ISSN: 1832-5505

Applied GIS

Vol-11 Issue-03 July 2023

Protect your data and get smart theft alerts for Android devices

Nikhil Bhomia[1], Dr. Kishor R. Kolhe[2]
Assistant Professor[1,2,]
MIT World Peace University, Pune, India

Abstract— People today think of smartphones as powerful devices, and a lot of smartphone apps use digital video interactions. When it comes to internet messaging, security of the cell phone is the most important thing. Mobile risks in their early stages watch out for attackers who are using different SMS scams. The technology is changing quickly in some important apps, like web browsers, email tools, and other apps that are popular and required on smartphones. We focus on keeping mobile users' info safe and also safeguarding them against camera threats. Users can get pictures and videos of the thieves if they are stolen.

KeywordsGPS (Global Positioning System), IMSI (International Mobile Subscriber Identity), SPY CAMERA, and SMS (Short Message Service) are some ideas.

INTRODUCTION

No one can miss the fact that smart phone theft is a big problem that can lead to big conversations about privacy, property, and public safety. Unfortunately, there isn't a good, low-cost way to keep smartphones from being stolen yet. A lot of smartphone users choose to put software on their phones that can help police find them if they are stolen. This trick won't keep the phone from being stolen. Getting the phone back might be helpful [1, 3].

A smart phone anti-theft solution is needed right away. It should be very sensitive and accurate, and it should be easy to use in all kinds of situations. A smart phone anti-theft solution is needed right away. It should be very sensitive and accurate, and it should be easy to use in all kinds of situations [12].

IMEI NUMBERS: AN OVERVIEW

An IMEI number is a distinctive, identity for mobile devices. Its original purpose was to allow Global System for Mobile communications operators to identify legitimately distributed devices and blacklist stolen ones[8].

An IMEI number is collection of following three elements:

- The first is the Type Allocation Code (TAC) of eight digits.
- A unique individual SNR of six digits used to identify each piece of equipment within the TAC.
- A check digit (CD), also referred to as a spare digit, of one digit calculated using the formula of Luhn (ISO/IEC7812); its original purpose was to avoid manual transmission errors.

Figure: - IMEI NUMBERS

An IMEI number is not random; it contains structured information that is guaranteed to generate unique values for each new manufactured device and to reflect various details about the associated device. The main goal of the attacker's is to *such* as his or her IMEI number (international mobile station equipment identity) [8, 5].

SPY CAMERA

BENEFITS: - The used spy camera able to capture clear image of thief and the surrounding environment. By forwarding such images in addition with the location to the device holder we can identify the theft and get the phone back [11].

LITERATURE SURVEY

TECHNIQUES USED FOR DETECTION AND SECURITY OF THEFT ANDROID

ISSN: 1832-5505
Vol-11 Issue-03 July 2023

DEVICES.

Identification system:-

Zahid et al. [3], proposed the system that monitors the user identification of mobile phone key that classify the original consumers among the fraud dynamically. The authors used custom data set of 25 users to point out the suggested system. That gives the fault rate lesser than 2% after detection mode, and the election of nearly zero after PIN authentication. They also connected their approach with five state-of-the-art procedures existing to identify basic user keystroke.

Implicit authentication using Multi-sensors-based system:-

Wei-Han et al [2] proposed system incessantly learns the user's behavior patterns and setting by allowing the user to use a phone without disturbing the user's actions. This approach also has the capability to update user model. The resultant elaborates the efficiency of the that only requires 10 second time to run this model and also 20 seconds to determine the abnormal as well as fake requests. In this approach the amount of accuracy realize can be extended up to 90-95%.

Data Protection and Privacy: -

Boshmaf et al. [1] address the problem of data protection from user-centered perspective and analyzed the user's need for data protection for smartphones systems. The authors outlined the types of data that users want to protect; they also investigated the practices of current users in the protection of such data and show how the security requirements vary across different types of data.

Kodeswaran et al. [8] have shown a framework to execute the privacy policies on smartphones, and to protect the enterprise data. This flow of information depends on the object involved in conforming IPC (Inter-Process Communication) and its data.

Steganography-based:-

Pang et al [4] proposed a various approach to occupy the blocks for hidden file. They are remarked by the relative block bitmap table and also utilize as abandoned blocks and dummy blocks respectively to obtain reasonable deniability. Unfortunately it has some common defects that mainly includes high I/O overhead as well as less use of space for storage and this type of defects are not tolerated by the mobile environment.

Detection and Security of theft Android Devices:-

SK. Piramu Preethika et al [10] describes to improved technique of stolen android device tracking. This framework uses SMS in offline, MMS in online and Camera (Front) to capture the picture. The user has to provide the alternative mobile number and email ID after installing the application. This approach works on the background and continuously checks the IMSI (SIM card) number, and capture the snapshot by using spy camera as well as send the notification to the registered or alternative number without his/her knowledge.

B. Srilekha et al [11] discuss about the logic of tracking the stolen phone with SIM Card & Theft Phone with changed SIM Card is tracked continuously. The mobile numbers can get the notification from the Theft Mobile. This process is continuously reworked to track the android mobile phone.

PROPOSED SYSTEM ARCHITECTURE.

ISSN: 1832-5505
Applied GIS
Vol-11 Issue-03 July 2023

In 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. Moreover this scheme can efficiently detect this type of defense attacks.

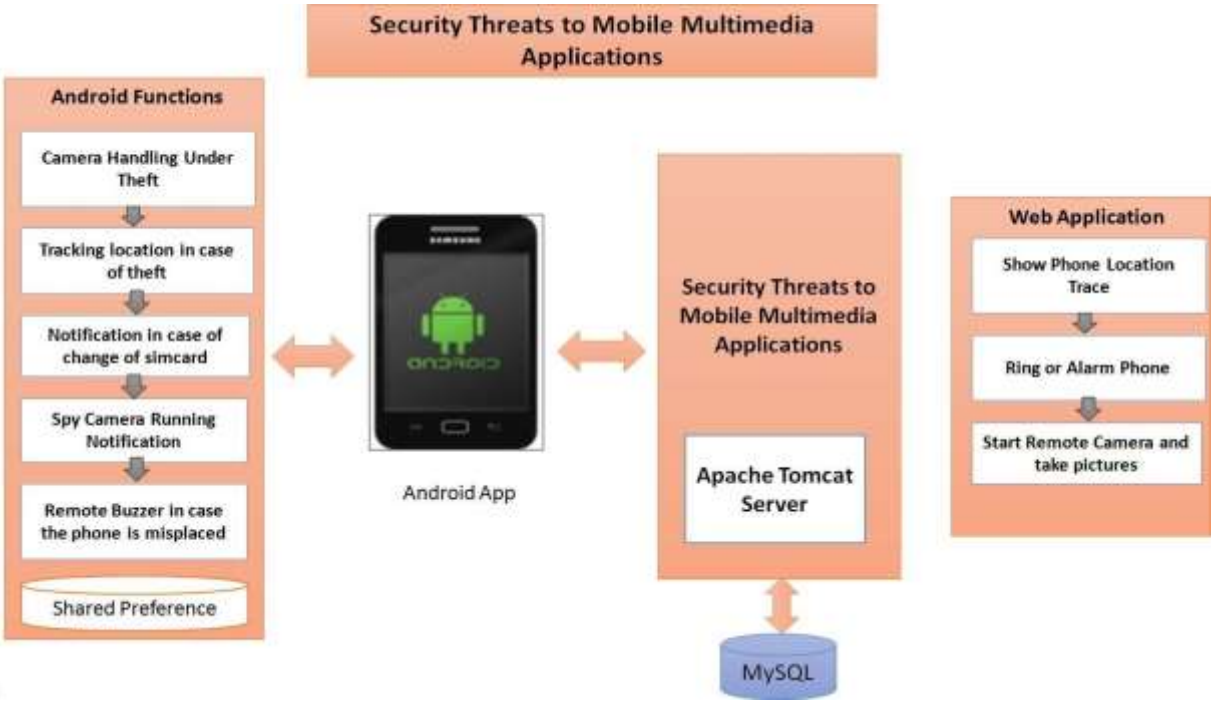

Figure: - System Architecture.

