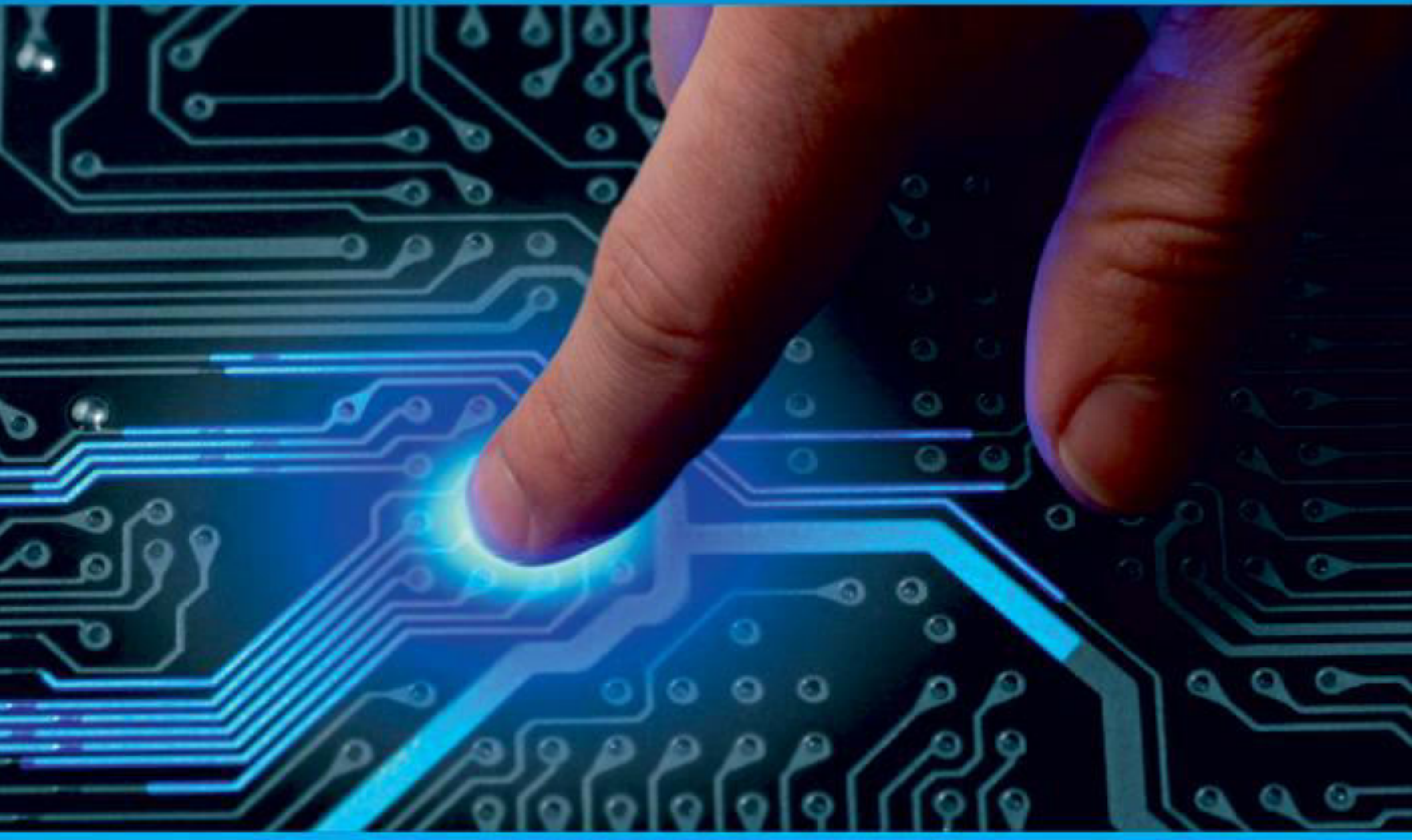
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

GPS Based Monitoring System Mobile Theft Tracing System

DR.P.ANITHA, VENKATESH B

Professor & Head, Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

ABSTRACT: The project entitled "MOBILE THEFT TRACING SYSTEM" is an Android Application developed using Eclipse as its Front end and Microsoft SQL Server 2008 as its Back end. In this Mobile Theft Tracing System first have to install the application in user device, then corresponding user has to register their details likes Name, E-mail ID, Secondary mobile number. Then the application is ready to use. It is mainly used to trace the third party user's photo graphic image and geo location information's. The photo graphic image is get through front camera and geo location information's is get through GPS services from the mobile device. Those information's are send to device holder registered E-Mail address, Secondary Mobile number in format of MMS, and also those information's are send to applications Online storage. The objective is to trace and identify the mobile phone which has been stolen by a thief using android technology This project develops an application to find the theft mobile phone with the help of photo graphic image and the geo locations information of the third party user. Those information's are delivered to user's E-Mail and applications online storages, the considering signal strength and fluctuation in location based application will monitor every action of the thief and generate report. Based on the generated reports the theft mobile phone can be traced. By this standalone application the theft mobile can be easily traced.

