TEST Engineering & Management

May - June 2020
ISSN: 0193-4120 Page No. 5090-5094

Locating Theft Mobile Using Efficient Face Recognition

[1]R Deepthi, [2]Prathiba J, [3]Harshini P, [4]Praneetha DS, [5]Prabhakar M

[1,2,3,4]Student, [5]Associate Professor, School of Computing and Information Technology, Reva University, Bangalore, India

Article Info
Volume 83
Page Number: 5090-5094
Publication Issue:
May - June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *16 May 2020*

Abstract

A thief after stealing the mobile, will automatically switches off and removes the SIM card to deactivate the mobile. When the user inserts a new SIM card into the stolen mobile, our application which is running in background will track the SIM card details and cross check with the cloud server for that particular IMEI number that is the actual SIM number via GPRS (Global Packet Radio). If not the actual user of the mobile he/she will get the alert in the shape of SMS (Short Messaging Service) or through Email along with the current GPS (Global Positioning System) location of the stolen mobile and the photo of the thief. Find out the stolen mobile with the help of GPS and GPRS. The thief face will be forwarded via Email, and will also contain necessary information like SIM card number, IMEI number, current location of the mobile, etc. We had proposed a different approach to find out the thief and the stolen mobile in a more accurate manner.

Keywords: IMEI number[1], GPS[2], GPRS[3], SIM[4], Face capturing[5], Lens[6], Sensor[7], Aperture[8], Shutter[9], SMS[10]

1. Introduction

Location privateness has become a critical concern because of the proliferation of GPS devices, web area services, WLAN and mobile ID based positioning technologies. The power to find a wireless device has been seemed into by several researchers. Localization might be active or passive. In passive Localization, the customers may not convey any device however in lively localization the users deliver devices, where the customers wherein approximately is thought. Even a mobile tool without a GPS monitoring system can send the situation information to the person with the assistance of radio emission transmission. There are two primary actions,

They are:

1: Gathering the state of affairs of user.

2: Exploiting the same facts to produce a service

Availability of the many devices like smart phones, Tablets, laptops, net books, wristwatches, TVs, etc. to be able to utilize numerous sensors like accelerometers, temperature gauges, GPS receivers, gyroscopes, etc. And therefore the availability of wi-fi Internet have made localization less difficult and simpler. Since clever handhelds have a range of sensors like compass, gyroscopes etc., it's possible to create tracking structures not most effective place aware, but additionally context aware. Location may be a a part of context but the context also encompasses situations like, if the consumer is moving, if he is taking turns etc. Gathering details enables to better music a private specifically for surveillance. More over context statistics can be applied to reduce network records switch for these styles of applications. As an example, if the tool is static there is no want of sending updates to the tracker device frequently. However effectiveness of context sensing relies upon on various things like if the person is carrying the tool in his/her pocket.

Consequently, all through this paper, a service for context monitoring of Smart handheld gadgets is proposed that takes under consideration both region of the tool and consumer context for better surveillance. This device can be implemented for monitoring place of people, misplaced or stolen devices etc. In a very person friendly way that saves effort. Also by evaluating contexts of friends, nearest and desirable people is also identified when necessary.

TEST Engineering & Management

May - June 2020
ISSN: 0193-4120 Page No. 5090-5094

2. Literature Survey

A literature survey is conducted to in order to provide a critical overview of what was found and justifies the conceptual framework as well as inform the methodology. The principal terminologies are as follows:

1) IMEI number

IMEI number stands for International Mobile Equipment Identity. It is not restricted to handiest cellular phones, it is associated with every device that can get connected to a network and it is the identity of the device when it connects to a network. It is unique for every device having a total length of 15 digits. If the device is a phone then one can dial *#06# and if the device is a tablet or dongle or Wi-Fi then one can find the IMEI number in the battery compartment or the mobile Broadband dashboard or in the settings. When a person loses his/her phone, with the help of this unique number, the user can deny the access of the unaccredited individual and aids in the detection of the theft phone. IMEI format is given by Telecommunication and structure by the BABT (British Approvals Board for Telecommunications). Usually people with an unsound mind will change the IMEI number which dishonourable and the prime cause to do so is to destroy the tracking s well as the model or origin of the theft phone. Since, every phone is endowed with GPS system, if an unique ID number is given to each GPS system, it will accurately locate the theft phone.

