dynamic behaviour is controlled by TAP in its second stage. Using this technology we can say that some features of smartphone devices such as security & usability is preserved by TAP.

III. PROPOSED SYSTEM ARCHITECTURE

Using our project, we emphasis on providing data safety and secure services to users of various android mobiles and in addition provide prevention against camera attacks. In case of theft; user can get the photos and video of the thief. Moreover, this scheme can efficiently detect this type of defense attacks.

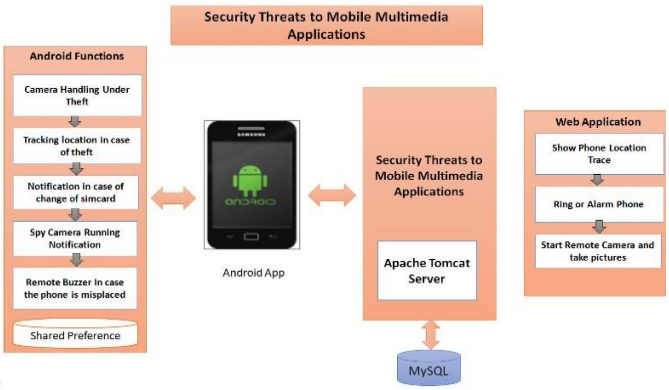


Figure: - System Architecture.

1. Camera Handling Under Theft.

a. Check CPU and ram usage of phone if performance is good then.
b. Stop the audio and vibrate mode.
c. Captures the camera pictures and save them on SD-card in the format that cannot be identified by the user of the phone.
d. Email photos/videos to owner and regain old audio and vibrate settings.

2. Tracking location in case of theft.

a. Owner goes to the website
b. Tracks the phone by its name or IMEI number
c. Owner gets location latitude and longitude along with area name

3. Notification in case of change of sim card.

a. Owner sim card numbers and their access dates are stored in the shared preference of phone
b. In case the SIM card is discarded then the mobile phone owner will get the notification.

4. Spy Camera Running Notification.

a. Our project will check If an any app is accessing camera
b. If the application is system's default camera app i.e. com.android.gallery3d then do not show any notification
c. Else an alert dialog is shown to the user.

5. Remote Buzzer in case the phone is misplaced

a. User can play a remote buzzer or ring an alarm in case if he/she wants to find out a misplaced handset in the house.

IV. ALGORITHM USED

1. GPS based distance formula

GPS Based distance formula is used to get distance between to latitudes and longitudes. It is also called Have sine Formula.

$$a = \sin^2(\Delta\varphi/2) + \cos\varphi_1 \cdot \cos\varphi_2 \cdot \sin^2(\Delta\lambda/2)$$

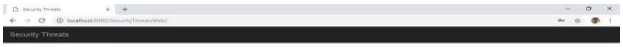
$$c = 2 \cdot \operatorname{atan2}\left(\sqrt{a}, \left(\sqrt{1-a}\right)\right)$$

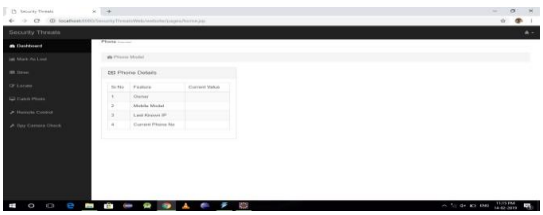
here,

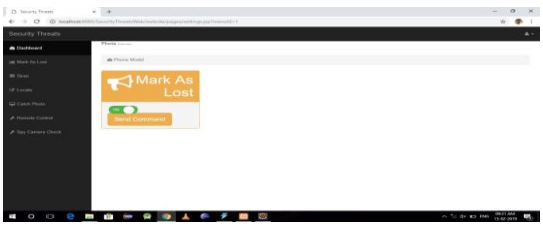
- φ represents latitude.
- λ represents longitude
- R represents radius of earth (mean radius = 6,371km).
- It should be noted that the angle should be in radians so that the functions of trig can be passed.

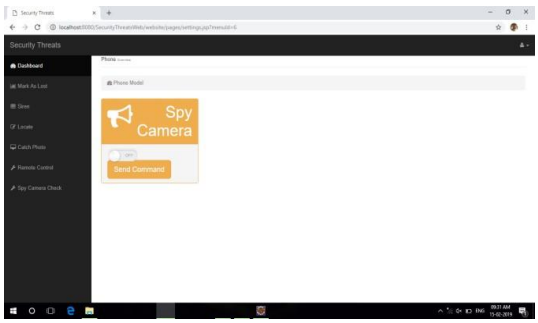
V. RESULT AND DISCUSSION

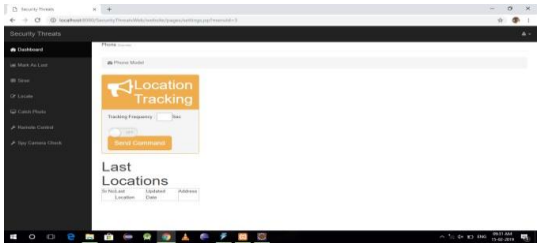
We can mark the device as lost whenever any device gets stolen and we will get the following functionality as shown in few screenshots below :-