KEYWORDS*:* Global Positioning System (GPS), Multimedia Message Service (MMS), photo graphic image, E-Mail.

I.INTRODUCTION

ANDROID

Android is a Linux-based operating system for mobile devices such as smart phones and tablet computer. It is developed by the Open Handset Alliance led by Google. Google purchased the initial developer of the software, Android Inc., in 2005. The unveiling of the Android distribution in 2007 was announced with the founding of the Open Handset Alliance, consortium hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. Google releases the Android code as open source, under the License. The Android Open Source Project AOSP is tasked with the maintenance and further development of Android.

Android has a large community of developers writing applications Application that extend the functionality of the devices. Developers write primarily in a customized version of Java. Application can be downloaded from third-party sites or through online stores such as Google Play formerly Android Market, the app store run by Google. Android was listed as the best-selling Smartphone platform worldwide in Q4 2010 by Canals with over 300 million Android devices in use by February 2012. According to Google's Andy Rubin, as of February 2012 there are over 850,000 Android devices activated every day. Developers write primarily in a customized version of Java. Application can be downloaded from third-party sites or through online stores such as Google Play formerly Android Market, the app store run by Google. The unveiling of the Android distribution in 2007 was announced with the founding of the Open Handset Alliance, consortium hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices.

ANDROID ARCHITECTURE

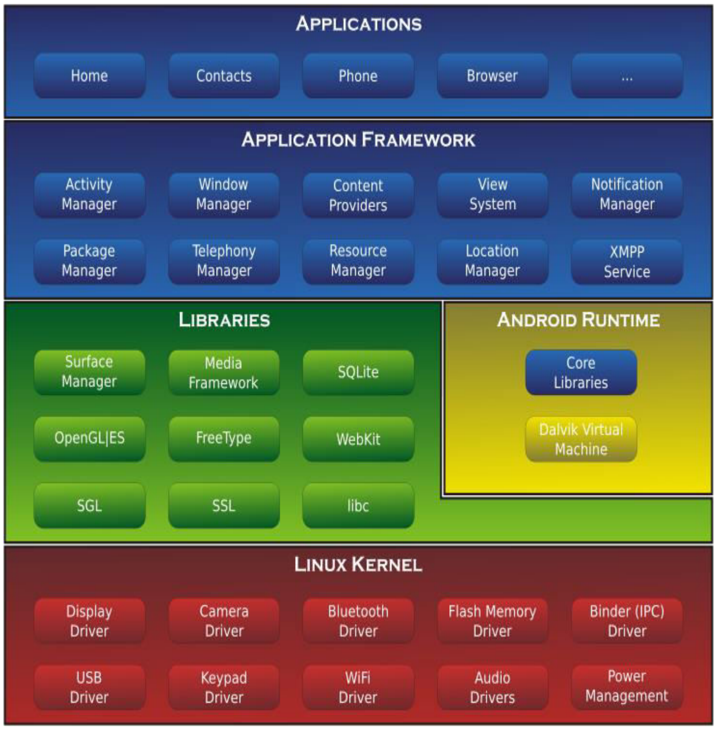


Figure 1: Android Architecture

Android Runtime

This is the third section of the architecture and available on the second layer from the bottom. This section provides a key component called Dalvik Virtual Machine which is a kind of Java Virtual Machine specially designed and optimized for Android. The Android runtime also provides a set of core libraries which enable Android application developers to write Android applications using standard Java programming language.

The Dalvik VM makes use of Linux core features like memory management and multi-threading, which is intrinsic in the Java language. The Dalvik VM enables every Android application to run in its own process, with its own instance of the Dalvik virtual machine.The Android runtime also provides a set of core libraries which enable Android application developers to write Android applications using standard Java programming language.

Application framework

The Application Framework layer provides many higher-level services to applications in the form of Java classes. Application developers are allowed to make use of these services in their applications.

Applications

They will find all the Android application at the top layer. They will write their application to be installed on this layer only. Examples of such applications are Contacts Books, Browser, Games etc.

