Nigerian Journal of Technology (NIJOTECH)
Vol. 40, No. 6 November, 2021, pp1086 –1095
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
http://dx.doi.org/10.4314/njt.v40i6.11

Design of a Mobile Smartphone Anti-Theft System

O. C. Agbonifo[1], A. H. Afolayan[2, *], O. H. Akinola[3]

[1,2] Department of Information Systems, Federal University of Technology, Akure, Nigeria
[3]Department of Computer Science, Federal University of Technology, Akure, Nigeria

Abstract
This research proposed an android-based-approach for the design of a mobile smartphone anti-theft system that is fit for performing Subscriber Identity Module (SIM) card discovery, location and mobility information fetching through Global Positioning System (GPS), sending the fetched location using Short Message Service (SMS), passing culprit's mobility information to the corresponding mobile operator to provide the mobile number, capturing culprit pictures using either the camera of the stolen phone or the culprit image captured by the mobile operator and transferring the information to the alternate email id and police/appropriate authority to capture the smartphone theft culprit. The system was developed using Android Studio IDE, Java programming language, and SQLite database. The system evaluation was carried out using a survey form integrated into the developed anti-theft system. On average, more than 80% of the participants found the framework to be simple and easy to use.

Keywords: Smartphones; Anti-Theft System; Subscriber Identity Module; Global Positioning System; Short Message Service

1.0 INTRODUCTION

A smartphone is a portable personal computer with a high-level versatile working framework with highlights valuable for handheld use. The smartphone is perhaps the most esteemed possession nowadays and is turning out to be more innovatively advanced and offer a greater number of features than fixed-line telephones [1]. Smartphones can be used to make and receive voice/video calls, send and get prompt messages. It consists of digital assistants, occasion schedules, media player, computer games, geographical positioning system, front and rear camera, and, advanced camcorder. Smartphones provide the benefit of speaking with anybody virtually through video-conferencing, electronic mail, and so on. It also offers the facility to store contact numbers which decreases the idea of the file system to store individual contacts [2].

A smartphone can undoubtedly be taken and the secret information stored on the phone memory can be effectively uncovered. Smartphone theft is perhaps the most well-known criminal practice in developing nations. There are few safeguards that the users of these smartphones can take to decrease the risk of their smartphone being stolen and to that, if the most exceedingly awful occurs, the thief can't get to the private information stored on the gadget. An anti-theft system is a technique or device for preventing unauthorized access to one's assets. It helps in reducing smartphones theft and increases the chance of recovering stolen smartphones.

This research paper proposed an android-based-approach for the design of a mobile smartphone anti-theft system that is fit for performing Subscriber Identity Module (SIM) card discovery, location fetching through Global Positioning System (GPS), capturing pictures, and moving the pictures to an alternate email address, sending the fetched location to the police/appropriate authority to track the smartphone theft culprit. The rest of this research paper is organized as follows: Segment 2 examined the literature review; Segment 3 describes the anti-theft framework technique; Segment 4 contains the results and discussions of the proposed framework; lastly, Segment 5 includes conclusions of the present work and directions of future work.

2.0 LITERATURE REVIEW

A lot of researches have been carried out in the anti-theft application research area. Authors [3] developed a smart approach to track the android operating system location. The research gives an excellent outline of how google maps can be integrated with a global positioning system network for tracking smartphones by utilizing latitude and longitude values. These values were thereafter

*Corresponding author **(Tel:** +234 (0) 8034121526**)**

Email addresses: ocagbonifo@futa.edu.ng (O. C. Agbonifo), ahafolayan@futa.edu.ng (A. H. Afolayan) and olamidimejiakinola@gmail.com (O. H. Akinola)

used for locating the current location of the android device. This interaction covers the rundown of the predetermined point where users can choose their starting position by typing the name of the location and finding the range of the android device from the starting position.

Researchers [4] developed a mobile tracking framework for finding friends and acquiring signals when friends are close by using location-based services (LBS). The paper combines hybrid location schemes which integrate satellite-based and network-based signals. This system enables location tracking using the radius maintained between the devices with the help of the system administrator. This utility works in open spaces only.

In a similar study conducted by [5], a smartphone tracking application utilizing a short message service (SMS) was designed. This application assisted by approximately informing the smartphone's original owner of the new SIM number inserted by the culprit. Immediately the SIM card is changed, the application will send a message to the alternated number registered during the installation of the smartphone tracking app. In addition, the paper also proposed an advanced global positioning system device tracker which updates the stolen smartphone location at 10 minutes intervals, and anytime there is location modification, it sends an electronic mail to the smartphone owner.

Also, a location-based service application for android smartphones was developed by researchers [6]. This application retrieved smartphone locations via the smartphone provider company network or satellites. This research additionally describes various android locations application programming interfaces (API) along with location manager, location provider, and location listener. The researcher concluded that the LBS has some limitations which include the absence of spread of the wi-fi network and the hassle of network congestion in the country.

Authors in [7] designed a location-based service application for android. The application consists of different components such as map view, map activity, and location-based application programming interface. The application also supports a multi-layer overlay that enables users to draw coordinates, capture photos, and strings on the map. The map view uses the file system and the networks in the application background. The map view is set up by the map activity. The activity life cycle maintains and controls all the threads in the application.

An android-based anti-theft system was developed by [8]. The system utilizes different services like multimedia messaging services as opposed to short messaging services. The system depends on the hardware of the Android-based smartphone such as cameras and its support for multimedia messages. The application works in the device background by storing the new SIM number in a variable and unceasingly checking for SIM changes. Each time SIM gets changed on the mobile device, the software takes snapshots and document a video at that instance and then sends an MMS including the snapshots to an alternate mobile number and the electronic mail provided during set up. This application is limited because it can only work when there is internet connectivity.

Similarly, research by [9] developed a mobile terminal anti-theft tracking system for android smartphones. The application automatically destroys secluded information and also tracks stolen smartphone locations. In this paper SMS and backstage monitoring, technologies are used to implement the remote SMS management function of the anti-theft tracking system. The system has three modules to enhance its functionality; they are the software parameter protection module, self-startup module, and SMS encryption module. The application did not only own a basic anti-theft function for automatically removing sensitive information, it additionally monitored the stolen or misplaced mobile phone silently using GPS.

