ANDROID & FIREBASE BASED ANTI THEFT MOBILE APPLICATION

Vedang Nikure[1], Pranay Ikhar[2], Vaibhav Kharalkar[3], Jayant manapure[4], Sweta Choudhari[5], Harshad Kubade[6]

[1] Assistant Professor, Department of Information Technology, Priyadarshini College Of Engineering, Nagpur, Maharashtra, India.

[2] UG Students, Department of Information Technology, Priyadarshini College Of Engineering, Nagpur, Maharashtra, India.

---***---

Abstract - *This initiative uses various GPS locations to locate stolen or lost phones. After installation, the program will run in the background. The unique user id and password, SIM number, backup phone number, email address, WhatsApp number, and present location of the phone are all stored in this application. When a phone is lost or stolen, the user receives images taken by the front camera, a GPS location on a different phone number, and an email address. With the help of this information, we can quickly identify the phone and the person who has stolen it using the intruder selfie feature in the app.*

***Key Words*: Mobile theft catcher, firebase, alert system, android application, smart notification.**

1.INTRODUCTION

On smartphones, sensitive info is stored in large quantities. The combination of this knowledge and smartphones' expensive price makes them a desirable target to feed physical theft. It goes without saying that the device proprietor would choose to reclaim the device in this circumstance. The info must also be protected from unauthorized access. In this research, we present the first anti-theft strategy that addresses these issues. Our recommendation is based on an innovative concept for a theft-deterrent honeypot account that protects the person's data while preventing a criminal from scrubbing the device clean.

Today's cell phones cost anywhere from 50k to 1.5 lakh rupees. Besides to the cash loss, a phone can also have its confidential data lost or stolen. According to a survey, there were more than 3.1 million missing smartphones in 2016. A separate study found that victims would spend about Rs. 41,069.33 to get back all of their private data, including photographs and videos. In turn, information leakage to the criminal is prevented and there is a high probability that the true owner of a stolen instrument will be able to retrieve it. The smartphone is a necessity for everyone. They significantly improve day-to-day living. Nowadays, people use cell phones for a wide range of activities, such as taking photos, viewing the internet, and conducting online banking. As shown in Figure 1. However, as malware becomes more sophisticated and advanced, it has been discovered that the perimeter defence strategy's joint efforts are becoming less and less effective. Malware that is constantly changing appears to always find methods to completely avoid the perimeter defence. We provide a detailed description of the most frequent exploitations at the hardware, software, and network levels of the current information system. The advantages and disadvantages of the most prevalent defence strategies employed in these levels are then covered

[1]

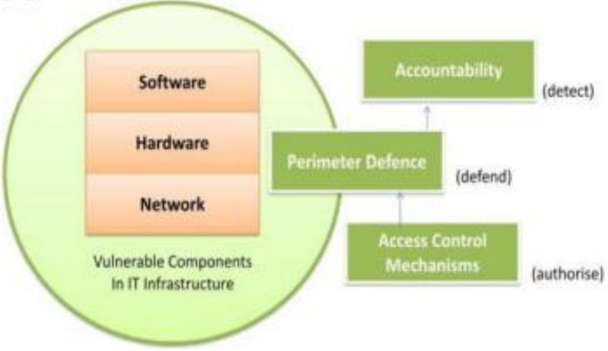


Fig. 1. Vulnerabilities and defense strategies in existing systems.

2. LITERATURE SURVEY

Priyadharshini S. et al, [2] Machine learning techniques have been used in this study to identify malicious Android applications. Open source datasets and Kaggle datasets are the ones who acquire the datasets. Here, data preparation and feature extraction methods are used to accelerate algorithm computation. Applying data pre�processing to data characteristics. In essence, it aids in normalizing the data within a certain region. Data pruning methods for feature extraction are employed. This document shows that data science is used for malware detection and aims to expose the use of machine learning (ML) methodologies for malware research.

