© March 2017 | IJIRT | Volume 3 Issue 10 | ISSN: 2349-6002

Mobile Information Catalog Surveillance

Abinaya S, Madhi Vadhani K, Elavarasi V
Computer Science and Engineering
KCG College of Technology
Chennai, Tamilnadu, India

Abstract: **Context based Mobile Information Catalog Surveillance is a mobile phone based communication application. This application will give the notification to the user whenever they want to communicate with their mobile virtually.This application proved to get the recent call logs details when you send a command as message to the Android mobile device. It is used on Business point of view surveillance and Security.If the user need to surveillance his mobile and he need to access the last message, call logs or you need to access the contacts which may be important ,our application will get such information and pass them in the text message format to the commander mobile. We can also change to profile mode, divert the calls to other mobile and get the location of the mobile through GPS. The commander is the owner who sent the command to the mobile to surveillance his mobile.**

I. INTRODUCTION

The objective defines whenever you want to access your device virtually and get some details dynamically.This app will satisfy your need for your convenience. To find the contact log from the Android mobile devices whenever we require the contact and change the profile mode of the device for our convenience. We can also change to profile mode, divert the calls to other mobile and get the location of the mobile through GPS. This application proved to get the recent call logs details when you send a message to the device. You can get the contact list based on alphabetic order.

II.RELATED WORK

K.S. Kuppusamy, Senthilraja.R , G. Aghila et.al [4]The smartphone usage among people is increasing rapidly. With the phenomenal growth of smartphone use, smartphone theft is also increasing. This paper proposes a model to secure smartphones from theft as well as provides options to access a smartphone through other smartphone or a normal mobile via Short Message Service. This model provides option to track and secure the mobile by locking it. It also provides facilities to receive the incoming call and sms information to the remotely connected device and enables the remote user to control the mobile through SMS. The proposed model is validated by the prototype implementation in Android platform. Various tests are conducted in the implementation and the results are discussed.

Jayvant H. Devare, Sonali D.Kotkar, DipaliN.Nilakh, Priyanka S.Solat et.al[6] Now a dayswe are dependent on our mobile phones, if we forget the phone at home it seems we have lost a limb. That time we think that it would be good to access our mobile remotely, like the web browser. The application like iMobile, instead of accessing the computer remotely, we will access the mobile phones. An application creates a TCP connection with web application and the mobile phone and retrieves all the data like missed calls, contacts and message. Sometimes Cell Phone companies block “Incoming” TCP connection towards the phone over network to overcome this problem, through the application SMS could be sends with the application IP addresses and then it would be the mobile phone establishing the TCP connection. Then, it could easily and securely send the data using the GSM or 3G network. The AES algorithm used for the security purpose.

Bilal Shebaro, Oyindamola Oluwatimi, Elisa Bertino[1] Mobile Android applications often have access to sensitive data and resources on the user device. Misuse of this data by malicious applications may result

in privacy breaches and sensitive data leakage. An example would be a malicious application surreptitiously recording a confidential business conversation. The problem arises from the fact that Android users do not have control over the application capabilities once the applications have been granted the requested privileges upon installation. In many cases, however, whether an application may get a privilege depends on the specific user context and thus we need a context-based access control mechanism by which privileges can be dynamically granted or revoked to applications based on the specific context of the user. In this paper we propose such an access control mechanism. Our implementation of context differentiates between closely located sub-areas within the same location. We have modified the Android operating systems othat context-based access control restrictions can be specified and enforced. We have performed several experiments to assess the efficiency of our access control mechanism and the accuracy of context detection.

Ann Skudlark, AT&T Labs et.al[5] In this paper1 a study of SMS messages in a large US based cellular carrier utilizing both customer reported SMS spam and network Call Detail Records (CDRs) is conducted to develop a comprehensive understanding of SMS spam in order to develop strategies and approaches to detect and control SMS spam activity. The analysis provides insights into content classification of spam campaigns as well as spam characteristics based on sending patterns, tenure and geolocation.

Deepak Kumar and Mohammed Abdul Qadeer [3]This paper describes a software application for android mobile platform that discovers various excited applications of SMSs over its traditional text messaging application. It shows how various features in android mobiles can be automated by SMS. By this application user can perform various operations in its mobile even if mobile is very far from him , like by sending a single text message we can fetch and store our contact numbers, fetch our device's location, auto respond to the incoming messages, send SMS from our remote mobile, fetching SIM and mobile details used for GSM network. Convenience to the user, security and efficiency are main issues that are considered. This application makes the use of services like telephony, location based services (LBS) and native android applications.

Bhushan Sonawane,Sagar Sonawane, Pradip Nikalje,SandipNagare[2]The application present on Mobile doesn't give extra features. They are not sufficient for our daily life. And if anyone is really interested should download from internet, but the problem is each and every function should download one by one and it causes cost too. Mobile users should have functions like when Mobile is loss to get it back. Also we forgot our mobile at home and we want to call someone and we don't remember contact number to call from somewhere else. So we face a problem. Suppose our mobile misplace and we already keep it as Silent. so there is problem of locating it. And we forgot our mobile at home and we need to attend all calls which are coming to our mobile. Security is more preferred by Mobile users. Hence to provide more security and easy availability we are providing a software named Windows Mobile Functioning controlling through SMS and Mobile Tracking.