Researchers [10] developed an anti-theft application for android phones. The purpose behind developing this project is to help users track their lost or misplace devices. The developed software permits simple commands that will assist the user to get hold of the smartphone's GPS location information through the friend's mobile phone URL. Also, the camera of the phone works in the background without knowing the culprit and records the culprit video as well as the captured pictures and sends this information to the actual owner.

Rekha et al. [11] developed teledroid anti-theft application for android devices. The android-based application is installed with preliminary registration of user mobile number, alternative mobile number, user passcode, and email identity. The software runs within the background of the android device. It has a platform for monitoring the present location of the mobile phone via GPS. Anytime the culprit changes the SIM card, instantly the SIM details, latitude, and longitude of the location will be sent to the alternate mobile phone number provided by the user during installation. The contacts and crucial files on the lost smartphone may be retrieved via e-mail and the file switch facility that is available in the application. The research is limited because the application can only work if the lost phone is switched on.

Research by [12] developed a system that routinely detects pickpocket and grab-and-run theft in which the thief grabs the smartphone from a victims' hands and runs away. There was an underline factor concerning smartphone screen locking mechanisms that users refuse to enable this operation on their devices because it takes a long time to unlock the devices and this also puts the victims' personal information at high risk when such devices are stolen. The system was intelligently built to support a drastic decrease in the number of periods a user is asked to provide a lock code. The system also warns smartphone users of PINs or passcodes only when theft occasions had been detected.

Arunkumar et al. [13] developed an android anti-theft mobile application with GPS Tracker and image acquisition. The researchers proposed an autonomous system that communicates with the owner via email and SMS when it detects SIM change. The application also sends the culprit's image and his location to the alternative email-id. This application was interconnected using GPS functionalities for the mobile tracking process. The application did not provide information about the location of the android-based smartphone via SMS.

Researchers [14] proposed a hardware-based anti-theft system for smartphones. The actual chip is embedded into the smartphone which can be accessed anytime by the user to track the smartphone even after the phone is reset and also provide support for remotely erasing the data stored, hence data integrity is achieved and the data is not stolen. The chip can communicate with the GPS sensor in the mobile and will provide the GPS location of the smartphone in real-time. The chip also has dedicated storage where users can store important information and confidential data that can be secured and can access it anytime. In future work, the researchers planned to expand the implementation to laptops.

An anti-theft application for android based devices to find stolen or lost devices through the use of sensors, cameras, and email was presented by [15]. Upon installation, the application works in the background and collects data from the sensors. This will alert the user by sending a message to the email that was provided during installation. This data will help users to find the stolen or lost device. For future work, the researchers emphasized the need for more sensors, video recordings, and location trackers.

Authors in [16] developed a Chaperone application. This application helps in detecting the owner's departure from the phone using active acoustic sensing. It provides an effective loss prevention solution by locking the phone immediately and alerting the owner before they leave without the phone. It does not require additional hardware. Chaperone uses active acoustic sensing to keep track of the user's movement via the built-in speaker and microphone. Chaperone consists of an acoustic signal generator, an audio manager that controls the speaker and the microphone, and a signal processor. Chaperone targets nearby opportunistic attackers, not Chaperone-aware active attackers. Phone lost through pickpocketing and snatching are not considered.

Machine Learning (ML) and Short Message Services (SMS) remote access-based model for protecting android devices from theft was developed by researchers [17]. The SVM-RBF model was trained on a feature-set extracted from the inertial sensor's data. The striking feature of this system is minimal configuration without interfering with human-assisted tasks. The researchers recommended that in future research work, elaborate methods can be applied to the training efficiency factor to get more efficient values. The research is limited because the system can only work when connected to the internet.

Adam et al. [18] analyzed some security difficulties and benefits delivered by mobile phone tracking innovations, particularly in selling and buying used handsets. The authors reviewed anti-theft and mobile tracking innovations literature to create guidance and make mindfulness for mobile phone owners as well as retailers. The researchers additionally referenced a few cases that might emerge due to smartphone theft, and some of these cases for instance may involve the police, who will carry out investigations to capture the culprits. In some of these scenarios, the incapability of the claimants to provide details that will enhance the police investigations might lead to guiltless individuals or people being erroneously caught as the offender. The research only reviewed related works; implementation of the anti-theft system was not carried out.

Researchers in [19] implemented an anti-theft vehicle tracking system that utilizes low-cost and dependable modules technology. The system is based on IoT services that consist of microcontrollers that can track vehicles in real-time, control the vehicles remotely when stolen by sending SMS to stop vehicle fuel line by relay, and thereafter notify the nearby police station in a short period using the haversine formulae by comparing the last coordinate received from the vehicle with coordinates of police stations. The anti-theft vehicle tracking system consists of two modules; the embedded system and the web application. The embedded system is placed in a hidden location in the vehicle that is unknown to the culprits. This module comprises the GPS, GSM, GPRS, relay, and microcontroller. To track the anti-theft vehicle, the GPS is used for retrieving the current location of the vehicle; the GSM/GPRS module for sending data to the host server to track the vehicle location in real-time via google map that is embedded within the application. The host server is used for transmitting data between the embedded system and web application. To improve on existing methods, the researcher equipped the proposed system with rechargeable batteries to ensure continuous operation even when the vehicle battery has been disconnected. The researchers concluded that the system could be improved to capture user authentication to turn on the vehicle.

Authors in [20] developed an IoT-based participatory anti-theft system for enhancing public safety in smart cities. In the developed system, Bluetooth Low Energy (BLE) is employed in tracing stolen assets. Anytime an asset is stolen, the owner informs the authorities in charge of the smart cities, which, thereafter broadcasts an alert signal to activate the BLE sensor. To trace the stolen object, the authorities use their GPS-enabled smartphones to scan the BLE tags through a specific smartphone client application and report the location of the stolen object to an operation center where asset owners can thereafter collect their missing assets.

Research by [21] developed a mobile anti-theft software. The mobile anti-theft helps users to find their device when lost using SMS commands without paying for any service in a cost-efficient manner. This app can work in offline mode, get precise location, detect SIM SWAP, and send the message to user emergency mobile number immediately. In this research work, if the user wants to capture the face of the intruder, then the user can use the capture command to capture both the front and back camera and save it to Google Drive, and the drive link will be shared through email or using SMS. This research had limitations since the intruder might hack into the phone owners' email addresses and reset the password to prevent the rightful owner from accessing the email.