Iliyasu Yahaya Adam et al., [3], the research discusses some security issues and potential benefits of mobile phone tracker technologies, particularly for companies that buy and sell used mobile devices. Emerge in relation to the theft or disappearance of phones. Police may become involved in some of the instances as they conduct digital investigations to find the offenders. Some complainants' inability to provide information that will help the police conduct a successful investigation may lead to the mistaken apprehending of an innocent person or people as the perpetrator of a crime related to phone theft. In order to help phone owners and prospective buyers and sellers of refurbished cellphones who want to safeguard their handsets from other GSM-related problems, the paper examines anti-theft and cellphone tracking technologies.

Abdulaziz Aldegheishem et al., [4], two innovative ETD models are created in this study. In the first model, a hybrid sampling strategy a synthetic minority oversampling method with an edited nearest neighbor is presented. Additionally, dimensionality reduction and information extraction from data on energy consumption are done using AlexNet. A moderate gradient boosting approach is then employed for categorization. In the second model, the actual distribution of the data on electricity usage is captured using a conditional Wasserstein generative stochastic network with a gradient penalty. To create more accurate statistics for the minority class, auxiliary provisional information is added to the formula. Additionally, GooLeNet architecture is used to minimize the dimensionality of the dataset.

Michael Becher et al., [5], the world is presently transitioning from an Internet-based to a mobile society, where previously unremarkable phones are being used for an increasing amount of information access. For instance, between 2016 and 2023, the proportion of mobile phones with full-fledged OS increased by almost 200%. Mobile protection is now necessary rather than inevitable. This review article offers a succinct summary of mobile phone security, attack vectors using the back-end system and the browser itself, as well as the layers of hardware and the user as an attack enabler. We highlight the contrasts and parallels between "normal" security and security for smartphones, and we conclude future study directions.

Julian Jang-Jaccard et al., [6], the overwhelming majority of businesses employ a perimeter defence security strategy to shield their IT infrastructure from any potential outside intrusion. This approach places a strong emphasis on "layered defence" or "defense in depth" tactics, which involve fortifying and enclosing vital internal computer assets, such as servers or sensitive data, to protect them.

Sanjana Kute et al., [7], the research that will be done for this thesis will be primarily focused on designing and developing an effective and convenient anti-theft device to address security issues that will help to interrelationship/stop theft. The suggested system offers house protection and monitoring. Webcams with sensors installed assist in identifying, notifying, and keeping users updated on trespassing events.

Zhenyu Cheng et al., [8], in this article, we suggest the Mobile Users' Information defender model, which effectively detects information theft by using convolutional neural networks to analyse the relationship between users' functioning patterns and network flows. Most of the apps that steal collected information can't function correctly in reality due to Command-and-Control server invalidation, system version incompatibility, etc.

A. Shabtai et al., [9], in this article, we introduce a novel behavior-based anomaly identification method for the network behavior of mobile applications. The main objective of the suggested system is to safeguard users of mobile devices and providers of cellular infrastructure from fraudulent applications by first identifying malicious attacks or applications that pose as legitimate ones that are installed on a handheld device, and second identifying previously published, well-liked applications that have been repackaged with malicious code. More specifically, we try to identify a brand-new class of mobile adware that can update itself that was just discovered on the main Google Android market.

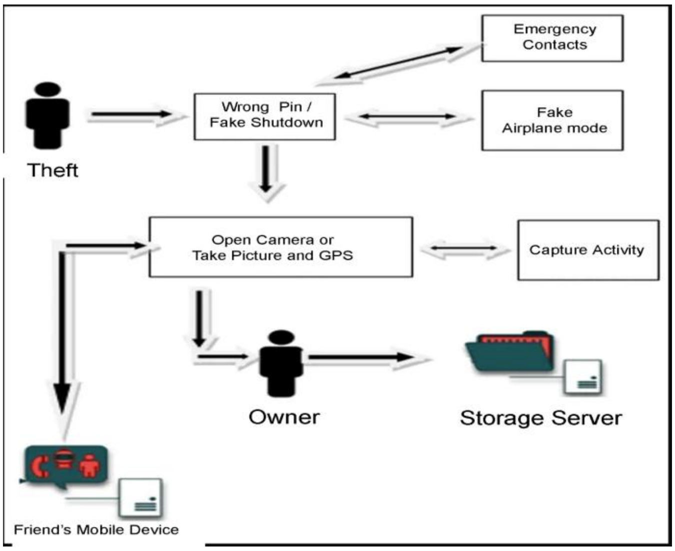
M. Conti et al., [10], this system was fully implemented by the authors, and we also carried out a comprehensive set of tests that demonstrate that approach can achieve precision as well as accuracy levels higher than 92% for the majority of the actions taken into consideration. The authors of this research evaluated solutions to three cutting-edge algorithms, and the results showed that our solution outperforms all of these immediate rivals.

