IMEI-based Mobile Device Tracking and Stolen Phone Identification System

Ngaira Mandela
School of Cyber Security and Digital Forensics
National Forensic Sciences University
Gandhinagar, India
ngairamandela@gmail.com

Tashi Wangchuk
Department of Information Technology
Royal University of Bhutan
Dewathang, Bhutan
tashiwangchuk.jnec@rub.edu.bt

Tumaini Mbinda
School of Cyber Security and Digital Forensics
National Forensic Sciences University
Gandhinagar, India
trmbinda@gmail.com

Kamboisssoi Damedjate
School of Cyber Security and Digital Forensics
National Forensic Sciences University
Gandhinagar, India
kamboissoidamedjate@gmail.com

Gideon Mwendwa
School of Cyber Security and Digital Forensics
National Forensic Sciences University
Gandhinagar, India
gideon.phdcs21@nfsu.ac.in

Joel Makopa
School of Cyber Security and Digital Forensics
National Forensic Sciences University
Gandhinagar, India
jpmakopa@gmail.com

Abstract— **Mobile device theft is a pervasive issue with serious implications for individuals and society. The rapid proliferation of smartphones, accompanied by their enhanced computing capabilities and diverse functionalities, has made them repositories of critical personal and financial information. The loss of a smartphone not only results in significant economic loss but also jeopardizes the privacy and security of the owner. Existing anti-theft measures, while providing some level of protection, often fall short in reporting lost devices, tracking, and recovering them can be time-consuming and, unfortunately, not always successful. This paper presents an IMEI-based Mobile Device Tracking and Stolen Phone Identification System, leveraging the International Mobile Equipment Identity (IMEI) numbers associated with mobile devices. The system employs device registration, real-time IMEI lookup, and collaboration with network service providers and law enforcement agencies to identify stolen devices swiftly and aid in their recovery. The proposed system provides an effective and efficient approach to enhance mobile device security.**

Keywords— IMEI, mobile device tracking, stolen phone identification, security, theft deterrence, IMEI database, network integration, device detection, law enforcement.

I. Introduction

Mobile devices have become integral to modern society, revolutionizing communication, information access, and various aspects of daily life. The widespread adoption of smartphones and other mobile devices is evident in the remarkable surge in usage over the past decade. According to statistics by Statista, the global number of smartphone users is projected to reach nearly 6.8 billion by 2028 [1]. This immense uptake underscores mobile devices' pivotal role in today's interconnected world.

Smartphones have become an intrinsic part of daily life, acting as repositories for an array of personal information, including contact lists, photos, videos, schedules, and sensitive financial data like bank accounts and passwords.

Consequently, the theft of smartphones poses not only a significant economic threat but also a grave risk to personal privacy and security. Upon gaining access to stolen phones, thieves can exploit them for fraudulent activities, including unauthorized cash withdrawals and scams targeting the victim's contacts. Reports from reliable sources, such as BBC News [2], underscore this issue's severity and global scale. For instance, in London, an alarming 250 mobile phones are reported stolen on the streets every day, according to data from the Metropolitan Police. This problem is not unique to London, as it is a global challenge with an upward trajectory in phone theft incidents. A survey conducted by Kensington's infographic [3] revealed that 70 million smartphones are lost yearly, and only 7% of the devices are recovered. These thefts encompass a range of scenarios, including device snatching, break-ins, and other forms of theft, highlighting the vulnerability of mobile devices to criminal activities [4].

Mobile phone snatching, a particularly prevalent form of mobile device theft, involves the forceful and often violent taking of a person's mobile phone. This criminal act is not limited to any specific region; it is a global issue affecting individuals across various demographics and locations. In bustling urban centers, crowded public transport, or even seemingly safe neighborhoods, mobile phone snatching has become an unfortunate reality, leading to substantial financial losses and, in some cases, physical harm to the victims [4]. Addressing mobile device theft is thus of paramount importance, necessitating innovative solutions that deter theft and aid in recovering stolen devices. In this context, the IMEI-based Mobile Device Tracking and Stolen Phone Identification System stands as a beacon of hope in the fight against mobile device theft. This system leverages the unique International

978-93-80544-51-9/24/©BVICAM, New Delhi, India

Mobile Equipment Identity (IMEI) assigned to each mobile device, providing a comprehensive framework to identify stolen devices and collaborate with law enforcement agencies for timely action and potential recovery.