Today's smartphones offer lots of capabilities like personal computers. Since smartphones are becoming smaller in size, they can easily be misplaced and stolen without the owner's knowledge and exclusive information stored on the phone memory can easily be uncovered. Finding such smartphones will become the owners' priority. Some of the existing anti-theft control applications are available at a price while other applications with viewer features are free. Some of the anti-theft applications could send GPS coordinates and SIM card details of the culprit via SMS, some applications could just send snapshots of the culprit via multimedia messaging service. Due to the limitation of the existing applications, there is a need for a more complete and robust anti-theft control application.

3.0 RESEARCH METHODOLOGY

The Anti-theft system is composed of objects that relate together to achieve the goal of the system. The objects include a Subscriber Identity Module (SIM) card, Mobile phone, Database, Mobile camera, and Global Positioning System (GPS). The proposed anti-theft application is loaded with features like SIM card discovery, location fetching through GPS, capturing pictures and moving the pictures to an alternative email address, sending the fetched location utilizing Short Message Service (SMS) on the off chance that there is no web network and tracking of the smartphone enrolled on the application. The framework of the Anti-theft system is illustrated in Figure 1.

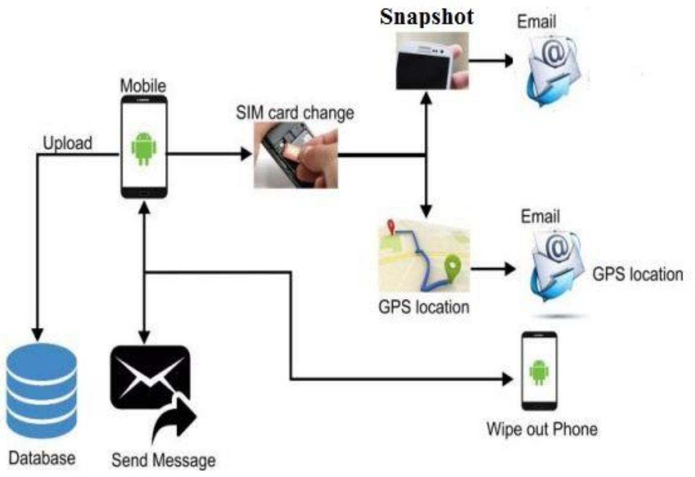


Figure 1: The Anti-Theft Android-Based Framework

The proposed anti-theft android-based application is installed with the registration of user mobile number, an alternate mobile number that is not stored on the smartphone, user password, email identity, and alternate email id. The users' details are stored in the database of the anti-theft application. Thereafter, the user is directed to activate anti-theft security features and the application continues to work in the background without interrupting users' activities.

Three methods were adopted to track the location and identify the smartphone theft culprit. The first approach uses the SIM card unique number to identify an unauthorized user. Short Message Service (SMS) alert is sent to the alternate phone number which is not in the device anytime the SIM card is changed and there is a mismatch between the new SIM card unique number and the previous SIM card unique number. This is done with the help of the Integrated Circuit Card ID (ICCID) immediately after the owner of the smartphone reports the theft on the web board of the application.

The second approach uses GPS to track the location of the stolen smartphone using the smartphone's unique International Mobile Equipment Identity (IMEI) number. The location of the stolen smartphone will be sent to the alternative email-id provided by the user during registration. The user would have been instructed not to open this alternative email-id using the smartphone. Also, the culprit's mobility information (latitude and longitude) will be passed to the corresponding mobile operator to provide the mobile number of the culprit within a given distance. The police or the appropriate authority can thereafter use the

location information sent to the user alternate email or use the culprit's mobile number to track
the smartphone or the smartphone theft culprit.

The third approach captures the images of the culprit using either the front and rear camera of the stolen phone. The captured image is sent to the user alternate registered email-id or uses the image of the culprit captured by the mobile operator during SIM card registration. The fetched location, culprit mobile number, and captured images will then be sent to police/appropriate authority to capture the smartphone theft culprit.

