International Journal of Computer Applications Technology and Research
Volume 5–Issue 12, 730-732, 2016, ISSN:-2319–8656

Smartphone Remote Detection and Wipe System using SMS

Nilesh Dorge
Department of Computer Engineering, Savitribai Phule Pune University, Pune, India

Atish Pawar
Department of Computer Engineering, Savitribai Phule Pune University, Pune, India

Suraj Khandbale
Department of Computer Engineering, Savitribai Phule Pune University, Pune, India

Abhijit Jachak
Department of Computer Engineering, Savitribai Phule Pune University, Pune, India

Shubham Nirmal
Department of Computer Engineering, Savitribai Phule Pune University, Pune, India

Prof. Jitendra Musale
Department of Computer Engineering, Savitribai Phule Pune University, Pune, India

Abstract: The project based on mobile application which functions on an Android operating system. The objective of this which enable the user to locate the mobile phone in a silent mode to General mode when it is misplaced as well as if it is lost and wipe the data from the device. To create an account the user needs to provide his /her mobile number, a password and 4 trustworthy numbers this completes the registration process. The application, which is still in a deactivation mode, will operate only when the phone is misplaced and the user sends the set password/ pass code from one of the 4 trustworthy numbers to one's own mobile number. This will change the profile of the misplaced phone i.e. switch it from the silent mode to the sound mode. It will also send an acknowledgement to the trustworthy number from which the user has sent the message. Furthermore, it will also provide the location with and also if mobile is lost then we can take back up from another mobile by using same application, we can also wipe the data remotely by sending the message**.**

Keywords: ***Real-time, location tracking, Android.***

1. INTRODUCTION

In this paper we are focusing on three major topics GPS, Mode conversion (silent to general) and Data Wipe & Recovery. Rapid evaluation of wireless technologies has provided a platform to support system in the domain of location tracking. Mobile devices such as phones are common and internet access is possible everywhere in daily. Worldwide out of 100% people who uses smart phone Probably 80% and above uses android operating system according to International Corporation market researches. Android is common with its open source nature and working capabilities on in expensive mobile devices. Location tracking is continuously monitoring a device by using obtained coordinates with GPS. Nowadays smart phone is mostly used by every human , sometimes some people face problem in finding the mobile are controlled by the smart phones, this Application helps to find the mobile when it is misplaced. This application is useful, when it is in silent and forgotten where it is placed.As enabling all the users to receive advantages and satisfaction, the smartphone have been applied in a variety range and it expand a range of security threat. Specially, security threat of the android phone by loss or stolen may cause the user data disclosure such as credit cards, login IDs, contacts, message, photos etc. To prevent these problems, network operators should provide some security by which intruder can not use mobile devices by and also need to support the remote lock and wipe services which delete users' data as in the state of factory reset.

2. ANDROID BASED ENERGY AWARE REAL-TIME LOCATION TRACKING SYSTEM.

EWAREL adopts a client-server scheme. User client is an android application that performs real-time background tracking and synchronizing to server in a given interval while internet connection is present .It stores location changes when internet access in not possible and synchronize as soon as mobile device is connected to internet. Monitoring client is also an android application to accomplish tracking of people to monitor. Monitoring application alerts when one of the clients does not send location data at predefined interval to server and becomes unreachable.

3. AUTO MODE CONVERSION

3.1 EXISTING SYSTEM

In the previous projects the message sent will be sent as a normal text message to the other mobile .But there is no application developed to change the modes of the mobile automatically by receiving a text message. For mobile recovery we have applications, which use Global Positioning System technology. If we want to change the mode we have to change it manually, this is the main disadvantage. So we have

proposed a new system to overcome the problems in the existing system

3.2 PROPOSED SYSTEM

In this project we will send a text message to mobile, it will check the message and it will help in converting the modes. There may be a situation where we cannot convert manually when the mobile is misplaced then it can convert from silent mode to general mode.

Fig 2:Mode conversion from silent to general by sending a message

4. THE REMOTE LOCK AND WIPE SYSTEM

4.1 THE REMOTE LOCK AND WIPE SYSTEM

It consists of a remote control module on a server and a command handling module on a smartphone (see Fig.1). The commands are sent by text message push notification message. For example, when the users send a lock command message to the smartphone via the remote control module, the remote handling module enables the password locking function to lock the smartphone. Similarly, by sending a wipe command message, all personal data is remotely deleted.