This paper presents a detailed examination of the IMEI-based Mobile Device Tracking and Stolen Phone Identification System. We delve into the system's architecture, functionality, and integration with network service providers. We demonstrate how Python programming is pivotal in real-time monitoring and alert generation [23]. Furthermore, we discuss the potential for future enhancements and collaborations to create a more secure mobile device ecosystem. In the subsequent sections, we delve into the technical aspects of the proposed system, outlining its architecture and operational mechanisms. Additionally, we discuss potential advantages and limitations, setting the stage for further research and advancements in this critical area of mobile device security. By focusing on the system's capabilities and potential, this paper aims to contribute to developing effective strategies to combat mobile theft and foster a safer mobile device ecosystem.

II. Related Work

The IMEI number acts as a distinctive identifier for mobile devices. Originally, its primary function was to allow operators of the Global System for Mobile Communications to recognize officially distributed devices and block those that are stolen and on the blacklist [5]. Presently, most anti-theft strategies for smartphones primarily offer passive security, focusing on minimizing privacy breaches and data loss post-theft. During a crisis, the victim transmits control commands to the stolen phone for remote locking, location tracking, data backup, or deletion, actions which do not intrinsically decrease the likelihood of losing the phone. Synchronica Plc has created Mobile Manager, a software tailored for Symbian smartphones, which allows businesses and service providers to quickly secure lost or stolen devices using its web-based application. This software allows for over-the-air wiping and locking, thus preventing unauthorized access to sensitive corporate or personal data [6]. Widely used anti-theft apps like Tencent Mobile Phone Manager [7] and Rising Phone Security Assistant [8] are designed to recognize when a SIM card is replaced. These apps automatically record the number of the new SIM card, enabling the device's owner to use Short Message Service (SMS) for remote operations such as data backup, deletion, or locking of the device. L. Subramanian et al. have recommended a design for a cloud-based security service framework tailored for smartphones in a business setting [9].

However, these corrective measures become less effective if a thief uninstalls the anti-theft apps or turns off the phone before the theft is noticed by the owner. [10] suggested a mechanism for remote erasure, allowing the phone owner to wipe private data even in the absence of Wi-Fi connectivity and after the SIM card has been removed. [11], [29] proposed SmartDog, a real-time smartphone anti-theft scheme to enhance smartphone security. By employing embedded motion sensors, SmartDog efficiently captured unique biometric patterns associated with how individuals retrieved their smartphones from pockets or bags. In the event of a theft attempt, SmartDog could detect unusual motions, even when observed by a potential thief, rendering the replication of the owner's actions highly challenging. Lookout Mobile Security [12] is dependent on detecting the SIM card. When the SIM card is changed, these apps instantly capture the number of the new SIM, enabling the owner to remotely execute tasks such as data backup, deletion, and locking through SMS commands. Moreover, applications like 360 Mobile Phone Guard [13] and Kingsoft Mobile Phone Guard [14] offer SMS alerts for SIM card changes, along with features for tracking, alarming, and securing the phone. Locating devices in its vicinity involves Bluetooth performing an inquiry scan. In this scanning process, Bluetooth issues a request to devices in proximity for their MAC addresses. Consequently, active devices equipped with Bluetooth modules transmit an inquiry request to the phone that is turned off. While Bluetooth suggests a scanning period of 10.24 seconds, this can be optimized to brief intervals of 11.25 milliseconds, recurring every 1.28 seconds, maintaining efficiency without any loss [15]. This enhancement aids in saving power and reducing disturbances with adjacent Piconets. With a sensitivity of -70dBm, the Bluetooth module is capable of detecting the MAC addresses of phones and safely updating them on the server without the need for pairing. Eminent reseracher have conducted several studies to better ubderstand the approach [26]- [28]

In [16], the authors introduced a system that monitors user identification on mobile phones to distinguish genuine consumers from fraudsters in real time. The authors conducted experiments using a custom dataset of 25 users to evaluate their proposed system. The results showed a less than 2% fault rate during the detection mode and almost zero false positives after PIN authentication. Additionally, the authors compared their approach with five existing state-of-the-art methods for identifying user keystrokes. [17], [30] introduced a system that continuously learns a user's behavioral patterns and settings without interrupting their phone usage. The system can also update the user model. The results showed that the model only requires 10 seconds to run and 20 seconds to detect abnormal or fake requests, with an accuracy rate of 90-95%. [18] discuss the logic behind tracking stolen phones with SIM cards and continuously monitoring phones that have changed their SIM cards. The process involves sending notifications to mobile numbers associated with the stolen device. This approach is constantly refined to track stolen Android mobile phones.