3. METHODOLOGY

3.1Problem Definition:

Personal data is on a mobile phone. There is a chance that this information will be misused if the phone is taken. Any issues, whether they be personal or financial, could arise. Finding the stolen phone is therefore a crucial job. There are some accessible technologies and methods. We can identify the missing phone using that. If a phone is lost or stolen in India, the procedure of finding it becomes extremely difficult. We must follow a drawn-out process and register a case at the police station. To facilitate an easy and comfortable procedure we came up with the idea of anti-theft mobile application and its features are further elaborated in the below section.

3.2 Proposed Methodology:



App Working:

- Once deployed, it operates in the background secretly to the thief.

- When a theft occurs, the application begins to function and provides a real-time Google Maps position of the stolen phone, as well as an automatic server data backup.

- Without the thief's knowledge, the application uses the front camera to capture pictures and videos of him or her and sends them along with their precise location to a registered email address.

- The application will pretend to Fake Shut Down while diverting the user's focus.

Regardless of whether the gadget has a mechanism for locking or not, there are two ways that it can be stolen. If the device is not secured by an unlocking mechanism, a thief will have instant access to the owner's data and may misuse user data on the device such as credentials to cause the owner further damage. For as long as the mechanism for unlocking is in position and the device is locked, it is useless to the burglar. Because of this, it will probably happen that the burglar will completely reset the device, which will result in the loss of all user data. Nowadays, a lot of important private data is stored on smartphones. Additionally, existing anti-theft applications will also be removed from the device, greatly decreasing the likelihood that the device's user can recover it. [11] These two possibilities are not satisfactory. Therefore, a solution is required that safeguards user data security while preventing unauthorized factory resets of the device. The authors of this work present the first method that can safeguard the privacy of a device owner's user data while prohibiting a thief from performing a factory reset and erasing any anti�theft software that has been loaded. [11] By activating the emergency warning, Theft Catcher, a lost phone finder, makes sure that anyone who obtains your phone gets into difficulty. Even if they switch off the device or activate airplane mode. It will capture covert pictures of the intruder and email them to you. To assist in locating missing phones, it additionally includes a cellphone tracker. False Shutdown, Fake Airplane Setting, and Intruder Detector are features of Theft Catcher. All of these were designed to notify your family to their safety and to send help.

Features of the Application

1. Emergency Contacts:
   Hammer communicates live location updates, photos, and audio files to those closest to you when it senses an SOS.

2. Fake Shutdown:
   Any tracking application in the universe is disabled the moment your phone is turned off. We made the decision to address the underlying issue as a result. Hammer will pretend that your phone is shutting down if someone attempts to do so, but it will actually send your Emergency Contacts a live location, pictures, and audio instead.

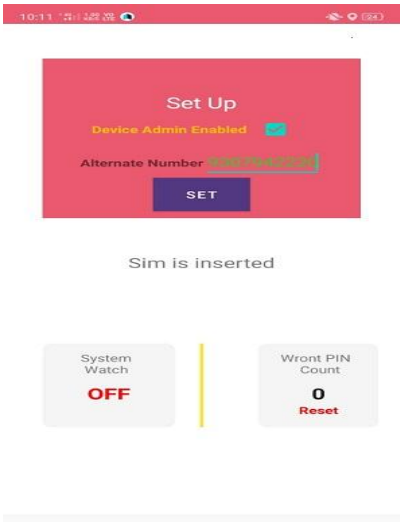
3. Fake Airplane Mode:
   Hammer simulates an airplane mode state when someone attempts to activate it, but instead sends live location, photos, and audios to your contact list for emergencies.