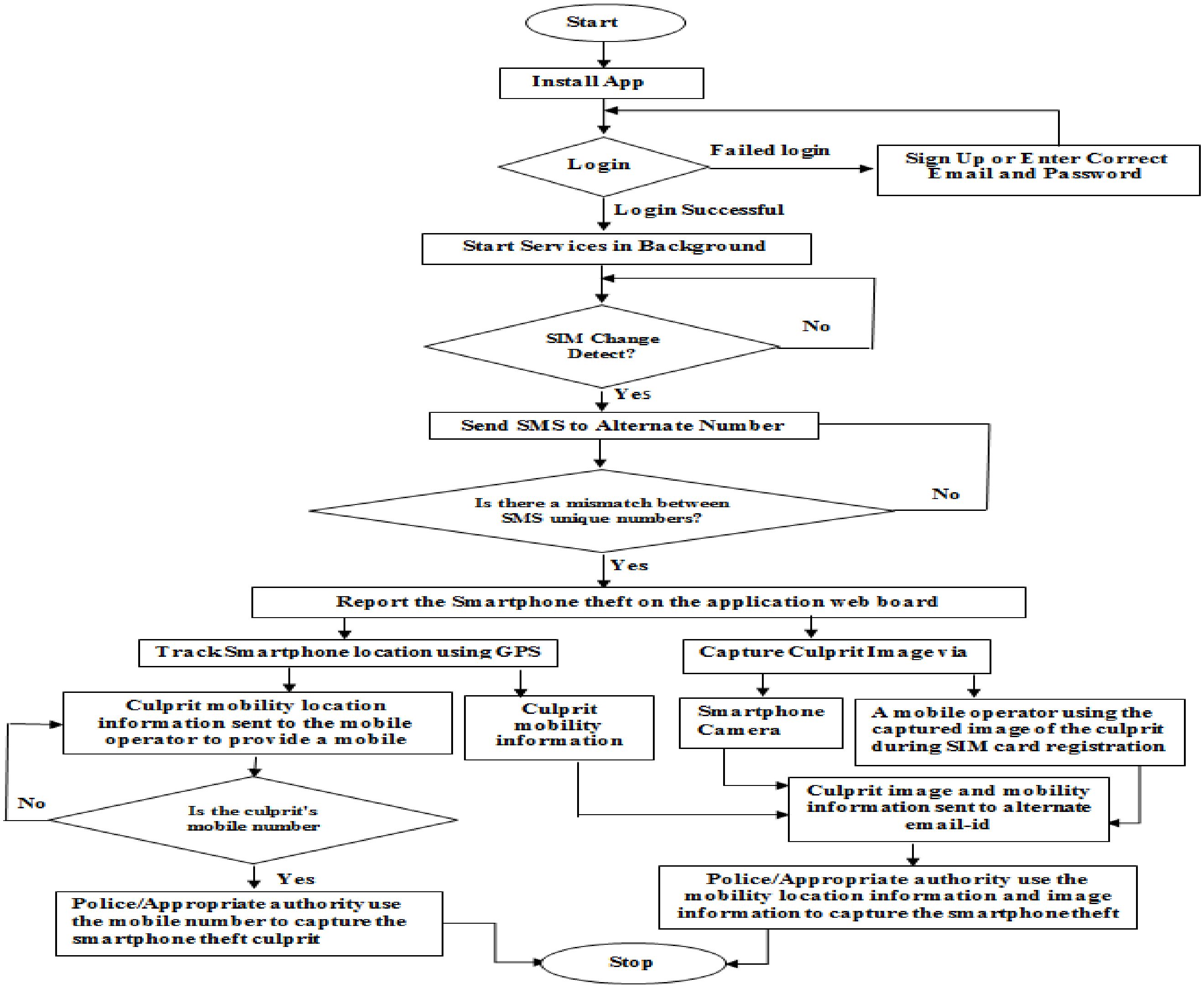

Start
Install App
Login
Failed login
Sign Up or Enter Correct Email and Password
Login Successful
Start Services in Background
SIM Change Detect?
No
Yes
Send SMS to Alternate Number
Is there a mismatch between SMS unique numbers?
No
Yes
Report the Smartphone theft on the application web board
Track Smartphone location using GPS
Capture Culprit Image via
Culprit mobility location information sent to the mobile operator to provide a mobile
Culprit mobility information
Smartphone Camera
A mobile operator using the captured image of the culprit during SIM card registration
No
Is the culprit's mobile number
Culprit image and mobility information sent to alternate email-id
Yes
Police/Appropriate authority use the mobile number to capture the smartphone theft culprit
Police/Appropriate authority use the mobility location information and image information to capture the smartphonetheft
Stop

Figure 2: Flow Diagram of the Anti-theft System

3.1 Haversine Algorithm

The haversine formula is a very accurate way of computing distances between two points on the surface of a sphere. In this research work, the Haversine algorithm is adopted for computing the shortest distance between two geographical locations using GPS coordinates. The input of this method is the latitude and longitude. The output is the value of the distance between the two locations (the remote app used for tracking the stolen smartphone and the stolen smartphone).

Given that radius of the sphere (r), longitudes $long1$, $long2$ of both points $p1$ and $p2$, latitudes $lat1, lat2$ of both points $p1$ and $p2$, distance (d) between two points $p1$ and $p2$. This can be illustrated with the following notations:

r = radius of the sphere; $lat1$ = latitude of point 1; $lat2$ = latitude of point 2;
$long1$ = latitude of point 1; $long2$ = latitude of point 2

$$a = \sin^2(\frac{lat2 - lat1}{2}) + \cos(lat1)\cos(lat2) \times \sin^2\left(\frac{long2 - long2}{2}\right) \quad (1)$$

$$c = 2 * a * tan2\big(sqrt(a) * sqrt\ (1 - a)\big) \quad (2)$$

$$d = r * c \quad (3)$$

where d is the distance between the two points; r is the radius of the sphere; c is the angular distance in radians and; a is the square of half the chord length between the points.

For any two points on a sphere, the haversine of the central angle between them is given by:

$$haversin\ \left(\frac{d}{r}\right) = haversine\ (\emptyset_2 - \emptyset_1) + c \quad (4)$$

where $haversin$ is the haversine function, d/r is the central angle and $\emptyset_1, \emptyset_2$ is the latitude of points $p1$ and $p2$

$$haver\sin(\theta) = sin^2\left(\frac{\theta}{2}\right) = \frac{1 - \cos(\theta)}{2} \quad (5)$$

3.2 *The Anti-theft System Implementation*

The Android application for the Anti-theft was developed using Android Studio IDE. The front-end designs were done using java programming language and the data from the front end were stored in SQLite database at the backend using a server-side scripting language (PHP) and the objects were wrapped using JSON. The application was deployed on an android smartphone environment.

3.2.1 Use Case Diagram

The use case diagram for the mobile smartphone anti-theft is given in Figure 3. It describes how the authorized user registers his/her details (which includes name, email, and password) and log in. The system then requires the authorized user to enter an alternate number which will receive SMS notification upon registration and SIM change. Also, the authorized user receives a report which contains GPS coordinates and snapshots in his/her registered email address. The authorized user can also remotely report his/her smartphone being missing by logging in to a remote website (panel.preyprojects.com) with their anti-theft account details.

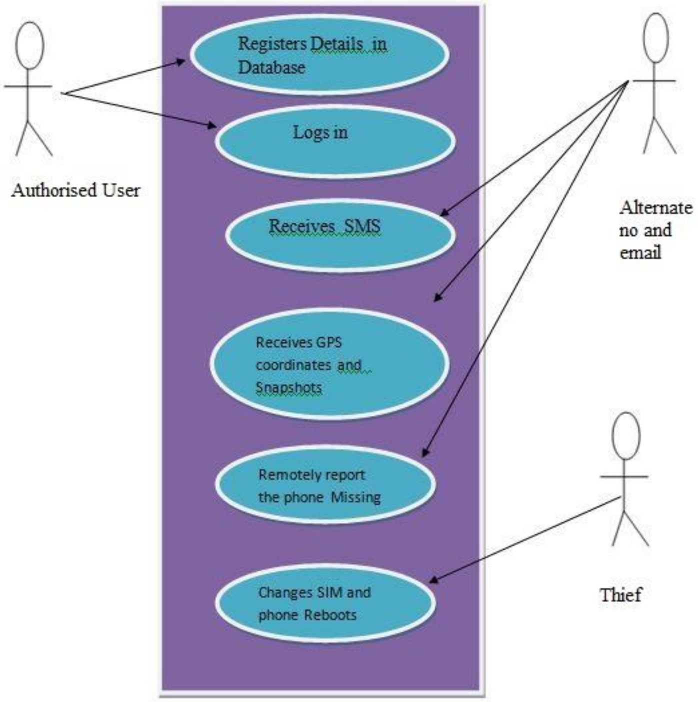

Registers Details in Database
Logs in
Receives SMS
Receives GPS coordinates and Snapshots
Remotely report the phone Missing
Changes SIM and phone Reboots
Authorised User
Alternate no and email
Thief

Figure 3: Use Case Diagram of Mobile Smartphone Anti-Theft System

3.2.2 Entity Relationship Diagram

The Entity-Relationship Diagram (ERD) shows the information created, stored, and used by the mobile smartphone anti-theft system. The system has three main components namely entities, attributes, and relationships. The entities in the mobile smartphone anti-theft system include the authorized user/owner, the theft, the mobile device, the alternative number, and the subscriber identification module. The entity ‘owner' has the following attributes: owner_id, IMSI, alternative number, owner name, email, and password. The entity 'theft' has the following attributes: IMSI, and GPS coordinates. The entity ‘mobile device' has the following attributes: type, model, and display. The entity ‘alternative number’ has the following attributes: name, location, and model. The entity 'SIM' has the following attributes: IMSI, service provider, and operator name. The relationships between these entities are as follows: a potential user/owner has n mobile device and n alternative number that has SIM came across a thief that stole the smartphone device, unknown to the thief that the mobile device is being monitored by GPS co-ordinates and IMSI. The relationship between the entities is shown in Figure 4.

4.0 RESULTS AND DISCUSSION

The documentation for the implementation of the android application for the anti-theft, the user interface design for the implementation, the performance evaluation, critical analysis of the developed system, and analysis of the result obtained are presented in this phase.

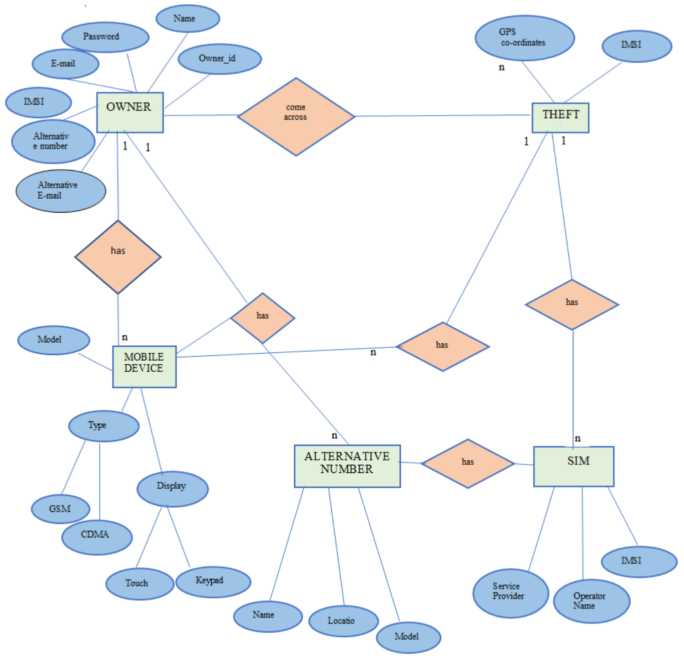
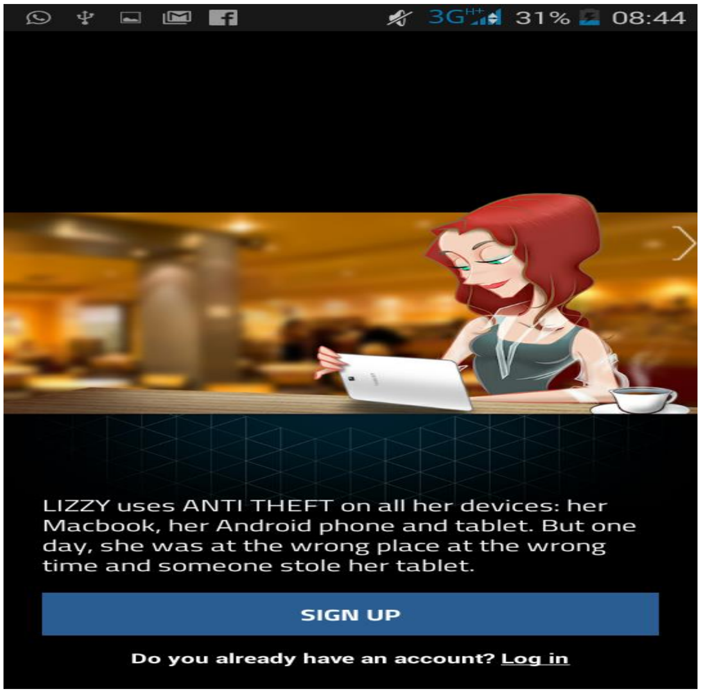


Figure 4: Entity-Relationship diagram for the Smartphone Anti-theft System

4.1. *Search Results*

The application is installed on an Android Smartphone, thereafter, the user sign-up via the home page as shown in Figure 5, from where the user is directed to the signup page where he/she register by supplying his/her name, email, and password. Figure 6. depicted the sign-up page. After creating an account, the user is required to submit an alternate number that is not in the device to receive an SMS notification anytime the SIM card is changed and there is a mismatch between the new SIM card unique number and the previous SIM card unique number. The alternative number page is shown in Figure 7. Thereafter, the user is directed to activate anti-theft security features and the application continues to work in the background without interrupting users' activities. The administration page is depicted in Figure 8. Once there is an occurrence of a stolen smartphone, the user begins to receive any reports on his/her alternative mailbox which is not in the device. The reports include a map showing the location of the device and the GPS location in terms of longitude and latitude, mobility information, and culprit image. Also, the culprit's mobility information (latitude and longitude) will be passed to the corresponding mobile operator to provide the mobile number of the culprit within a given distance. The police or the appropriate authority can thereafter use the location information sent to the user's alternate email or use the culprit's mobile number to track the smartphone or the culprit. The missing device report page is depicted in Figure 9. The device camera (primary and secondary) takes snapshots and the anti-theft application generates a list of wireless networks where the device is and sends a report to the user's alternative email. The camera and wireless network reports are shown in Figure 10.