2) GPS

There are a constellation of satellites, those satellites are continuously beaming facts on this planet that is in turn is obtained by gadgets consisting of your smartphone or navigational units, allowing you to see where the phone is currently present and the whereabouts of the phone. GPS stands for Global Positioning System which. The most commonly used system is Navistar referred to as GPS. GPS satellites are organised in such a way that almost from everywhere on the surface of the earth can have direct line of sight of at the least 4 GPS satellites to calculate three positions coordinated and the clock deviation. With all the GPS signals broadcasting at 1.57542GHZ and 1.2276GHz. Usually, not always the GPS in a phone is switched on so during such an unfortunate situation it is difficult to track the phone so there are paid GPS tracking applications such as Waze that is facilitated for both android and iOS that provides additional protection for your phone. This circumspect application doesn't on the home screen and also difficult to disable, helping the person find their theft phone.

3) SIM

SIM stand for Subscriber Identity Module and It identifies what offerings the cellular phone subscriber is using and they are of quite low capacity holding under a MB of data and the information they hold is pivotal when you don't have any wifi signal SIM card shops 54-bit number that sets out as a distinctive adjunct and consumes eight bytes of storage. When you switch on your telephone and first truss with the mobile community then your telephone will skip your SIM card in your SIM card's ID variety along side an authentication key also recognised inside the SIM card in your cellular cellphone provider, your issuer then engender a unpremeditated wide variety and makes use of the key to answer out a response wide variety at the equal time and that random quantity is delegated back on your telephone. The same calculation is done with the authentication key to generate another response number, if both the numbers in shape your issuer will recognise This and coalesce your phone to the network

4) Face Capturing

A camera in a plane comprises of
Lens (to structure the image)
Sensor (to print the image)
Aperture (to control the light that pounds on the sensor)
Shutter (to control time until when the sensor is revealed)

A light sensor in a phone sharpens and lights photos and also help regulate screen brightens. Once the phone is lost and when an unauthorised user accesses the data the camera will capture the facial image and send it to the numbers set in advance by the user.

Related work

According to "Android Mobile Security with Auto boot Application":- M,Umamaheshwaran, S.Pratheepa Devapriya, Dr. R.Nedunchelian: IJET Vol 5 No 3 - 2013 and Detection of Lost Mobile on Android Platform":- Shreya K. Patil, Bhawana D. Sarode, Prof, P.D. Chowhan: IJARCET 2014

The application developed will provide the current latitudinal and longitudinal values using the in built GPS when the phone is stolen. The values are stored in the memory with the help of a SIM card.

Drawback

Once the phone it will not be stagnant and will be moving from one place to another to another. When the SIM card is changed then both SIM card numbers will be compared, if they are identical there will not be any change in the location otherwise it will provide the geographical values of the current location due to which tracking the theft phone becomes very cumbersome.

According to Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices":- Michael Becher, Felix C. Freiling Johannes Hoffman, Thorsten Holz : IEEE 20111

This paper emphasis on the mobile network security and the attacks regarding the security with the help of. Offensive trajectory the use of the again end machine and the web browser It withal shows the differences as well as

May - June 2020
ISSN: 0193-4120 Page No. 5090-5094

similarities between "normal" security and mobile security, and also draws attention on the future enhancements in this area.

Drawback

Since the mobile technologies are advancing so is the attack in mobile technologies who want to exploit user data is also increasing with the same pace. Security is a very important aspect concerning the user information. So compromising on mobile security leads to creating a multitude of difficult scenarios.