In [19], a refined method is introduced for locating stolen Android devices, leveraging SMS for tracking when offline, MMS for online tracking, and the front camera to take snapshots. [20] conducted an analysis of anti-theft solutions accessible to users, aiming to protect private information on stolen Android phones. They examined the application of "remote wipe" and "remote lock" features across 10 prominent anti-theft applications, concluding that remote locks are often ineffective due to substandard implementation methods. In essence, existing anti-theft tools are insufficient in preventing phone theft and can be circumvented through several techniques. Consequently, there's an urgent requirement to develop a proactive and instantaneous anti-theft system that can swiftly identify theft incidents and alert the user, thereby preventing theft from occurring initially.

III. Proposed System

The IMEI-based Mobile Device Tracking and Stolen Phone Identification System is a comprehensive, integrated solution to combat mobile device theft and promote security. This multifaceted architecture comprises several key components that work in synergy to identify stolen mobile devices and serve as a deterrent against theft, as shown in Fig 1.

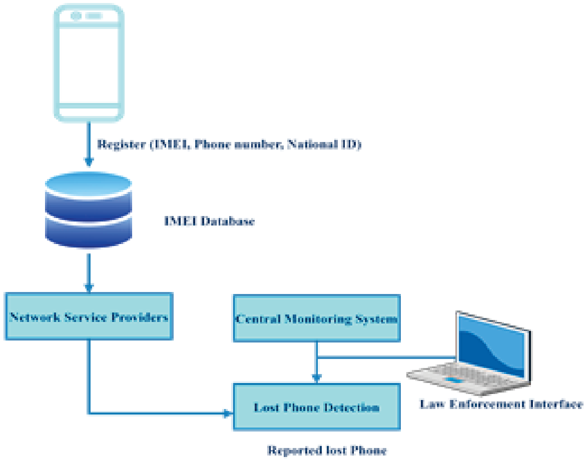

Register (IMEI, Phone number, National ID)
IMEI Database
Network Service Providers
Central Monitoring System
Lost Phone Detection
Law Enforcement Interface
Reported lost Phone

Fig. 1. Proposed System Architecture

Firstly, the system involves Mobile Devices, the individual smartphones or mobile devices registered within it. Each device possesses a unique International Mobile Equipment Identity (IMEI) number, a critical identifier in this context. The IMEI Database is the centralized repository for storing IMEI numbers, associated phone numbers, and the respective national IDs of device holders. It plays a crucial role in efficiently retrieving and storing information to identify stolen devices quickly. Network Service Providers are essential partners in this system. They integrate with the IMEI database, enabling real-time communication and information exchange. They collaborate to identify devices connected to their networks and validate the associated IMEI numbers. At the heart of the system is the Central Monitoring System, which monitors and manages its overall functionality. This component is responsible for processing alerts triggered by detecting stolen devices and interfaces with network service providers and the IMEI database for real-time data updates. The system includes a secure Law Enforcement Interface to facilitate law enforcement efforts. This portal or interface grants authorized access to the IMEI database, allowing law enforcement agencies to query and retrieve information related to stolen devices. The system's device detection mechanism is automated and continuously monitors the network for connected devices. It identifies IMEI numbers as devices connect to the network and initiates IMEI lookups against the IMEI database to identify stolen devices promptly. Through the collaborative efforts of these components, the IMEI-based Mobile Device Tracking and Stolen Phone Identification System aims to deter theft and enhance the recovery of stolen mobile devices.

A. Device Registration and IMEI Database

The device registration process begins upon purchasing a mobile device, where the device holder must register their device in the system. During registration, the device holder inputs the unique International Mobile Equipment Identity (IMEI) number of the device, along with the associated phone number and the national identification details of the device holder. The provided phone number should be active and associated with the device holder. The IMEI database serves as the central repository for storing device information and holding records of IMEI numbers, associated phone numbers, and the respective national IDs of the device holders. Each entry in the database links a specific IMEI number to a phone number and its associated national ID, enabling efficient and quick retrieval of information when a registered device connects to a mobile network.

During the registration process, the IMEI number, phone number, and national ID provided by the device holder are associated with the IMEI database. This association enables subsequent tracking and identifying stolen devices based on their IMEI numbers. To maintain privacy and security, strong security measures are in place to safeguard the IMEI database, ensuring that personal information, including phone numbers and national IDs, is securely stored and accessible only to authorized users. Compliance with data privacy regulations and industry best practices is integral to maintaining user privacy and data security [25]. The IMEI database is regularly updated to reflect changes in phone numbers or device ownership, ensuring its accuracy and usefulness in identifying stolen devices. Efficient mechanisms are in place to handle updates, deletions, and additions to the database as new devices are registered or existing ones are updated.