LIZZY uses ANTI THEFT on all her devices: her Macbook, her Android phone and tablet. But one day, she was at the wrong place at the wrong time and someone stole her tablet.

Figure 5: Home Page

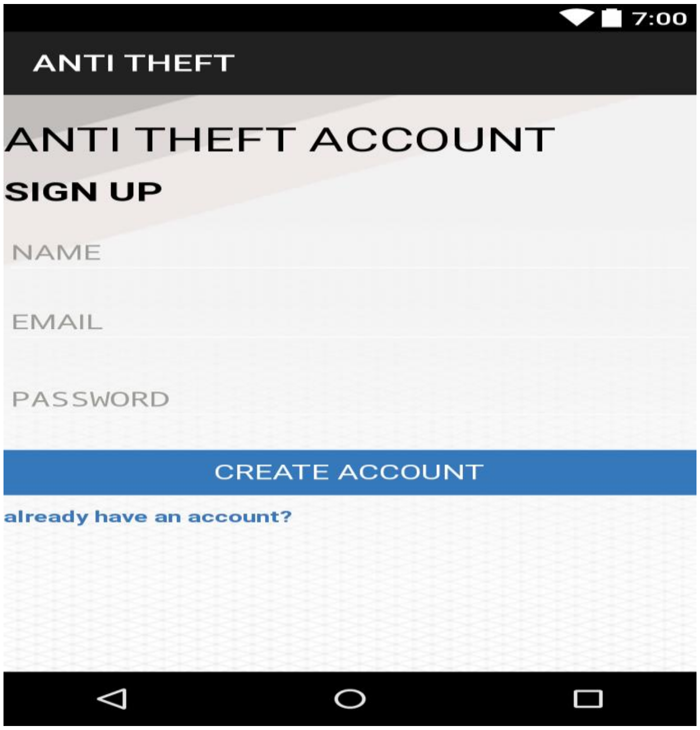
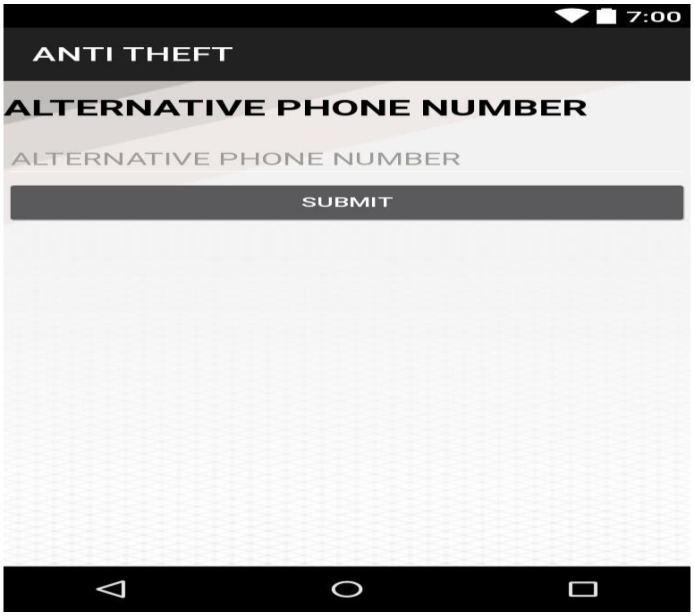


Figure 6: Sign Up Page



7:00

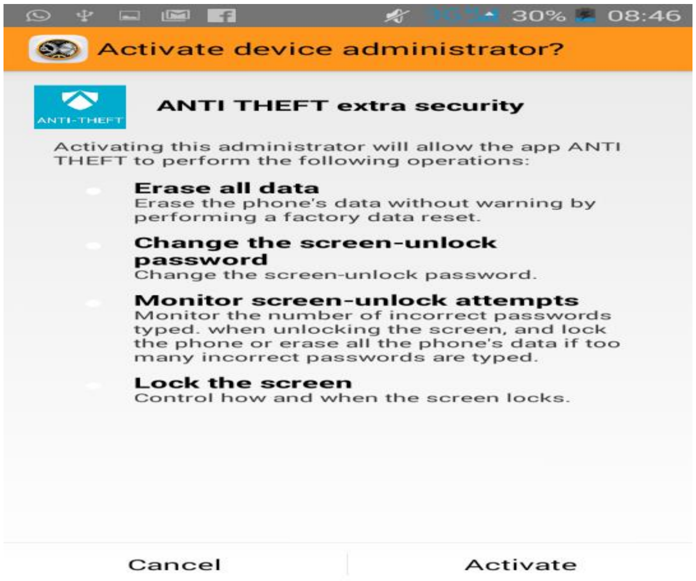
ANTI THEFT

ALTERNATIVE PHONE NUMBER

ALTERNATIVE PHONE NUMBER

SUBMIT

`**Figure 7:** Alternative Number Page



30% 08:46

Activate device administrator?

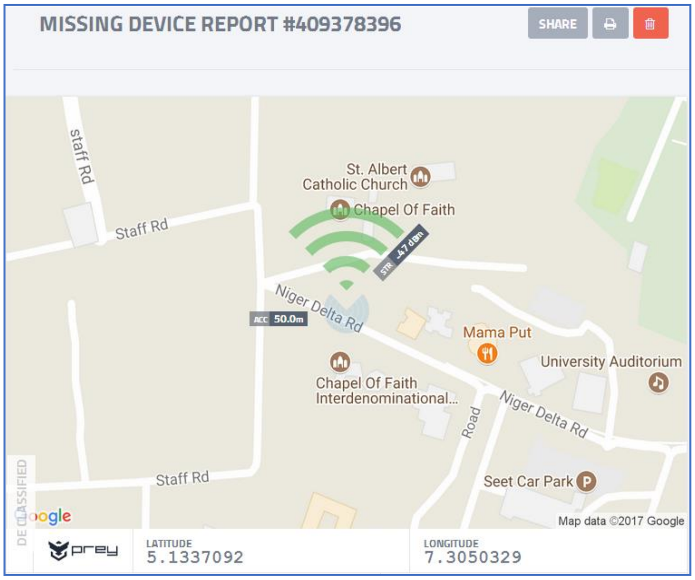
ANTI THEFT extra security

Activating this administrator will allow the app ANTI THEFT to perform the following operations:

- **Erase all data**
  Erase the phone's data without warning by performing a factory data reset.
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed. when unlocking the screen, and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.