ANDROID APPLICATION COMPONENTS

There are following four main components that can be used within an Android application:

Components	Description
Activities	They dictate the UI and handle the user interaction to the smartphone screen
Services	They handle background processing associated with an application.
Broadcast Receivers	They handle communication between Android OS and applications.
Content Providers	They handle data and database management issues.

Figure 2: Components of Android

USER INTERFACE

Android’s user interface based on direct manipulation, using touch inputs that loosely correspond to real-world actions, like swiping, tapping, pinching and reverse pinching to manipulate on-screen objects. The response to user input is designed to be immediate and provides a fluid touch interface, often using the vibration capabilities of the device to provide hepatic feedback to the user.

Internal hardware such as accelerometers, gyroscope,proximity sensors are used by some applications to respond to additional user actions, for example adjusting the screen from portrait to landscape depending on how the device is oriented, or allowing the user to steer a vehicle in a racing game by rotating the device, simulating control of a steering wheel. Android devices boot to the home screen, the primary navigation and information point on the device, which is similar to the desktop found on PCs.

Android home screens are typically made up of app icons and widgets; app icons launch the associated app, whereas widgets display live, auto-updating content such as the weather forecast, the user's email inbox, or a news ticker directly on the home screen. A home screen may be made up of several pages that the user can swipe back and forth between, though Android's home screen interface is heavily customizable, allowing the user to adjust the look and feel of the device to their tastes.

The status bar can be pulled down to reveal a notification screen where application display important information or updates, such as a newly received email or SMS text, in a way that does not immediately interrupt or inconvenience the user

MEMORY MANAGEMENT

Since Android devices are usually battery-powered, Android is designed to manage memory RAM to keep power consumption at a minimum, in contrast to desktop operating systems which generally assume they are connected to unlimited mains electricity. When an Android app is no longer in use, the system will automatically suspend it in memory - while the app is still technically open suspended application consume no resources e.g. battery power or processing power and sit idly in the background until needed again.

It has the dual benefit of increasing the general responsiveness of Android devices, since application don't need to be closed and reopened from scratch each time, but also ensuring background application don't waste power needlessly. Android manages the application stored in memory automatically when memory is low, the system will begin killing application and processes that have been inactive for a while, in reverse order since]

SECURITY AND PRIVACY

Android applications run in a sandbox, an isolated area of the system that does not have access to the rest of the system's resources, unless access permissions are explicitly granted by the user when the application is installed.

Before installing an application, the Play Store displays all required permissions a game may need to enable vibration or save data to an SD card, for example, but should not need to read SMS messages or access the phonebook. After reviewing these permissions, the user can choose to accept or refuse them, installing the application only if they accept. The sandboxing and permissions system lessens the impact of vulnerabilities and bugs in applications, but developer confusion and limited documentation has resulted in applications routinely requesting unnecessary permissions, reducing its effectiveness. Several security firms, such as Lookout Mobile Security, AVG.Technologies, and McAfee,have released antivirus software for Android devices. This software is ineffective as sandboxing also applies to such applications, limiting their ability to scan the deeper system for threats.

Research from security company Trend Micro lists premium service abuse as the most common type of Android malware, where text messages are sent from infected phones to premium-rate telephone numbers without the consent or even knowledge of the user. Other malware displays unwanted and intrusive adverts on the device, or sends personal information to unauthorized third parties.

Security threats on Android are reportedly growing exponentially however, Google engineers have argued that the malware and virus threat on Android is being exaggerated by security companies for commercial reasons, and have accused the security industry of playing on fears to sell virus protection software to users. Google maintains that dangerous malware is actually extremely rare, and a survey conducted by F-Secure showed that only 0.5% of Android malware reported had come from the Google Play store. The sandboxing and permissions system lessens the impact of vulnerabilities and bugs in applications, but developer confusion and limited documentation has resulted in applications routinely requesting unnecessary permissions, reducing its effectiveness.

Google currently uses their Google Bouncer malware scanner to watch over and scan the Google Play store application. It is intended to flag up suspicious application and warn users of any potential issues with an application before they download it. Android version 4.2 Jelly Bean was released in 2012 with enhanced security features, including a malware scanner built into the system, which works in combination with Google Play but can scan application installed from third party sources as well, and an alert system which notifies the user when an app tries to send a premium-rate text message, blocking the message unless the user explicitly authorizes it.