B. Integration with Network Service Providers

Integration with network service providers is a fundamental aspect of the IMEI-based Mobile Device Tracking and Stolen Phone Identification System. Collaborating with mobile network operators is essential for real-time tracking and monitoring of mobile devices, aiding in the system's core functionality. The system establishes integration with network service providers to enable seamless communication and data exchange, facilitated through agreements and protocols that ensure a standardized and secure exchange of information. This integration allows real-time communication with the network infrastructure, monitoring device connections and detecting IMEI numbers when devices connect to the mobile network. During the device connection process, the system verifies the IMEI number of the connecting device by cross-referencing it with the IMEI database through the integrated network infrastructure, enabling an IMEI lookup request to determine the associated phone number and national ID. The communication between the system and network service providers is encrypted and secured to protect sensitive data during transit [21]. In case of a stolen device being detected, alerts are promptly sent to the respective network service provider, informing them of the stolen device's presence on their network. This triggers coordinated actions involving network service providers, the central monitoring system, and law enforcement, facilitating tracking and potential recovery of the stolen device. The integration process adheres to regulatory requirements and compliance standards, ensuring the legality and ethicality of the system's operations. Integration with network service providers enables the system to tap into the network infrastructure for real-time monitoring, significantly improving the speed and accuracy of stolen device identification and creating a more secure mobile device environment to combat mobile device theft effectively.

C. *Device Connection and IMEI Lookup*

The device connection and IMEI lookup processes are indispensable in the IMEI-based Mobile Device Tracking and Stolen Phone Identification System. When a mobile device connects to a mobile network, its unique International Mobile Equipment Identity (IMEI) number is detected and recorded by the system. Subsequently, an IMEI lookup process is initiated, involving querying an integrated IMEI database to determine if the IMEI is registered and linked to a phone number and national ID. This database query returns vital information associated with the provided IMEI, including the phone number and national ID. If the IMEI is flagged as stolen in the database, an immediate alert is generated, signaling that the connected device is stolen. This real-time processing ensures swift action, aiding in tracking and recovery efforts. The information retrieved from the IMEI database is disseminated to the central monitoring system and, if necessary, to law enforcement for further action. These processes are instrumental in swiftly identifying stolen devices, contributing to a more secure mobile device environment by facilitating prompt actions to mitigate theft and aid in device recovery [22].

D. *Alerts and Law Enforcement Interface*

Alerts and the Law Enforcement Interface are indispensable components of the IMEI-based Mobile Device Tracking and Stolen Phone Identification System, synergistically enabling rapid response and action in cases of detected stolen devices. First, the system's Alert Generation triggers when the IMEI lookup process identifies a stolen device through the IMEI database, promptly generating an alert. This alert is then relayed to the central monitoring system, acting as a centralized hub for monitoring and managing alerts. The Alert Details encompass crucial information, including the detected IMEI number, associated phone number, and any supplementary data from the IMEI database. To ensure efficient handling, the alerts are prioritized based on severity and urgency, allowing law enforcement to focus on critical cases promptly. The Law Enforcement Interface serves as a secure gateway, allowing law enforcement agencies to input the IMEI of a suspected stolen device and perform an IMEI Query. This query retrieves vital information associated with the provided IMEI, including the phone number and national ID. However, access to this interface is strictly regulated, permitting only authorized personnel to retrieve data from the IMEI database.

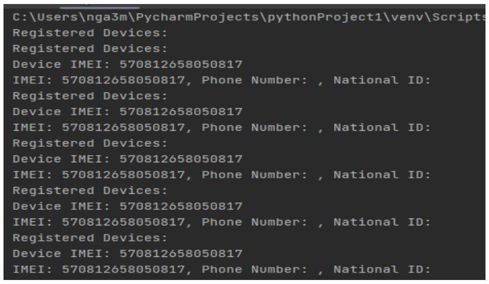
E. *Device Detection Mechanism*

The Device Detection Mechanism is vital to the IMEI-based Mobile Device Tracking and Stolen Phone Identification System. It acts as the vigilant overseer of the mobile network, constantly scanning for new device connections and aiding in immediate tracking and identification of stolen devices. Operating around the clock, this mechanism ensures continuous monitoring of the mobile network infrastructure, swiftly identifying any devices that link to it. Upon connection, the mechanism captures each device's unique International Mobile Equipment Identity (IMEI) number, initiating an automated IMEI lookup process. This lookup, executed in real-time for efficiency, queries the integrated IMEI database to ascertain if the detected IMEI number corresponds to a registered device. Should the IMEI be flagged as stolen in the database, an alert is promptly triggered, setting off a chain of actions within the system. The generated alert is communicated to the central monitoring system, which processes and prioritizes the information, ensuring timely and appropriate action. The Device Detection Mechanism also aids in keeping the IMEI database current by contributing information on newly connected devices and their respective IMEI numbers. Designed with scalability and reliability, this mechanism seamlessly accommodates varying network traffic volumes, maintaining operational accuracy even under heavy load [24]. Striving to have minimal impact on network performance, it operates efficiently within the network infrastructure without causing significant latency or disruption.

Moreover, stringent data privacy and security measures are in place to safeguard the captured and transmitted data. Beyond its technical functions, this mechanism is a deterrent against mobile device theft through its continuous monitoring and real-time detection capabilities, discouraging potential thieves and contributing to a safer mobile device ecosystem. In essence, the Device Detection Mechanism embodies the system's watchful eyes and ears, ensuring swift responses to incidents of device theft and playing a vital role in recovery efforts, ultimately enhancing the security of mobile devices.

IV. Results And Discussion

Following the IMEI-based Mobile Device Tracking and Stolen Phone Identification System simulation, comprehensive data was collected to evaluate its functionality and efficiency. The experiment simulated various scenarios related to mobile device theft, network connectivity, and law enforcement interactions.

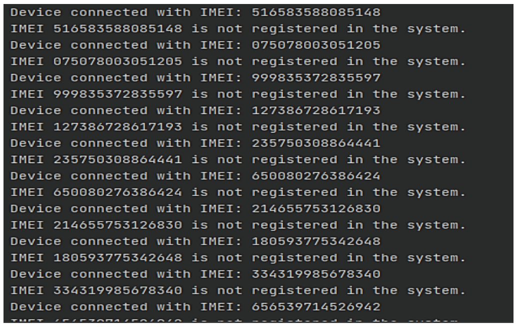


```
C:\Users\nga3m\PycharmProjects\pythonProject1\venv\Scripts
Registered Devices:
Registered Devices:
Device IMEI: 570812658050817
IMEI: 570812658050817, Phone Number: , National ID:
Registered Devices:
Device IMEI: 570812658050817
IMEI: 570812658050817, Phone Number: , National ID:
Registered Devices:
Device IMEI: 570812658050817
IMEI: 570812658050817, Phone Number: , National ID:
Registered Devices:
Device IMEI: 570812658050817
IMEI: 570812658050817, Phone Number: , National ID:
Registered Devices:
Device IMEI: 570812658050817
IMEI: 570812658050817, Phone Number: , National ID:
```

Fig. 2. IMEI database of registered devices

Several devices were registered and associated with their IMEI numbers, phone numbers, and national ID numbers, as shown in Fig 2, and added to the IMEI database.

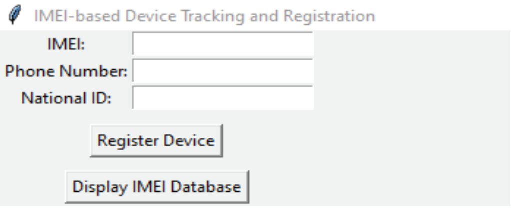
At the network service providers' interface, all the added devices in the database were compared with the existing devices and identified whether the connected device was registered in the system. If the newly added device were registered in the system, it would be detected and associated with the phone number it was connected with, as shown in Fig 3.



```
Device connected with IMEI: 516583588085148
IMEI 516583588085148 is not registered in the system.
Device connected with IMEI: 075078003051205
IMEI 075078003051205 is not registered in the system.
Device connected with IMEI: 999835372835597
IMEI 999835372835597 is not registered in the system.
Device connected with IMEI: 127386728617193
IMEI 127386728617193 is not registered in the system.
Device connected with IMEI: 235750308864441
IMEI 235750308864441 is not registered in the system.
Device connected with IMEI: 650080276386424
IMEI 650080276386424 is not registered in the system.
Device connected with IMEI: 214655753126830
IMEI 214655753126830 is not registered in the system.
Device connected with IMEI: 180593775342648
IMEI 180593775342648 is not registered in the system.
Device connected with IMEI: 334319985678340
IMEI 334319985678340 is not registered in the system.
Device connected with IMEI: 656539714526942
```

Fig. 3. Network service provider interface

Fig 4 indicates the device registration interface of the system to the mobile phone sellers; before the device is given out, it has to be registered so that the device's IMEI can be linked to the national ID and the buyer's phone number.