Cancel | Activate

Figure 8: Anti-theft Security Administration Page

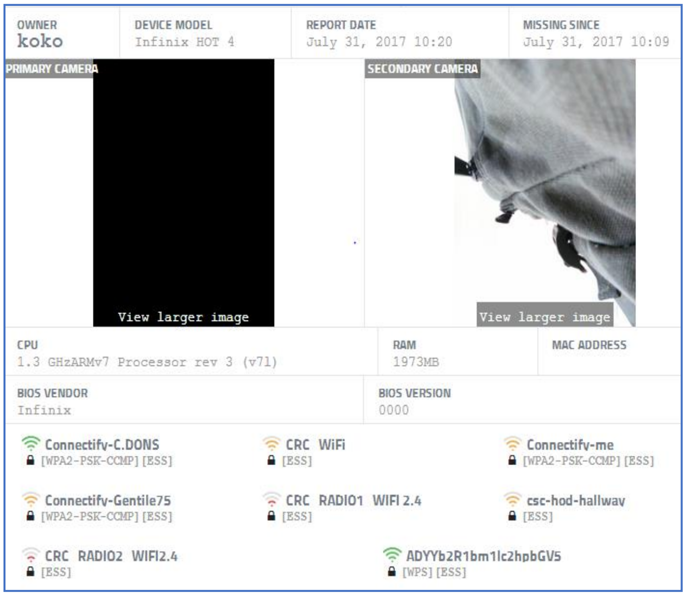


MISSING DEVICE REPORT #409378396

LATITUDE
5.1337092

LONGITUDE
7.3050329

Figure 9: Missing Device Reports of a User (Map Data)



OWNER	DEVICE MODEL	REPORT DATE	MISSING SINCE
koko	Infinix HOT 4	July 31, 2017 10:20	July 31, 2017 10:09

CPU	RAM	MAC ADDRESS
1.3 GHzARMv7 Processor rev 3 (v71)	1973MB	

BIOS VENDOR	BIOS VERSION
Infinix	0000

Connectifv-C.DONS [WPA2-PSK-CCMP] [ESS]
CRC WiFi [ESS]
Connectifv-me [WPA2-PSK-CCMP] [ESS]
Connectifv-Gentile75 [WPA2-PSK-CCMP] [ESS]
CRC RADIO1 WIFI 2.4 [ESS]
csc-hod-hallwav [ESS]
CRC RADIO2 WIFI2.4 [ESS]
ADYYb2R1bm1lc2hpbGV5 [WPS] [ESS]

Figure 10: Camera and Wireless Network Reports

Comparing these results findings with the existing results reported in the literature. This application overcomes one of the drawbacks of Google’s “Find My Device” which enables device owners to secure or recover a lost device, but they can only work in an online mode. This research improves on [11], [13], and [21] which had limitations in relying only on sending SMS commands, location fetching using GPS, and sending commands to email in tracking smartphones. This research includes sending mobility information to the mobile operator to provide the culprit's mobile number and captured image during SIM registration. This anti-theft system is fit for performing SIM card discovery by sending an SMS alert to the registered alternate phone number which is not in the device anytime the SIM card is changed and there is a mismatch between the new SIM card unique number and the previous SIM card unique number. Location and mobility information fetching through GPS, sending the fetched location by means SMS on the off chance that there is no web network and passing culprit’s mobility information to the corresponding mobile operator to provide the mobile number of the culprit within a given distance. Capturing culprit pictures using either the front and rear camera of the stolen phone or using the culprit image captured by the mobile operator during SIM card registration and sending the images to the user alternate registered email-id. Tracking the smartphone and the culprit by the police or the appropriate authority using the culprit mobile number and images.

4.2. System Evaluation and Testing

The anti-theft application was tested within and outside the Federal University of Technology, Akure environment. There were a total number of 105 users (students and others) that participated in the survey. The application was installed on their smartphones and they all registered with their details. The metrics used for the evaluation of the system are ease of use, accuracy, responsiveness, and novelty of the system's ability to detect theft. The participants answered the survey for each metric on a scale of five, four, three, two, and one. Five means "Excellent", Four means "Very Good", Three means "Good", Two means "Average" and one means "Fair". Table 1 shows the summary of users' responses to the online survey.

Table 1: Summary of Users' Responses to Online Survey

S/N	Question Item	Excellent	Very Good	Good	Average	Fair
1	Was the application easy to access by you?	12 (11.43%)	72 (68.57%)	17 (16.19%)	2 (1.91%)	2 (1.91%)
2	Was the application accurate and free of errors?	49 (46.67%)	46 (43.81%)	6 (5.71%)	3 (2.86%)	1 (0.95%)
3	How does the application respond to your inputs?	55 (52.38%)	42 (40%)	5 (4.76%)	2 (1.91%)	1 (0.95%)
4	How would you rate the system's ability to detect a theft?	47 (44.76%)	50 (47.62%)	4 (3.81%)	2 (1.91%)	2 (1.91%)

According to the results in Table 1, 11.43% of the participants rated the system's ease of use to be excellent. the system's ease of use metric got the first-highest percentage of "very good" rating in the survey, which is 68.57%. 16.19% rated it to be good while 1.91% rated it to be average and fair respectively. 46.67% of the participants rated the system's accuracy to be excellent. 43.81% rated it to be very good, while 5.71%, 2.86%, and 0.95% rated the system’s accuracy to be "Good", "Average", and "Fair" respectively. The system responsiveness metric got the second-highest percentage of "excellent" rating in the survey, which is 52.38%. 40% rated it to be very good, 4.76% rated it to be good while 1.91%, 0.95% rated it to be average and fair respectively. The last metric measures the novelty of the system's ability to detect theft. The system's novelty got 44.76% of the excellent rating. 47.62% t of the participants believe the novelty to be very good. 3.81% of the participants found the system’s novelty to be good, 1.91% to be average and 1.91% considered it to be fair. Altogether, an exceptionally huge extent of participants found the novelty of the system to be good. According to these results, the system found very high usability, with high accuracy. It also performed very well at providing required results to users, as the majority of the users rated it well in this regard. Also, the system rated fairly high in detecting mobile theft (previously unknown) theft to users. The results call for the need for more intelligent systems to serve this purpose in the future.