Android smart phones have the ability to report the location of Wi-Fi access points, encountered as phone users move around, to build databases containing the physical locations of hundreds of millions of such access points. These databases form electronic maps to locate smart phones, allowing them to run application like Foursquare, Google Latitude, Facebook Places, and to deliver location-based ads.

Third party monitoring software such as Taint Droid, an academic research-funded project, can, in some cases, detect when personal information is being sent from applications to remote servers.

II.RELATED WORK

The software is mainly developed to find the theft mobile phone from the owner of the mobile phone. The photo of the thief and location of the thief will be send to the owner’s E-Mail ID. While registering the application, the owner has to enter the E-Mail ID. To that mail ID, the photo of the thief and location of the theft mobile phone will be send. By setting the time interval’s the photo and location will be send. This system uses android based mobile phones for the software to be run. The photo of the thief is not only stored in the email ID of the user, but also stored in the gallery of the user’s phone. After recovering the theft phone, the user can delete that photo from the mobile phone. GPS tracker contains GPS module to receive the GPS signal and calculate the coordinates. With the help of Internet the location and photo of the thief is send to the user’s mail address. By using the algorithms the application will be processed.

Dijkstra’s Algorithm is used to find the shortest path from one node to another node in a graph. Global Positioning System is used for adding a new functionality in Dijkstra’s algorithm. In this paper, using Global Positioning System the position parameter is added in the Dijkstra’s algorithm. . By using this current position, the distance can be determined from one node to another node. The shortest path can also find out using this distance. For this an algorithm is proposed.

This system is developed using these technologies like GPS, Google Map & GPRS (Global Packet Radio Service) .the consists of GPS enabled device like mobile phones embedded in the bus, which find out its current coordinates periodically after some interval & send it to the database for the being processed & analyzed.

Location based services offer many benefits to mobile user to retrieve the information about their current location & process that data to get more useful information near to their location. Using a GPS assisted phone & a web service using GPRS ,location based services can be implemented on Android based smart phones to provide services like advising client of current traffic conditions, providing routing information , helping them find nearby hotels. In paper location based services is implemented through Google Map on Android Phones to give multiple services to the user based on their location**.**

III.EXISTING SYSTEM

This section deals with some of the existing works related to the proposed mobile solution, mainly, using tracking systems through GPS or GSM cell. Sangwoo Cho et.al. presents a method to track a mobile device by monitoring the signal powers of the mobile transmitter measured at several base stations. The tracking method uses a constrained Bayesian bootstrap filter with signal power measurements in order to improve accuracy. The signal power measurement is a non-linear function of the position of a mobile. They compare the signal power measurements at several base stations with the power maps (non-linear function of the position of a mobile) to get the likelihood at each position. This method aims mobile devices that are mounted in vehicles and the movement of the devices is restricted in a road. Another mobile tracking approach is proposed by Chao-Lin Chen et.al. It uses a hybrid location scheme, which combines both the satellite-based and the network based signals. The proposed scheme uses the two-step Least Square method to estimate the three-dimensional position (i.e. the longitude, latitude, and altitude) of the mobile devices. The Kalman filtering technique is exploited both to eliminate the measurement noises and to track the trajectories of the mobile devices. A fusion algorithm is employed to obtain the final location estimation not only from the satellite-based but also from the network-based systems. Most of the above-mentioned systems, provide dedicate solutions using tracking methods to monitor a mobile device. But by just enabling the cell phones with GPS system and retrieving the information about the new SIM would be insufficient to track the Smartphone. Hence came the idea of developing SAPt - A Stolen Android Phone Tracking application, an efficient and unique application with few more features which help in controlling the lost android Smart phone and retrieving it back. This application uses location-based services (LBs) like GPS or global system for mobile (GSM) network to track a mobile device.

IV.PROBLEM DESCRIPTION

The software is mainly developed to find the theft mobile phone from the owner of the mobile phone. The photo of the thief and location of the thief will be send to the owner’s E-Mail ID. While registering the application, the owner has to enter the E-Mail ID. To that mail ID, the photo of the thief and location of the theft mobile phone will be send. By setting the time interval’s the photo and location will be send. This system uses android based mobile phones for the software to be run. The photo of the thief is not only stored in the email ID of the user, but also stored in the gallery of the user’s phone. After recovering the theft phone, the user can delete that photo from the mobile phone. The manual work to find the theft mobile phone is difficult. It may be or may not be found the mobile phone. The manual work is very difficult. By this software the theft mobile phones can be found out easily via the GPS System in the mobile phone. After recovering the theft phone, the user can delete that photo from the mobile phone. This system uses android based mobile phones for the software to be run. It may be or may not be found the mobile phone.