4. Intruder Selfie:
   We will snap a photo of you and forward it to your registered email if someone repeatedly tries to unlock your cell device without success.

5. RESULT

Splish Screen:-

Setup Screen:-



Set Up

Device Admin Enabled ☑

Alternate Number 9307942230

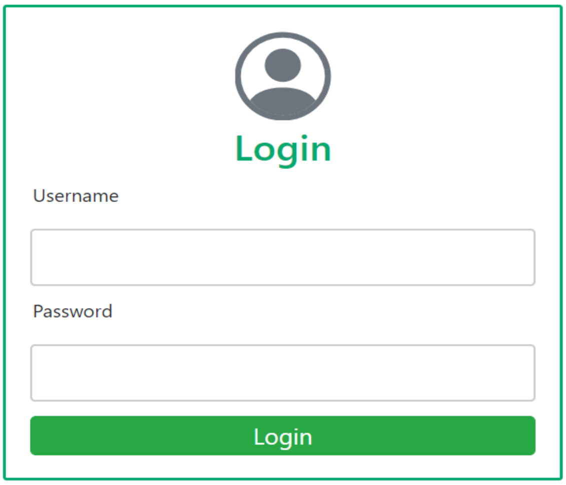
SET

Sim is inserted

System Watch
OFF

Wront PIN Count
0
Reset

Login Page:-



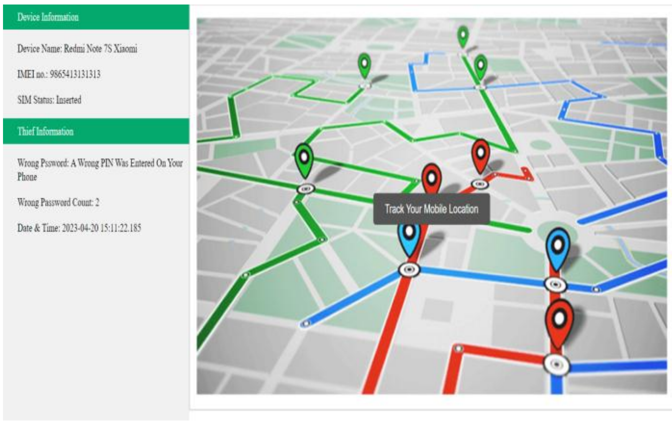
Login

Username

Password

Login

Mobile Information:-



Device Information

Device Name: Redmi Note 7S Xiaomi

IMEI no.: 9865413131313

SIM Status: Inserted

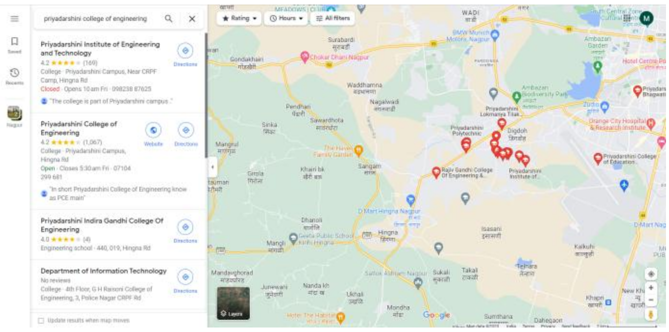
Thief Information

Wrong Pssword: A Wrong PIN Was Entered On Your Phone

Wrong Password Count: 2

Date & Time: 2023-04-20 15:11:22.185

Live Location:-



priyadarshini college of engineering

Priyadarshini Institute of Engineering and Technology
4.2 ★★★★ (169)
College · Priyadarshini Campus, Near CRPF Camp, Hingna Rd
Closed · Opens 10 am Fri · 098238 87625
"The college is part of Priyadarshini campus."