IMEI-based Device Tracking and Registration

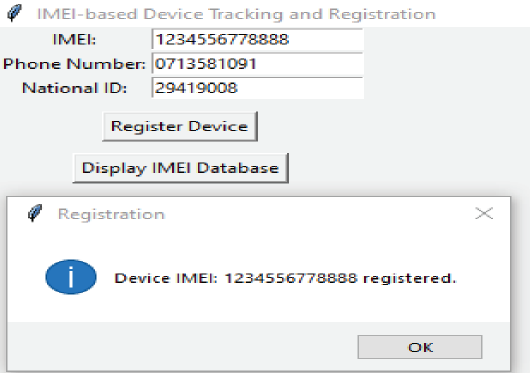
IMEI:

Phone Number:

National ID:

Fig. 4. IMEI Registration Interface

Fig 5 displays the successful registration of the device to the IMEI database.



IMEI-based Device Tracking and Registration

IMEI: 1234556778888

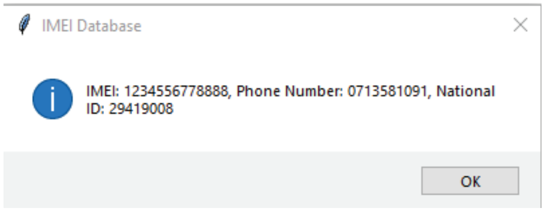
Phone Number: 0713581091

National ID: 29419008

Device IMEI: 1234556778888 registered.

Fig. 5. IMEI Registration Notification.

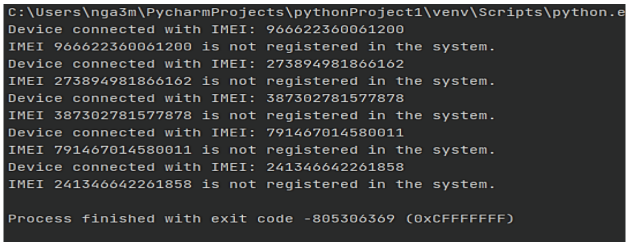
Fig 6 shows the query of the IMEI database that can be queried to identify the IMEI and the registered phone number and national ID linked to ensure accuracy.



IMEI: 1234556778888, Phone Number: 0713581091, National ID: 29419008

Fig. 6. IMEI database Query

The network service provider can monitor the devices in real time as they are connected to the network with their IMEI number, as shown in Fig 7.

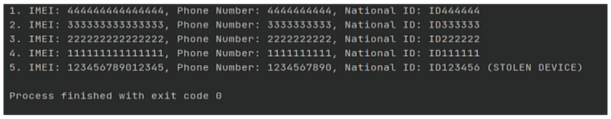


```
C:\Users\nga3m\PycharmProjects\pythonProject1\venv\Scripts\python.e
Device connected with IMEI: 966622360061200
IMEI 966622360061200 is not registered in the system.
Device connected with IMEI: 273894981866162
IMEI 273894981866162 is not registered in the system.
Device connected with IMEI: 387302781577878
IMEI 387302781577878 is not registered in the system.
Device connected with IMEI: 791467014580011
IMEI 791467014580011 is not registered in the system.
Device connected with IMEI: 241346642261858
IMEI 241346642261858 is not registered in the system.

Process finished with exit code -805306369 (0xCFFFFFFF)
```

Fig. 7. IMEI Monitoring From The Network Service Provider

Fig 8 shows the detection of a stolen device when the IMEI does not match the registered ID and national ID.

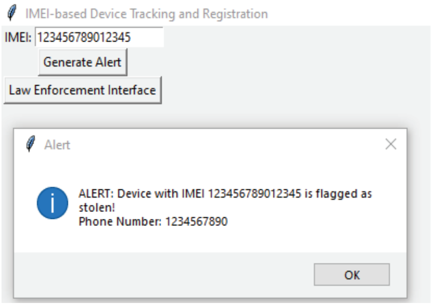


```
1. IMEI: 444444444444444, Phone Number: 4444444444, National ID: ID444444
2. IMEI: 333333333333333, Phone Number: 3333333333, National ID: ID333333
3. IMEI: 222222222222222, Phone Number: 2222222222, National ID: ID222222
4. IMEI: 111111111111111, Phone Number: 1111111111, National ID: ID111111
5. IMEI: 123456789012345, Phone Number: 1234567890, National ID: ID123456 (STOLEN DEVICE)

Process finished with exit code 0
```

Fig. 8. Stollen Device Identification

After the system detects a stolen device, it generates an alert on the system and the law enforcement interface indicating the device's phone number, as shown in Fig 9.