4.2 COMMAND INTEGRITY PROBLEM

The remote lock and wipe service will be very useful when the smartphone is lost or stolen. However, there might be the case that the wrong user misuses this function by sending such commands to the normal users in order to interrupt the service. Thus, it is very important to check if the command is originated from the trusted server. In other words, the integrity of the commands must be checked. The traditional way to provide the integrity checking is simply to apply a digital signature scheme such as RSA or DSA signature. Note that RSA or DSA signature requires the key size of 1024 bits (i.e, 128 bytes) long to protect against active attackers over the wireless network. An obstacle here is that the command integrity checking should be provided only with the SMS message which is 80 bytes long

When the SMS command notification is sent, the remote control module creates a secret key from the password using PBKDF. Using HMAC function with the secret key, the message authentication code (MAC) is generated on the command message along with the timestamp which is added to protect against the well-known reply attack. Then, the command message is sent with the MAC to the designated smartphone.

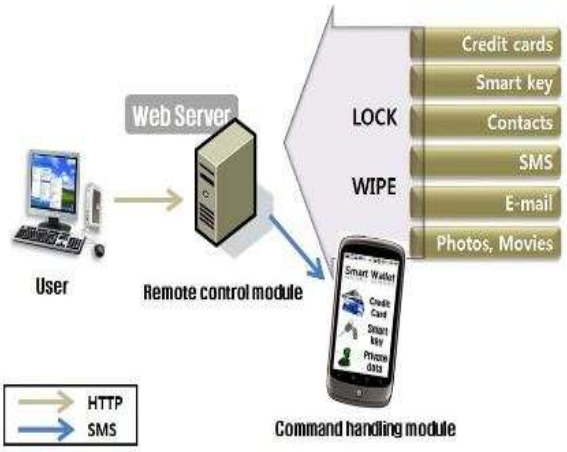

Fig. 1. Remote Lock and Wipe System

In server when the app is started by the user, user can perform 3 actions edit secret code ,start service and add contacts .Edit secret code will give permission to edit the secret code, add contacts will allow to add the contact numbers for client, start service will start the application. Now, client will start the application, after that user will enter the secret code, enter the receiver number and user will send the text message. When server receives the text message, it will check with secret code and perform different operations like tracking the location of device ,mode conversion (silent to General mode) And data wipe and recovery.

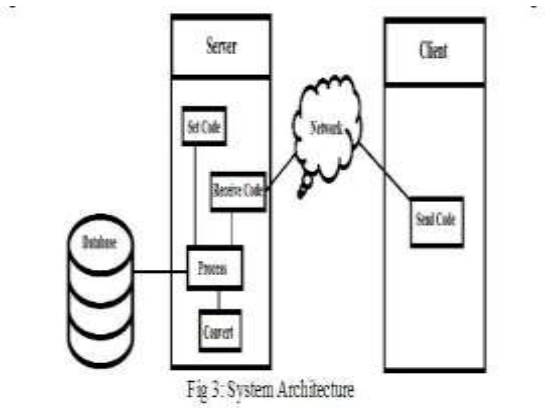

Fig 3: System Architecture

5. CONCLUSION

This application is developed in android platform and this provides higher curiosity to the android users. This system provides the location of device and efficient method for finding out the smart phones where it is placed(in silent mode) it is helpful in changing from silent mode to General Mode and also The remote lock and wipe service is necessary to protect against the private data disclose. At the same time, it must prevent the unknown user from launching DOS attacks that sends such commands to the normal users intentionally.

6. REFERENCES

[1]http://compnetworking.about.com/od/basicnetworkingconcepts/a/networktypes.html

[2]http://homeguides.sfgate.com/advantages-smart-house 8670.html

[3]http://en.wikipedia.org/wiki/Mobilesecurity

[4]Smartphone OS Market Share http://www.idc.com/prodserv/smartphone os-marketshare.jspast accessed January 15th, 2105.

[5]K.Jones and L. Liu, What where wiAn analysis of millions of wi access points,PORTABLE07. IEEE International Conference on Portable Information Devicespp. 25,29,2007

[6]Y . Cheng,Y. Chawathe, A. LaMarca, and J. Krumm, Accuracy characterization for metropolitan scale Wi - Fi localization, in Proceedings of the 3rd international conference on Mobile systems, applications, and services. ACM p.245 , 2005.

[7]Y.F .Chang, C.S. Chen, and H. Zhou, " Smart Phone For Mobile Commerce",Computer Standards Interfaces ,Vol . 31, Issue 4, June, 2009

[8]Sha k G. Punfa and Richard P. Mislan , "Smartphone Device Analysis", Small Scale Digital Device Forensics Journal , Vol. 2, No. 1, June, 2008.

[9]A . Menezes , P. van Oorschot , and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996

[10]RSA Laboratories, "PKCS 5 v2.0: Password - Based Crypto - graphy Standard",March, 1999.