Priyadarshini College of Engineering
4.2 ★★★★ (1,067)
College · Priyadarshini Campus, Hingna Rd
Open · Closes 5:30 am Fri · 07104 299 681
"In short Priyadarshini College of Engineering know as PCE main"

Priyadarshini Indira Gandhi College Of Engineering
4.0 ★★★★ (4)
Engineering school · 440, 019, Hingna Rd

Department of Information Technology
No reviews
College · 4th Floor, G H Raisoni College of Engineering, 3, Police Nagar CRPF Rd

□ Update results when map moves

5. CONCLUSION

Our work on the Anti-Theft Mobile Application fulfils the need of the user of the application for the protection of their contacts, bank information, and other personal information from thieves. With the help of firebase technology, we can connect and send SMS to whoever we want, and with the user's legal permission, the phone's camera and contact access is taken to take action on the thief. The proposed application is made using java technology as its backend and XML for frontend designing. The suggested idea is adaptable to different platforms and scenarios and is universal. Although this method is a crucial advancement in the creation of anti-theft mechanisms, it has more potential in the future. Potential upgrades include safeguarding different user data repositories, like the SIM card and device preferences. Since the SIM card is no longer frequently used to store personal data as well as the device settings do not hold highly sensitive information, these storages were not considered in our approach. The development of alternative methods that simulate the owner's account data from throughout the honeypot account is another area of future work. [11] The automatic or semiautomatic generation of false data is one of these methods.

6.REFERENCES

[1] S. N. Julian Jang-Jaccard, "A survey of emerging threats in cybersecurity,," Journal of Computer and System Sciences,, Vols. Volume 80, ISSN 0022-0000,, no. Issue 5, https://doi.org/10.1016/j.jcss.2014.02.005., pp. Pages 973-993,, 2014,.

[2] S. P. a. S. Shanthi, "A Survey On Detecting Android Malware Using Machine Learning Technique," 7th International Conference on Advanced Computing and Communication Systems (ICACCS), no. doi: 10.1109/ICACCS51430.2021.9441712., pp. pp. 1621-1627,, Coimbatore, India, 2021,.

[3] C. V. A. V. Iliyasu Yahaya Adam, "Problems and Prospects of Anti-Theft and Mobile Phone Tracking: A case in Nigeria," 7th International Symposium on Digital Forensics and

Security (ISDFS), no. DOI:10.1109/ISDFS.2019.8757527, June 2019.

[4] M. A. N. J. N. A. M. S. a. H. A. Abdulaziz Aldegheishem, "Towards Sustainable Energy Efficiency with Intelligent Electricity Theft Detection in Smart Grids Emphasising Enhanced Neural Networks," IEEE Access, vol. VOLUME 9, no. DOI - 10.1109/ACCESS.2021.30565664, 2021.

[5] F. C. F. J. H. T. H. S. U. C. W. Michael Becher, "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," IEEE Symposium on Security and Privacy, vol. 11 , no. DOI 10.1109/SP.2011.29, pp. 1081-6011, 2011.

[6] S. N. Julian Jang-Jaccard, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, Vols. Volume 80, ISSN 0022-0000, no. Issue 5, doi.org/10.1016/j.jcss.2014.02.005., pp. Pages 973-993, 2014.

[7] R. P. V. M. M. G. Sanjana Kute, "Theft Detection System," Iconic Research and Engineering Journals, vol. Volume 4 Issue 10, no. ISSN: 2456-8880, April 2021.

[8] X. C. Y. Z. S. L. a. J. X. Zhenyu Cheng, "MUI-defender: CNN-Driven, Network Flow-Based Information Theft Detection for Mobile Users," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, vol. vol 268, no. doi.org/10.1007/978-3-030-12981-1_23.

[9] L. T.-C. D. M. L. R. B. S. Y. E. A. Shabtai, "Mobile malware detection through analysis of deviations in application network behavior," Computers & Security, vol. Volume 43, no. ISSN 0167-4048, doi.org/10.1016/j.cose.2014.02.009, pp. Pages 1-18, 2014.

[10] L. V. M. R. S. a. N. V. V. M. Conti, "Analyzing Android Encrypted Network Traffic to Identify User Actions," in IEEE Transactions on Information Forensics and Security, vol. vol. 11, no. doi: 10.1109/TIFS.2015.2478741, pp. pp. 114- 125, Jan. 2016.

[11] A. T. C. H. Sascha Groß, "ThiefTrap – An Anti-theft Framework for Android," Security and Privacy in Communication Networks, no. DOI:10.1007/978-3-319-78813-5_9, pp. pp.167-184, January 2018.