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 ofthe 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 no

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.

II. SYSTEM FLOW (FLOW CHART)

Following is the detail system flow of the proposed system,

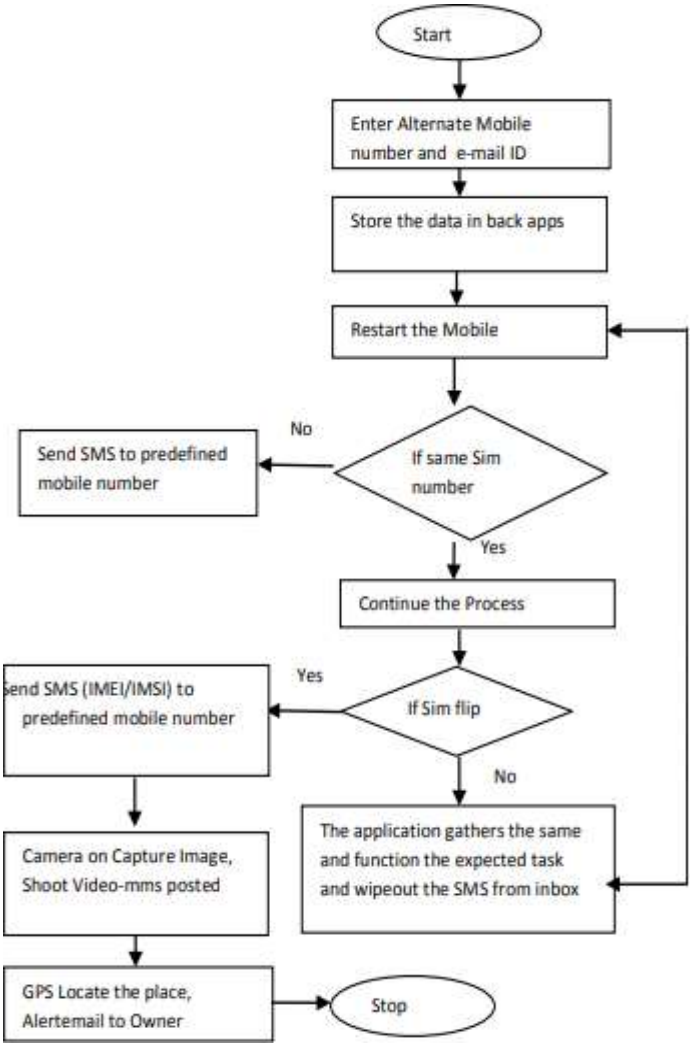

Figure: - System Flow.

RESULTS AND DISCUSSION

1. Tracking IMEI and IMSI Number :-

Using GPRS and GSM Technology we can easily know the stolen mobile location and trace the person. After that

captured details posted through the email and SMS.

2. GPS location:-

In the section stealth mobile location is traced using the GPS application so that it forwarded every action of the thief location and sent the captured location value to the original smartphone users.

Figure: - Location Tracking

3. Capturing Image:-In this situation 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.

Figure: - a) overall view of the phone environment; b) scene captured by phone camera

4. Alert SMS:-

In this SMS alert, place where the stolen mobile was kept will be intimated to the owner or make a call to police.

CONCLUSION

This paper gives a quick look at some of the different methods experts use. This page talks about an anti-theft program platform for Android. This method requires a long-term business security solution because it shows pictures and movies of the thief. Using this app will make it easy to find the thief, catch him or her, and put in jail. It will also help you find the location of an Android-based smartphone and they can search inPerson

through text messages.

REFERENCES

[1] I. 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.

[14] P. Aldrian, "Fast Eyetracking,"

[15] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," IEEE Symp. Security and Privacy 2012, 2012, pp. 95–109.

[16] R. Schlegel et al., "Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones," NDSS,2011,pp. 17–33.