3. Problem Definition

1. The predominant objective of the challenge is to find out a stolen mobile with the help of SIM (Subscriber Identity Module).
2. Intermittently we unintentionally drift to replace our smartphone someplace and we cease up searching for it. Hit there to on occasion we're lucky sufficient to get our telephones returned but sometimes we in no way get it back. Hence to avoid such situations and keeping the recent demand for phones in mind, we have decided to broaden this project.
3. This application which is running in background gets triggered instantly when the individual who has embezzled the smartphone and replaces the sim and activates the phone. That consumer will no longer be aware that a message is dispatched to the preordained numbers.
4. The actual user of the mobile will get the alert in the shape of SMS (Short Messaging Service), MMS (Multimedia Messaging Services) or through Email.

4. Proposed System

Among our friends circle or group members will help to get that information once again when you're SIM or Mobile is lost.

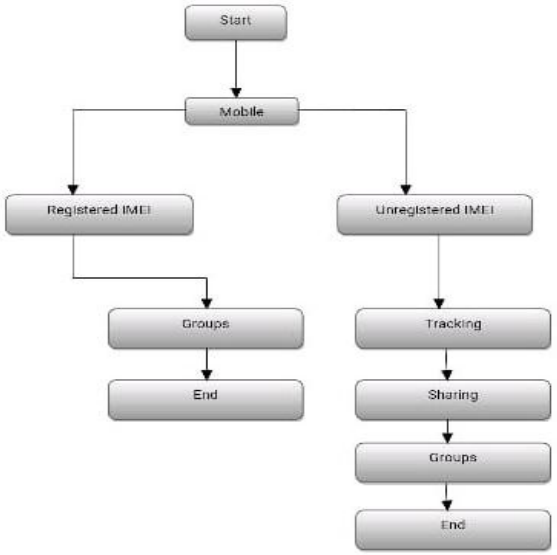
We they get connected to a new friend a new contact alert will rise among your friends circle and when your mobile is lost u can able to trail the place of your The paper emphasis a method to direct towards Anti-theft primarily based on smart phones by exercising unique services. Android based totally Application is hooked up in consumers mobile which is hired to trace the SIM Card ID (IMEI). If Phone is embezzled SIM card would be replaced, and our Application that is coextendingly operating in background of the cellular, will Tract the SIM Card ID. Incase the SIM card is modified then GPS is commenced routinely and specific and accurate region of the thief will be captured. The assets of the application includes:

Conviently become aware of the robbery mobile
Limited burdernsome process
Completely self-regulating mechanism
Supervision not necessary

A thief after stealing the mobile, will automatically switches off and removes the SIM card to deactivate the mobile. When a user inserts a replacement SIM card into the stolen mobile, our application which is running in background will track the SIM card details and cross visit the cloud server whether for that exact IMEI number is that the actual SIM number via GPRS (Global Packet Radio). If not the particular user of the mobile he/she will get the alert within the kind of SMS (Short Messaging Service) or through Email together with this GPS (Global Positioning System) location of the stolen mobile and also the photo of the thief. discover the stolen mobile with the assistance of GPS and GPRS. The thief face are going to be forwarded via Email, and can also contain necessary information like SIM card number, IMEI number, current location of the mobile, etc. We had proposed a unique approach to search out out the thief and also the stolen mobile during a more accurate manner.

Modules

Groups
Sharing contact details
SIM tracking



Groups

Maintaining friend's circles is one kind of good activity; it helps us to sort out our personal or official problems in many ways.

There are two types of details sharing in between the groups they are public and private mode, public sharing is visible to all viewers and private sharing is visible only to your friends circle or friends.

Sharing Contact Details

Sharing your contact and profile details smartphone.

Sim Tracking

When you find a latest SIM gets introduced to the smartphone for the same IMEI number then an event is

TEST Engineering & Management

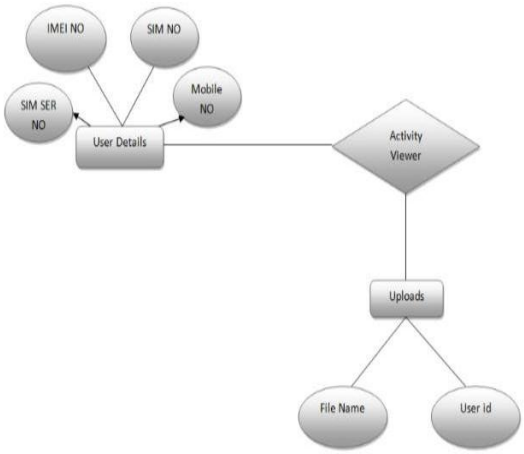
May - June 2020
ISSN: 0193-4120 Page No. 5090-5094

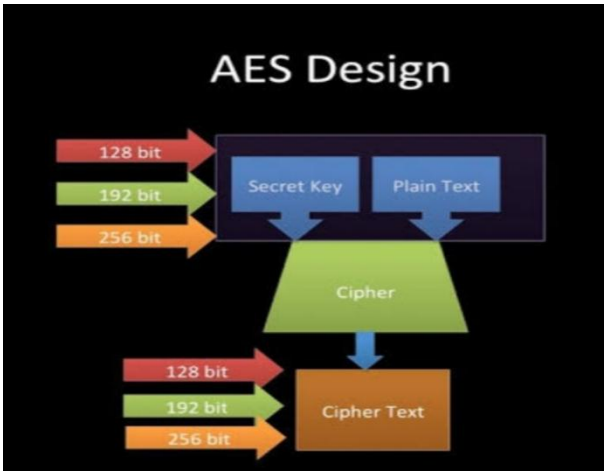
triggered and the front camera will capture the face of the thief and send an SMS, MMS, and Email to the actual owner of the mobile.

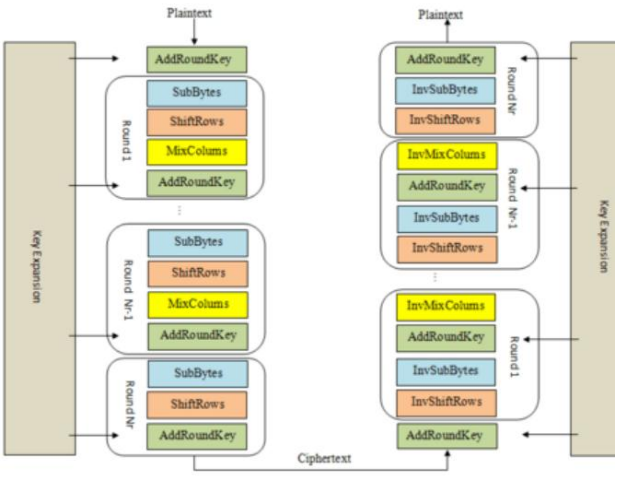
In case the owner does not notify the SMS, MMS or Email, the group members will get intimation, then they can inform to the actual owner.