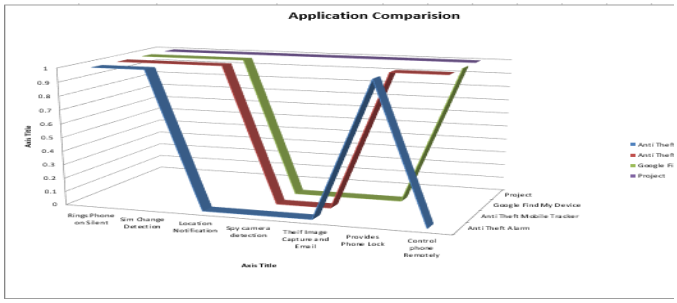
VI. COMPARATIVE ANALYSIS

We compare the functionality of our application with the current google android device finder and we get the following results:-

S. No.	Feature	Google Device Finder	My Application
1	Play Sound	Yes	Yes
2	Locate Device	Yes	Yes
3	Wipe Out Data	Yes	Yes
4	Remote Control	No	Yes
5	Capture Pictures	No	Yes
6	Spy Camera Check	No	Yes

VII. GRAPHICAL ILLUSTRATION

	Anti Theft Alarm	Anti Theft Mobile Tracker	Google Find My Device	My Application
Rings Phone	1	1	1	1
Sim Change Detection	1	1	1	1
Location	0	1	1	1
Spy Camera Detection	0	0	0	1
Thief Image Capture	0	0	0	1
Phone Locks	1	1	0	1
Control Phone Remotely	0	1	1	1



VIII. CONCLUSION

In communication world such as that of wireless multimedia, the most important aspect or the security issue is related to the mobile phone devices. In today's technological world, one of the most powerful operating systems is android due to which many researchers from various fields have chosen this as a field of their research. However, some researchers have researched about multimedia security of mobile devices. Smartphones store a plenty of complex information. Since these smartphones stores such important and complex data of the user due to which these devices become the main target for the physical theft attack. In such cases the users want to get back their devices as well as the information to be protected from such unwanted thief or malicious users to use this data illegally.

Using this project, we focus on providing data security to mobile users and in addition provide prevention against camera attacks. In case of theft, user can get the photos and video of the thief. Also we can lock our device after getting a message of SIM change so that the thief cannot get access to the complex data of the owner.

REFERENCES

1. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding Users' Requirements for Data Protection in Smartphones," in 2012 IEEE 28th International Conference on Data Engineering Workshops, 2012, pp. 228–235.
2. W. Lee and R. Lee, "Multi-sensor authentication to improve smartphone security," in Conference on Information Systems Security and Privacy., 2015, pp. 1–11.
3. S. Zahid, M. Shahzad, S. Khayam, and M. Farooq, "Keystroke-based user identification on smart phones," in Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2009, pp. 224–243.
4. H. Pang, K. L. Tan, and X. Zhou, "StegFS: a steganographic file system." pp. 657-667.
5. D. Ghosh, A. Joshi, T. Finin, and P. Jagtap, "Privacy Control in Smart Phones Using Semantically Rich Reasoning and Context Modeling," in 2012 IEEE Symposium on Security and Privacy Workshops, 2012, pp. 82–85.
6. N. Xu et al., "Stealthy Video Capturer: A New VideoBased Spyware in 3g Smartphones," Proc. 2nd ACM Conf. Wireless Network Security, 2009, pp. 69–78.
7. F. Maggi, et al.,"A Fast Eavesdropping Attack against Touchscreens," 7th Int'l. Conf.Info. Assurance and Security, 2011, pp. 320–25.
8. P. Kodeswaran, V. Nandakumar, S. Kapoor, P. Kamaraju, A. Joshi, and S. Mukherjea, "Securing Enterprise Data on Smartphones Using Run Time Information Flow Control," in 2012 IEEE 13th International Conference on Mobile Data Management, 2012, pp. 300–305.
9. R. Raguram et al., "ispy: Automatic Reconstruction of Typed Input from Compromising Reflections," Proc. 18th ACM Conf. Computer and Commun. Security,2011, pp. 527–36.
10. SK. Piramu Preethika and A. Sasi Kumar "EdTAM: Efficient Detection of Theft Android Mobile" Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/97940, November 2016.
11. B. Srilekha , Dr. V. Dhanakoti "Mobile Tracking Based on Phone Theft Detection" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016.
12. A. P. Felt and D. Wagner, "Phishing on Mobile Devices," Proc. WEB 2.0 Security and Privacy, 2011.
13. D. Li, D. Winfield, and D. Parkhurst, "Starburst: A Hybrid Algorithm for Video-Based Eye Tracking Combining Feature-Based and Model-Based Approaches," IEEE Computer Soc. Conf. Computer Vision and Pattern Recognition — Workshops,2005, p. 79.