IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Geofencing Location Tracking

Prashant Raut, Jay Gosavi, Vishal Gangavane, Parikshit Kathe, Sachin Hissal
Sinhgad Institute of Technology, Lonavala, Pune, Maharashtra, India

Abstract: *Mobile phone vulnerability has expanded along with mobile phone usage, which has dramatically increased. Android cell phones come in a range of prices and appeal to a wide audience. It has become crucial to protect people's sensitive and confidential data. There are numerous methods for protecting Android cell phones. There are numerous techniques available, including the GPS tracking system, image capture, password security, and more*

Keywords: GPS Tracking, Image capture, Password Changing, SIM Detection.

I. INTRODUCTION

This software is used to locate a lost mobile. It manages the user's new registration using their name and alternate phone number in order to gain access. When the phone is turned on, a picture of the owner is automatically taken. This application is used to report a device's location. The application will immediately send geographic location information to the original user's alternate phone number in the event that an Android has been stolen and the mugger switches the SIM card already registered with it. This research report tracks both the stolen phone with the original SIM card and the stolen phone with a new SIM card on a regular basis. The stolen mobile sends an SMS alert to the registered mobile number. This procedure serves as a real-time tracking mechanism for android mobile devices.

II. PROPOSED WORK

System Architecture

A. Detection of Stolen Mobiles

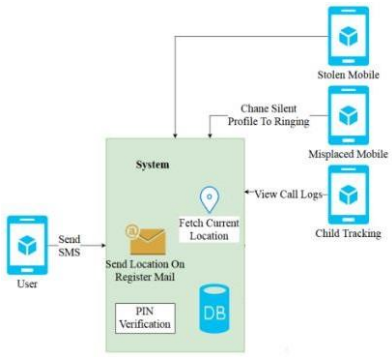
In this scenario, the user will send an SMS in a predetermined format and with a PIN using the stolen mobile device. The device will retrieve the present position and take pictures with the front and rear cameras. The registered email address is then supplied this information.

B. Mobile Device Missing Detection

In this scenario, the user will send an SMS with a PIN in a predetermined format from a lost mobile device. The system will switch from a silent to a general profile, get the current location, and take pictures with both the front and rear cameras. The registered email addresses are then supplied this information.

C. Child Tracker

In this scenario, the parent will send an SMS containing a PIN in a predetermined format to the child's mobile device. The device will retrieve the current location and use the front and rear cameras to take pictures. The registration email address then receives this information. Parents can view their children's phone logs as well.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

III. SOFTWARE MODEL

In addition to location tracking, the suggested software architecture offers a number of other features that increase the tracking process' efficacy and efficiency.
The following features have been added:

1) GPS location monitoring

The U.S. Department of Defense sent 24 satellites into orbit to form the Global Positioning System (GPS), a satellite-based navigation system. Despite being used for a wide range of purposes today, GPS was initially developed for military usage. GPS usage is free of setup or subscription costs. The accuracy of modern GPS receivers is astounding, typically within 15 metres [4].
We are utilising GPS functionality in this software to correctly pinpoint the position of the stolen smartphone by taking advantage of this accuracy. The GPS receivers in the user segment, like the ones built into the majority of smartphones today, pick up those signals and can use a minimum of four signals to derive a three-dimensional location based on those signals.

2) Monitoring location via a network provider Network-based methods make use of the network architecture of the service provider to pinpoint the handset. From the perspective of a mobile operator, the benefit of network-based approaches is that they may be applied without interfering with the phones. The quantity of base station cells also affects how accurate network- based approaches are [5]. The location is determined by the Network Provider based on the presence of cell towers and WiFi access points, and the information is received using a network lookup. Due to its poor precision, position monitoring through a network provider is not recommended, but there is no harm in utilising it in addition to GPS as a tracking method [6]. Similar to WiFi positioning, cellular network positioning (Cell-Id positioning) makes use of a base station's unique identification made up of the mobile network code, mobile country code, cell tower identifier, and geographical area identifier (LAI). Unique identifiers must be connected to a positional reference, such as a GPS position fix. A mobile phone can search up the currently received base stations in a database using these distinctive identifiers via an IP- based network connection in order to determine the position. Cell-Id positioning is relatively imprecise since base station reception zones are significantly bigger than those of WiFi hotspots, but it uses very little energy because mobile phones frequently measure the distances to adjacent base stations for handover or location management.
In conclusion, it can be said that WiFi positioning has an obvious advantage over GPS in that it is ideal for indoor positioning and uses a reasonable amount of power, but that it also has some drawbacks.

3) Sending a text-message to the registered number Mobile devices are most commonly used for text-based messaging, which allows users to connect with one another additional people who use short message services (SMS). With SIM card services, the SMS is transmitted from one mobile handset to another. The three functionalities mentioned above are made more effective by this one. The benefit of sending a text message from a stolen smartphone is that we will be able to obtain the SIM card's identifying number, allowing us to quickly determine who the owner of that SIM card is. Unfortunately, it is not possible to directly track an individual's identification using their SIM number; a legal procedure is necessary instead.