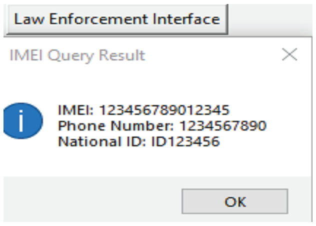
IMEI-based Device Tracking and Registration

IMEI: 123456789012345

ALERT: Device with IMEI 123456789012345 is flagged as stolen!
Phone Number: 1234567890

Fig. 9. Generated alert for stolen device

The law enforcement interface can be used to query and identify which phone number has been associated with the device again; hence, get in touch to arrest the new device owner to query how they got the device if it was reported missing, as shown in Fig 10.



IMEI: 123456789012345
Phone Number: 1234567890
National ID: ID123456

Fig. 10. Stollen Device Query Details

Law enforcement and other partners can also use the proposed system to generate a report indicating the statistics of the stolen and registered devices in the country, as shown in Fig 11.

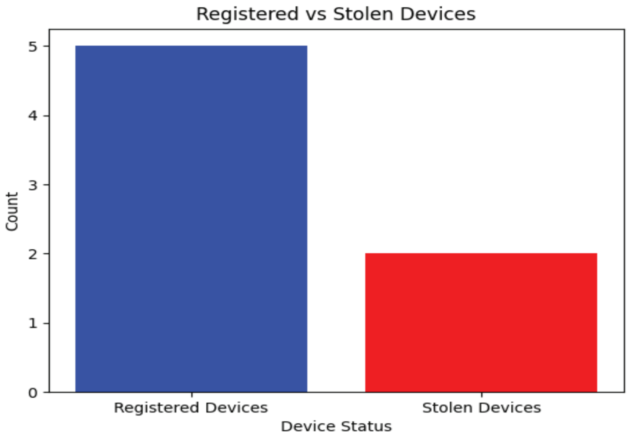


Fig. 11. Report Of Stollen Device Against The Registered Devices

V. Conclusion

The IMEI-based Mobile Device Tracking and Stolen Phone Identification System presented in this paper represents a significant advancement in mobile device security. By harnessing the unique International Mobile Equipment Identity (IMEI) associated with each mobile device, the system offers an effective approach to swiftly identifying and recovering stolen devices. Through our research and implementation, several key insights and outcomes have emerged. Firstly, device registration, involving the association of IMEI numbers with phone numbers and national IDs, is a crucial initial step. This creates a comprehensive database that forms the system's backbone, allowing for efficient real-time IMEI lookup. Integration with network service providers enhances the system's capabilities by enabling real-time communication and tracking of device connections. This collaboration streamlines identifying stolen devices when they connect to the mobile network. The device connection and IMEI lookup processes, facilitated through Python programming, showcased the effectiveness of this language in handling real-time tasks. Python's simplicity, extensive libraries, and robust threading capabilities proved invaluable in creating a responsive and efficient system. Furthermore, the collaboration with law enforcement agencies, facilitated through a secure interface, underscores the system's potential for aiding in criminal investigations and device recovery. The timely generation and management of alerts prioritize stolen device identification, further reinforcing the system's efficacy. While this system represents a substantial step towards enhancing mobile device security, several areas warrant further research and development. Future work should focus on refining the registration process, enhancing database security, and exploring AI and machine learning advancements to bolster theft detection algorithms.

References

[1] J.Degenhard, “Europe: Mobile internet users 2010-2029,” Statista,https://www.statista.com/forecasts/1145332/mobile-internet-users-in-europe.

[2] Y. Rufo, “Mobile phone stolen every six minutes in London, says met police,” BBC News. Available: https://www.bbc.com/news/uk-england-london-66442069.

[3] S.Briscoe “The problem of mobile phone theft”. NSW Bureau of Crime Statistics and Research; 2001.

[4] N.F.M. Zamri, N.M. Tahir, M.S.A.M.Ali and N.D.K. Ashar, "Snatch Theft Detection Using Deep Learning Models," Lecture Notes in Networks and Systems, vol. 559 LNNS, pp. 260–274, 2023.

[5] 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.

[6] A. A. Shaker, N. Mandela, and A. K. Agrawal, “Review on Analyzing and Detecting Crimes,” Communications in Computer and Information Science, vol. 1893 CCIS, pp. 116–127, 2023, doi: 10.1007/978-3-031-43140-1_11/COVER.

[7] "Tencent Mobile Phone Manager," http://m.qq.com/anti_theft/login.jsp.