V.PROPOSED SYSTEM

The project presents a tracking system which is capable of detecting the lost or theft mobile phone from the owner. By using the GPS in the mobile phone the theft mobile phone can be found. Along with the location the photo of the thief can be send to the owner’s mail address. By using the Get Location Module the location of the mobile can be traced in this application. From the Google, the API is got and it is installed in the system. Thus the location can be tracked by the application. To get the Photo of the thief, the front camera should be initially activated. Then only the photo of the thief can be taken. Now with the help of Internet the location and photo of the thief is send to the user’s mail address. By using the algorithms the application will be processed. By this application, the lost or theft mobile phone can be traced easily and faster than the manual work. By this application the manual work to detect the location of the phone is reduced and done efficiently. Along with the location the photo of the thief can be send to the owner’s mail address. By using the Get Location Module the location of the mobile can be traced in this application. From the Google, the API is got and it is installed in the system. Thus the location can be tracked by the application. Along with the location the photo of the thief can be send to the owner’s mail address. By using the Get Location Module the location of the mobile can be traced in this application. From the Google, the API is got and it is installed in the system. Thus the location can be tracked by the application. By using the Get Location Module the location of the mobile can be traced in this application.

Today the technology has reached its peak in this circumstance if a mobile phone has been stolen by a third party or else missed by user's, the mobile phone takes the photograph of the thief's, without their knowledge of that thief. This photograph image along with the geo location is sent to the registered email id of the user mobile phone. Now the user with that information along with the IMEI number can seek the help of police to identify their mobile which has been stolen. This method helps for the quick recovery of the theft mobile phone.

ADVANTAGES

- To trace and identify the user's android device.
- To identify third party geo location and photographic image.
- To share an information to user's registered mail-id.
- Make an easy to find third party information.
- To provide better accuracy, efficiency and reliability.

VI.CONCLUSION

The Practical application of Mobile Theft Tracing System has been developed successfully by using Android. By this application, the theft Android mobile phones can be found by using the GPRS position. In existing MTTS can only send SMS and details about SIM and GPS co-ordinates when theft is detected. On theft detection their system would send an SMS to the owner alerting him of the phone number of the thief without the knowledge of thief in stealth mode. Then their system would retrieve GPS co-ordinates from satellites and then send a second SMS. Then MTTS would connect to internet and send those GPS co-ordinates to Google maps and then using Google maps API, it would retrieve the postal address of the stolen phone and send it as an SMS to the relatively stored number. For a company in a transportation, can track their vehicles easily by checking online anytime from anywhere. This solution also contains a chatting mechanism where administrator or user can chat with each other to pass information.

REFERENCES

1. Bhattacharya, S.Bluck, H.:kjaergaard, M.b.: Nurmi,P.(April 2014), "Robust and Energy-Efficient Trajectory Tracking fpr Mobile Devices", Mobile Computing, IEEE Transactions on (Volume:14 , Issue: 2), pp.430-443
2. Juan Lei; Zhenhua Wang; Yihong Wu; Lixin Fan(July 2014), "Efficient pose tracking on mobile phones with 3D points grouping", Multimedia and Expo (ICME),2014 1EEE International Conference , pp.1-6
3. M. Mohana (2007),"Guaranteed and consistent mobile transaction in Broadcast Envirnoment", Prentice Hall publications.
4. Md. Subrun Jamil, Fouzia Ashraf Mousumi (2008), "Short Messaging Service (SMS) Based m-Banking System", Addison-Wesley publications.
5. Mohammad Shirali-Shahreza, M. Hassan Shirali-Shahreza (2007),"Mobile Banking Services in the Bank Area", Wiley India Ltd(rs).
6. Nakib, A.Daachi, B.:Dakkak, M.:Siarry,p.(Oct.2014), "Mobile Tracking Based on Fractional Integration", Mobile Computing , IEEE Transactions on (Volume:13 , Issue: 10),pp. 2306-2319
7. Saifullah M Dewan (2010),"Issues in M-Banking: Challenges and Opportunities", TATA McGraw Hill Education Private Limited.
8. Shan chu, Lu yao-bin (2009),"Trust transference in mobile banking: an investigation of the initial trust", Pearson Education.
9. Taipei,Taiwan(sep 2014),'Smart Insulating container with Anti-theft Features by M2M Tracking",ISBN:978-1-4799-5967-9, pp:140-147

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING