Theft Detection for Secured Access in Android Devices

P.Kanimozhi ¹, Adityan ², N.Padmapriya ³

¹,²Associate Professor, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram.
³UG Scholar, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram.

¹chandrankani@gmail.com , ³priyaiifetcse@gmail.com

Abstract. The purpose of this project is to build up an android application which provides location tracking functionality for android device using SMS. Additionally, we can track the photos of a person who stole our android mobile device this task underpins android OS and makes correspondence with the telephone through SMS and E-mail. Utilizing basic SMS orders, you can follow your android gadget's location tracking: We can track the lost phone using simple SMS commands. Camera can be controlled externally in theft device to capture images. Mobile devices are said to be portable and can be carried by a person from one location to another. There is frequent theft of mobile devices and the existing system consists of monitoring the walking movement of user and patterns are analysed when there is a variation in movement then the mobile device will be locked. The proposed system is used to save another alternate number of the user. Message is sent from alternate number to theft android device and we can retrieve the GPS location.

Keywords- theft prevention, Gait recognition

1. Introduction

In recent years, mobile theft has grown to a large extent. The pecuniary value of android devices frequently led to mobile theft. Lack of anti-theft mechanisms is also considered to be one main reason for perennial mobile theft. So, we have provided additional feature in motion. Though the main area of application is sports biomechanics, since the walking style is not the same for all human beings, we have implemented an additional feature to GAIT recognition for developing a theft prevention android application. Though the existing system already allows us to lock the mobile. Finding the theft mobile remains unsolved. The goal is to build up an android application which gives area following usefulness to android gadget utilizing SMS. The principle reason for this venture is to build up an android application which gives area of the following usefulness to gadget utilizing SMS, at the hour of theft.

Additionally, we can capture the photo of person who uses our android mobile device after theft. This photograph is captured by the front camera of the theft mobile. Capturing functionality is controlled through SMS commands. Mode of communication with theft mobile is through SMS, once the photograph, PS location is collected the details are then sent as to email and alternate number respectively.

2. Related Works

A mobile phone in silent mode can be incredibly precarious to discover. In that case there is a chance of losing the wireless signal; where you can insert a resource in to a cell phone sensor or a phone locator. The above mentioned are only just apparatuses, when it is close to a wireless signal, call signal will be there which produces sound making awareness there the phone is nearby. Once you lost the signal in the mobile phone, you should ask someone to call your mobile phone, until your
phone shows that signal is nearby. At the point when the signal is got, you have to decide where to begin the searching process for your phone.

**Article I. Mobile Phone Tracking using IMEI number:**

Once you get to know the IMEI number of your stolen phone, you can contact the police and provide a complaint to them with your phone's IMEI number so that they can track your lost phone.

Another way to avoid usage of the theft phone is to block your SIM, by contacting your service provider.

![Existing System Diagram](image1)

**Fig 1: Existing System**

3. Framework methodology

The system design for the application consists of four important elements they are user, application, location tracker, and camera.

![Proposed System Diagram](image2)

**Fig 2: Proposed System**

**End user:** user who can register using email id, alternate number, and password. He /She can use the application to track the lost device.

**Location tracking:** Used to track device using GPS and network service location.

**Camera:** Used to capture the photograph of the person using device after theft.

**User info database:** User to store user details username and password for login purpose, also used to store email and alternate contact number for communication purpose.
SYSTEM MODULE:
There are four modules in the application

A User information storage
In the user information storage phase, we can store all the user related details in My SQL database. User is prompted to provide details like username, password, Email address, alternate phone number. Username and password combination are used to authenticate the user to login to the application. While details like email address and alternate phone number are used for communicating device like location and photograph.

B Command information storage
In this module we can update the commands like camera for capturing the pictures of the person who theft our mobile phone. Here we can additionally commands to track the mobile device. This will ease the access to the user to track the android device these are the observations done in SMS feature update.

C Track user
In track user phase we can add the GPS for tracking purpose to continually track the mobile device and share the location. Registered user-based SMS commands for tracking, which went sent to device will track the location. The user can be notifying if new SIM card details inserted in the phone.

D Camera access
We can control camera of the device using simple SMS commands. Using SMTP, we send the photos to our registered mail id. Registered user-based SMS commands for tracking, which went sent to device will capture the photograph of the person using the device using front camera. The captured photograph is then sent to registered email address.