5.0 CONCLUSION AND RECOMMENDATION

Theft is one of the most extremely typical and most established criminal practices. At the point when there is no means of identification, people might claim objects to their advantage to the detriment of the original owner. This research paper established a cost-effective and user-friendly android-based anti-theft system that can help in recovering stolen or misplaced smartphones. The anti-theft system can identify SIM cards mismatch using the SIM unique number, location, and mobility information fetching through GPS, sending the fetched location by means SMS on the off chance that there is no web network and passing culprit’s mobility information to the corresponding mobile operator to provide the mobile number of the culprit within a given distance, captures the culprit pictures using either the front and rear camera of the stolen phone or uses the culprit image captured by the mobile operator during SIM card registration and transfer the images to the user alternate email address, which will be used by the police and the appropriate authority to track the smartphone and the culprit.

The system evaluation was carried out using an online survey form attached to the developed system. The metrics considered are ease of use, accuracy, responsiveness, and novelty of the system's ability to detect theft. 11.43% of the participants found the anti-theft system very easy to understand, 68.57%, 16.19% of the participants rated the system to be "Very Good" and "Good" respectively. Few percentages of the participants rated the system average and fair. Although system evaluation revealed that the system can perfectly detect smartphone theft, further research can attempt to integrate more security features into the application. Also, the application will not work if the lost smartphone gets switched off.

REFERENCES

[1] Sonia, C.V. and Aswatha, A.R. “AALTm: An Android Application to Locate and Track Mobile Phones”, *International Journal of Engineering Trends and Technology*, 4(5), 2013, pp. 1-8.

[2] Sharmila, K. and Sivasankari, A. “Smart Theft Alert for Android-Based Devices”, *International Journal of Computer Techniques*, 3(4), 2016, pp. 1-6.

[3] Muthumurugesan, D. Nalini, S. and Vinodini, R. “Smart Way to Track the Location in Android Operating System”, *IOSR Journal of Computer Engineering*, 12(4), 2013, pp. 27-32.

[4] Jayashree, J., Nirupama, K., Vijayashree, J. and Anish, K.F. “Mobile Tracking Application for Locating Friends using LBS”, *International Journal of Engineering Science and Technology*, 1(2), 2013, pp. 1-6.

[5] Mondal, A., Masud, A., Biswas, N.K. and Sarder, E. “Smartphone Tracking Application using SMS service”, *International Journal of Electronics, Electrical, and Computational System*, 2(4), 2013, pp. 1-7.

[6] V. Seema, K. Unmesh, S. Ganesh, and P. Pradynesh, “Location-Based Services on Smart Phone through the Android Application”, *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 1, pp. 1-6, 2014.

[7] Shu, X., Du, Z. and Chen, R. "Research on Mobile Location Service Design Based on Android," in 5th International Conference on Wireless Communications, Networking and Mobile Computing, October 2009, pp. 1-4.

[8] Khan, A. U. S., Qureshi, M. N. and Qadeer, M. A. “Anti-Theft Application for Android-Based Devices,” in IEEE International Advance Computing Conference (IACC), 2014, pp. 365-369.

[9] Luo, Y., Wang, J. and Feng, C. “Design and implementation of mobile terminal anti-theft tracking system based on Android platform,” in 2nd International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII), 2016, pp. 506-512.

[10] Deore, S. Khodade, K. and Patil, S. “Anti-Theft Application for Lost or Misplaced Android Phones”, *International Journal for Innovative Research in Multidisciplinary*, 3(4), 2017, pp. 224-231.

[11] Rekha, R., Sahana, B., Sahana, V.P. Shamitha, A., and Chaithra, “Teledroid Anti-Theft Application for Android Devices”, *Advances in Computing*, 7(2), 2017, pp. 44-47.

[12] Xinyu, L. David, W. and Serge, E. “Detecting Phone Theft Using Machine Learning”. Proceedings of the International Conference on Information Science and System, 2018, pp. 30-36.

[13] Arunkumar, R., Logaprakash, M. and Shajini, J.J. “Android Anti-Theft Mobile Application with GPS Tracker and Image Acquisition”, *International Journal of Management, Technology, and Engineering*, 8(X), 2018, pp. 1689-1696.

[14] El-Fiorenza, J.C., Udayakumar, D., Rajah, C. and Karthikeyan, M. “Hardware-Based Anti-Theft System for Smartphones”, *International Journal of Recent Technology and Engineering*, 7(5C), 2019, pp. 171-174.

[15] Shetty, A. and Trivedi, A. “Anti-Theft Application for Android-Based Devices”, *International Journal of Research and Analytical Reviews*, 6(1), 2019, pp. 11-13.

[16] Chen, J. Hengartner, U. Khan, H. and Mannan, M. “Chaperone: Real-time Locking and Loss Prevention for Smartphones,” in Proceedings of the 29th USENIX Security Symposium, August 12–14, 2020, pp.325-342.

[17] Sawant, T., Shah, D., Sontakke, S. and Gunjgur, P. “An ML and SMS remote access-based model for Anti-theft protection of Android devices,” in ITM Web of Conferences, 2020, pp. 1-6.

[18] Adam, I.Y., Varol, C. and Varol, A. “Problems and Prospects of Anti-Theft and Mobile Phone Tracking: A case in Nigeria,” in 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-5.

[19] Ali, A.S., Hasan, A.H. and Lafta, H.A. “Antitheft Vehicle Tracking and Control System Based IoT”, *Journal of Critical Reviews*, 7(9), 2020, pp. 88-92.

[20] Papadakis, N., Koukoulas, N., Christakis, I., Stavrakas, I. and Kandris, D. “An IoT-Based Participatory Antitheft System for Public Safety Enhancement in Smart Cities”, *Smart Cities*, 4(2), 2021, pp. 919–937.

[21] Rajkumar, M., Rani, P.S., Yasin, S.M. Rakesh, K. and Vignesh, S. “Mobile Anti-theft Software (MATS)”. [Online]. 11(2), 2021, pp. 665-675.