[8] "Rising Phone Security Assistant," http://mobile.rising.com.cn/android/.

[9] L. Subramanian, G Q. M. Jr., and P. Stephanow, "An architecture to provide cloud based security services for smartphones," in proceedings of 27th Meeting of the Wireless World Research Forum, 2011.

[10] X. Yu, Z, Wang, L. Sun, W. Zhu, N. Gao, and J. Jing, "Remotely wiping sensitive data on stolen smartphones," in proceedings of the 9th ACM symposium on information, computer and communications security, 2014, pp. 537-543.

[11] S. Chang, T. Lu, and H. Song, "SmartDog: Real-Time Detection of Smartphone Theft," Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, pp. 223–228, May 2017.

[12] "Lookout Mobile Security," https://www.lookout.com

[13] http://www.ijinshan.com/hd/oneshow2012/oswebsjws.htm.

[14] "360 Guard," http://shouji.360.cn.

[15] D. Mubanda, N. Mandela, T. Mbinda, and C. Ayesiga, “Evaluating Docker Container Security through Penetration Testing: A Smart Computer Security,” 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI), pp. 415–419, Nov. 2023, doi: 10.1109/ICCSAI59793.2023.10421124.

[16] L.Simon, R. Anderson, "Security analysis of consumer-grade anti-theft solutions provided by android mobile anti-virus apps," in proceedings of the 4th Mobile Security Technologies Workshop, 2015.

[17] W. Lee and R. Lee,“Multi-sensor authentication to improve smartphone security” In Conference on Information Systems Security and Privacy ,2015, pp. 1 ‑ 11.

[18] B. Srilekha and V. Dhanakoti, “Mobile Tracking Based on Phone Theft Detection”,International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, pp. 2278-102,2016.

[19] SK. Piramu Preethika and A. Sasi Kumar, “EdTAM: Efficient Detection of Theft Android Mobile”,Indian Journal of Science and Technology, Vol 9(44),2016.

[20] S.Zahid, M.Shahzad, S.Khayam, and M. Farooq,"Keystroke-based user identification on smart phones" In International Workshop on Recent advances in intrusion detection, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 224 – 243.

[21] J. Degenhard, "Europe: Mobile internet users 2010-2029," Statista,https://www.statista.com/forecasts/1145332/mobile-internet-users-in-europe.

[22] S.J. Alsunaidi and A.M.Almuhaideb, "A strong smartphone authentication model to control cellular network access using blockchain" Wireless networks, Vol.27 No.4, pp.2301-2321, 2021.

[23] Y. Rufo, "Mobile phone stolen every six minutes in London, says met police," BBC News, https://www.bbc.com/news/uk-england-london-66442069.

[24] H.R.Arabnia, L.Deligiannidis, M.R.Grimaila, D.D. Hodson, K.Joe et al., "Advances in Parallel & Distributed Processing, and applications," In Proceedings from PDPTA'20, CSC'20, MSV'20, and GCC'20. Springer International Publishing; 2021 Oct 18.

[25] S. Shakya, K.L.Du, and K. Ntalianis, "Sentiment analysis and deep learning" In Proceedings of ICSADL 2022 pp.1

[26] D.D.Solomon, Sonia,K. Kumar, K.Kanwar, S.Iyer, "Extensive Review on the Role of Machine Learning for Multifactorial Genetic Disorders Prediction" Archives of Computational Methods in Engineering 31, no. 2 pp.623-640, 2024.

[27] M. Bhakuni, K. Kumar, Sonia, C. Iwendi and A. Singh, "Evolution and Evaluation: Sarcasm Analysis for Twitter Data Using Sentiment Analysis", Journal of Sensors, vol. 2022, pp. 10, 2022.

[28] D.D.Solomon, S.Khan, S.Garg, G.Gupta, A.Almjally, B.I.Alabduallah, H.S. Alsagri, M.M.Ibrahim, A.M.A.Abdallah, "Hybrid Majority Voting: Prediction and Classification Model for Obesity". Diagnostics Vol.13 No.15, pp.2610, 2023.

[29] J. Sharma, M. Arora, Sonia and A. Alsharef, "An illustrative study on Multi Criteria Decision Making Approach: Analytical Hierarchy Process," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 2000-2005.

[30] Suman, Sonia, R. Jasrotia,S.P. Singh, "A MCDM-based framework for selection of photovoltaic cell technology using novel information measure under Pythagorean fuzzy environment" Int. j. inf. tecnol. Vol.15, pp.4233–4242,2023.