System Design

Module Diagram

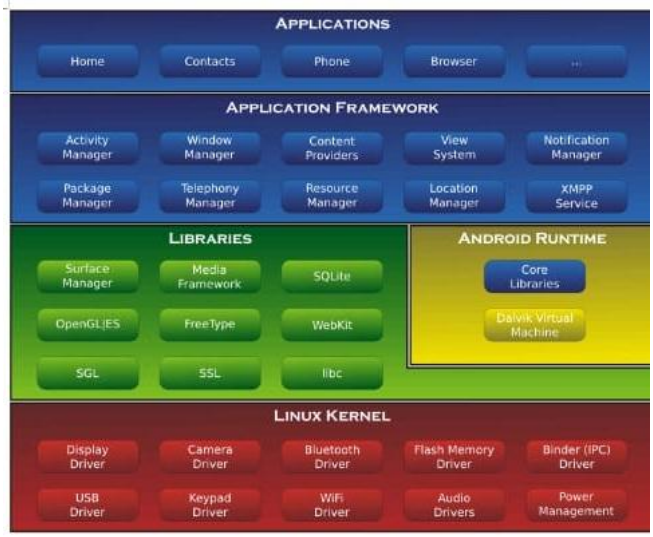




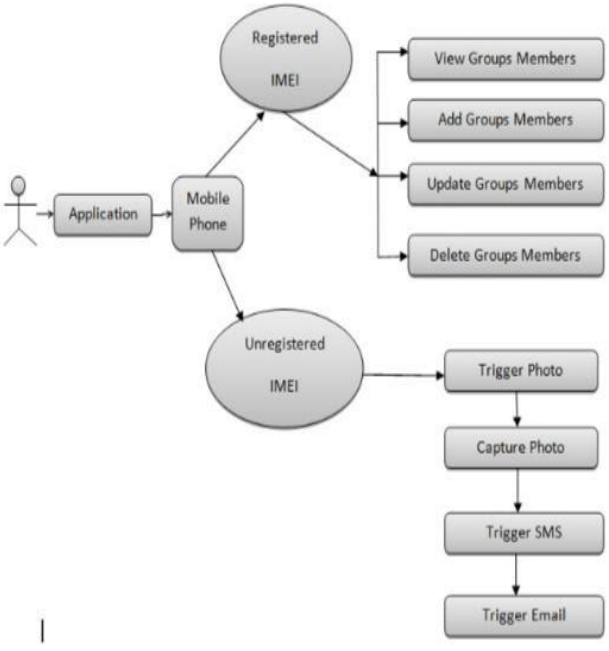


5. Applications

1. This work performs a definitivemobile software being "find my friends". It includes a Smart phone integral, which has multiple software detector and a possible server integral which covers data regarding precise application (like vicinity identified region)
2. Using pioneer mobile Global Positioning System tracking application, one will be able to locate their Android device in real time. It supports features like photo sending and recording videos.
3. The user can track the correct current location of their android phone. They can send location matter automatically and manually. This works properly for almost all browsers including android phone.



Use Case Diagram



May - June 2020
ISSN: 0193-4120 Page No. 5090-5094

6. Expected Outcome and Result

Each Subscriber Identification Module card is recognized by its Integrated Circuit Card ID (ICC-ID). ICC-IDs are stored in the SIM cards and are also engraved on the SIM card body amid a process called personalization. As started, the mobile a software correlates ICC ID of the currently using SIM card with the predetermined ICC ID to hit upon unapproved SIM card inside the smart phone. Soon after the SIM is replaced the consumer promptly receives the notification about the International Mobile Equipment Identity number and the knowledge about the contemporary SIM insinuated. The consumer is intended to codify a cell number in the cellular software which facilitates to ship notifications as well as messages to the consumer's SIM card number.

7. Conclusion

The paper stages a completely unique theft deterrent software for smartphones supported gadgets. appliance disposes an employer safety for the answer profoundly engages consumers and site through the medium of SMS and email concerning the consumer to spot the wrongful individual and cause them to be seized and jailed. It uplifts effective appliance offering the knowledge regarding the situation about the android based smart phone including the assistance of SMS. Through the appearance ahead ones space, already stated the mechanization is expanding everyday. At present the application is accessible for particularly smartphones. Forthcoming enhancements comprises of instantaneous and future essentials by handing directive progress of the appliance through shooting the photo and video of the thief.

References

[1] Android board Based Intelligent Car Anti-Theft System Through Face Recognition Using GSM and GPS Conference Paper (PDF Available) · October 2016 with 908 Reads Conference: International Conference on Signal, Power, Communication, Security, and Com

[2] Face Recognition in Mobile Devices Article (PDF Available) in International Journal of Computer Applications 73(2):13-20 · July 2013

[3] Android Mobile Security with Auto boot Application- M,Umamaheshwaran, S.Pratheepa Devapriya, Dr. R.Nedunchelian: IJET Vol 5 No 3 - 2013