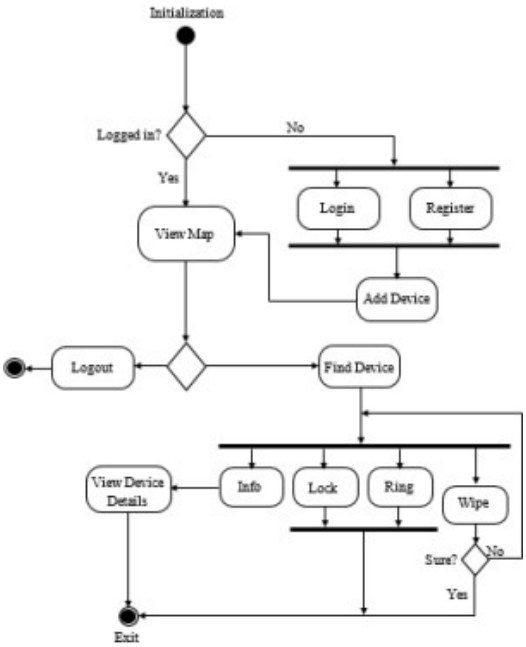
Algorithm

The following is the proposed model's algorithm:
Step 1: Start the gadget. Enter the contact information and email address number.
Step 2: Use Wi-Fi or mobile data to access the internet.
Step 3: The stolen bit is set to "false" and the device's IMEI, email address, and phone number are registered in a remote database.
Step 4: The client programme is operating as a Service in the device's background

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Step 5: Verify the value of the stolen bit for the device's IMEI in the remote database.

Step 6: If the stolen bit is "false," keep running in the background and conduct another check in a day or two. If the stolen bit is set to "true," collect the device's current location coordinates, the SIM card number, take a front-facing photo with the device's camera (if one is available), plot the location coordinates on Google Maps, send a text message to the registered contact number (if the SIM card has changed), and email all the information to the registered email address.



IV. SOFTWARE REQUIREMENTS

Flutter

Flutter is an open-source UI software development kit created by Google. It is used to develop cross- platform applications for Android, iOS, Linux, macOS, Windows, Google Fuchsia, and the web from a single codebase. First described in 2015, Flutter was released in May 2017.

Android Studio

Android Studio is the official integrated development environment for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. It is available for download on Windows, macOS and Linux based operating systems.

Flutter Libraries

Pub is the package manager for the Dart programming language, containing reusable libraries & packages for Flutter and general Dart programs.

Google Maps Api

The Google Maps Platform is a set of APIs and SDKs that allows developers to embed Google Maps into mobile apps and web pages, or to retrieve data from Google Maps.

Firestore

Cloud Firestore is a NoSQL document database that lets you easily store, sync, and query data for your mobile and web apps - at global scale.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

V. RESULTS AND DISCUSSION

The application outputs that are displayed in the Results section are discussed.

1. Screenshot of the registration interface: Here, users can register by filling out the form's necessary fields.
2. Screenshot of the Locate Device Interface: By entering a missing device's L-CODE in the field provided, a user can utilise this interface to locate it. The application directs the user back to the Map Interface once the L-CODE has been entered and verified.
3. Screenshot of the control device interface: When a user locates a device successfully, this interface is called. A component of the Map Interface, it. It features four buttons (INFO, LOCK, WIPE, and RING), and when pressed, a red arrow points to the lost device's present location on a map.
4. Screenshot of the Device Info Interface: Details of the missing device are displayed on this interface. It appears when the Control Device Interface's Info button is clicked.
5. Screenshot of the Confirm Wipe Interface: The Confirm Wipe Interface appears when a user presses the WIPE button and displays a message of confirmation.

VI. CONCLUSION

The most often used techniques for protecting Android mobile phones include the GPS tracking system, image capture, password/biometric changes, etc. These techniques are then followed by a number of further procedures that enable the server to communicate with lost mobile phones using a GPS tracking system and to communicate with an alternative SIM number via SMS, enabling the server to locate lost or stolen Android mobile phones.

REFERENCES

[1] http://www.gartner.com/it/page.jsp?id=12246 45
[2] Survey about mobile theft in USA : http://www.symantec.com/about/news/release/a rticle.jsp? prId=20110208_01.
[3] Survey about mobile theft in India : http://asiarelease.asia/norton-survey-reveals-1-in-2-indians-is-avictim-ofmobile-phone-loss-or- theft/.
[4] http://en.wikipedia.org/wiki/Global_Positionin g_System.
[5] http://en.wikipedia.org/wiki/Mobile_phone_tr acking#Netw ork-based.
[6] http://en.wikipedia.org/wiki/Mobile_phone_tracking.
[7] Simulating Power Consumption of Location tracking algorithms, 2012 IEEE 36th International Conference on Computer Software and Applications.
[8] http://en.wikipedia.org/wiki/Global_Positioning_Syste m.