SYSTEM REQUIREMENTS:

A. Hardware requirements:
The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system.

B. Software requirements:
The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. The software requirements provide a basis for creating the software requirements specification. Below are the software requirements,

Table: 1: Software Requirements

| HARDWARE REQUIREMENTS     | SOFTWARE REQUIREMENTS                        |
|---------------------------|----------------------------------------------|
| Processor: Dual core or above | Device: GPS enabled Android OS mobile.       |
| Keyboard: Standard windows keyboard | Development Kit: Android SDK 2.3, Java JDK 1.6 |
| Hard Drive: Minimum 32 GB; Recommended 64 GB or more | Language: JAVA |
| RAM: Minimum 4 GB | IDE: Eclipse Helios, Android Emulator. |
| Monitor: 15 LCD or CRT Monitor or | Platform: Window 7/XP. |
performance.Metrics

In system implementation, the information system is operating and allowing the client to take
over for the assessment and performance process is ensured.

GPS tracking functionality:
Here, the functionality of getting location details of theft android device. Here we use the track
command to retrieve the location details of the theft mobile phone,
Step 1: Start.
Step 2: Send the “track” command to theft mobile device.
Step 3: If the GPS location is turned on and there is internet connectivity the device after receiving the
message will notify the location to user.
Step 4: Send location information to user.
Step 5: End.
Location details include latitude and longitude information of the theft device, provided the device
should have GPS/location turned ON.

Image capture functionality
Here, the functionality of capturing photographs of the person using device after theft. Android device
recognizes the keyword “camera” command and turn on the camera to capture the images. So that the
user can know the theft person.
Step 1: START
Step 2: Checks the status of the theft device.
Step 3: The user can send the camera command to enable the camera to turn on.
Step 4: Capture the images of theft person
Step 5: After capturing the image the user will be notified to the registered email

Recovering SIM details:
If the SIM card is changed in the theft mobile device, user is notified with the SIM details, collected
details are sent to registered alternate number.
Step 1: START
Step 2: Checks the SIM details.
Step 3: If the SIM differs from the earlier one, retrieve the SIM details.
Step 4: Collected details are sent to user’s registered alternate number.

A. Captured photograph
If the command sent as SMS is “camera” then the front-camera of the device is turned on, photo is
captured and sent to the registered email address
Fig 3: Captured photograph
B Location details
If the command sent as SMS is “track” then the location details including latitude and longitude are sent to the registered alternate number, provided GPS is turned on in the device

Fig 4: Location details
5. Conclusion
The proposed method increases the lifetime of network, improves the throughput, reduces the power utilization, end to end delay and increased packet delivery ratio.

References

[1]. Virtual Safe: Unauthorized Walking Behaviour Detection for Mobile Devices Dakun Shen, Ian Markwood, Dan Shen, Yao Liu University of South Florida, Tampa
[2]. G. Bajrami, M.O. Derawi, and P. Bours. Towards an automatic gait recognition system using activity recognition (wearable based). In Proceedings of the Security and Communication Networks, 2011 Third International Workshop on, pages 23–30, 2011.
[3]. M. O. Derawi, C. Nickel, P. Bours, and C. Busch. Unobtrusive user authentication on mobile phones using biometric gait recognition. In 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pages 306–311, Oct 2010.
[4]. Y. Gao, C. Zhou, and D. Shang. A smart phone anti-theft solution based on locking card of mobile phone. In Proceedings of the 2011 International Conference on Computational and Information Sciences, pages 971–974, 2011.
[5]. T. Saha H. Lu, J. Huang and L. Nachman. Unobtrusive gait verification for mobile phones. In Proceedings of the 2014 ACM International Symposium on Wearable Computers, 2014
[6]. Y. Ren, Y. Chen, M. C. Chuah, and J. Yang. Smartphone based user verification leveraging gait recognition for mobile healthcare systems. In 2013 IEEE International Conference on Sensing, Communications and Networking (SECON), June 2013
[7]. M. Shahzad, A. X. Liu, and A. Samuel. Secure unlocking of mobile touch screen devices by simple gestures: 2013.
[8]. H. M. Thang, V. Q. Viet, N. Dinh Thuc, and D. Choi. Gait identification using accelerometer on mobile phone.
[9]. J. R. Usherwood, A. J. Channon, J. P. Myatt, J. W. Rankin, and T. Y. Hubel. The human foot and heel–sole–toe walking strategy
[10]. M. Muaaz and R. Mayrhofer. Smartphone-based gait recognition: From authentication to imitation.