III MODULES

This application proved to get the recent contact details when you sent a message to the device. And we can change the Profile mode of the device for need to avoid your device from other people surveillance.This application is works on sorting algorithm.We can also change to profile mode,divert the calls to other mobile and get the location of the mobile through GPS. If it is highly confidential then we can shut down our device from outside of the area.Then you may want to see contact list those which are think from your mind alphabetical contacts you can get from your mobile.

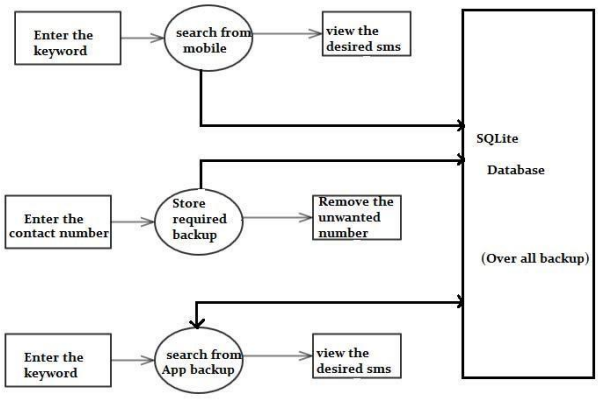

Fig:Arcitecture diagram

A)Send the SMS from mobile :

SMS stands for short message service. SMS is also often referred to as text , sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The SMS Manager manages SMS operations such as sending data to the given mobile device. You can create this object by calling the static method SmsManager.getDefault() as follows:

SmsManager smsManager = SmsManager.getDefault();

Once you have SmsManager object, you can use sendDataMessage() method to send SMS at the specified mobile number as below:

smsManager.sendTextMessage("phoneNo", null, "SMS text", null, null);

Apart from the above method, there are few other important functions available in SMS Manager class.

B) Database read the Message Body

This article is useful for you if you want to develop your own SMS (or another service) handler. As a sample, I choose received SMS handler that receives SMS, encrypts them, and puts into the SMS table of the Android system database.Manifest is a very important part of an Android application. You can find everything about the Android manifest by this link.And now I'll try to describe every line that is important for us.The first are permissions . The application must receive, write and read SMS from the database.The main class that receives the SMS is SmsReceiver. It extends BroadcastReceiver class. This is the main concept of any Android service or receiver. Any child of BroadcastReceiver must contain the on Receive method, which receives Context and Intent parameters. You can find all additional information on the Android developer documentation site.

C)Compare the message content to Database :

TextSecure can use SMS/MMS to communicate with non-TextSecure users. The app can therefore be used to replace the default SMS/MMS application. Messages that have been sent via SMS/MMS and messages that have been sent via the user's data connection can be distinguished by color. Green text bubbles indicate SMS-based communication and blue text bubbles indicate communication over a data connection. By default, TextSecure will send the messages over the user's data connection if possible. This means that if the user sends a message to another registered TextSecure user, there is no SMS charge associated with the message. It is merely treated as an additional data transfer. If the data connection is unavailable, the application will fall back to using SMS/MMS to transport the message. The application will automatically encrypt all conversations held with other registered TextSecure users. In the user interface, encrypted messages are denoted by a lock icon. Media and other attachments are encrypted in the same way as other messages. Regardless of whether the messages were sent to another TextSecure user or not, TextSecure can store the messages in an encrypted database on the user's device if the user has a pass phrase enabled.

D)To retrieve the Contacts from Mobile :

Data Doctor is one of a number of so-called recovery tools on the market for various tasks such as retrieving lost photos and mobile phone messages. Some are totally rubbish. Before and after using anything of this sort, we recommend you update your Internet Security or anti-virus software and run a security scan on your PC and check for anything that might cause concern. Most such programs let you have a trial of the software whereby it scans the media card or disk to be recovered and shows you whether or not your images are still there, then puts up a pay-wall so you pay a fee to get at the content you want to retrieve. Any such software you use should give you at least given you this much information before you pay for it. Software to retrieve information from a SIM card works in a similar fashion but won't work if there's PIN code on the SIM card preventing access. The other issue is whether the messages you want to recover were stored on the SIM in the first place or were actually stored on the phone memory. If you've removed the SIM from one phone and put it in another handset, this could be where your messages have gone. If you deliberately deleted the messages, they may simply be gone forever. Although forensics will allow messages to be recovered, it's doubtful that a program such as the one you have will be able to dig sufficiently deep into the phone to do this. Two other file recovery options to try are Recuva and

Restoration. We've used these with some success for getting back accidentally deleted items.

E)To retrieve the Message from Mobile:

We receive the information through the SMS for our mobile at many times. SMS -based transactional alerts are SMS's sent each time a change occurs in a bank account, for example, or when our credit card is used then we will get an SMS on our mobile phone.
Suppose we left the mobile we can't access the information from our mobile without any intruder. Reading cell phone text messages online is an idea that crosses the minds of many parents of tweens and teens. Businesses can also use this capability to track monitor any individual abuse of company cell phones as well as recording business text conversations. Multimedia phones now make it possible to read text messages online by allowing access to Internet applications that will track cell phone messages sent through Short Message Systems. Software is available to track messages sent from cell phone to cell phone.

F)To change the profile Mode:

This is the ability to set volume level, turn on and off radios, and adjust screen brightness based on the time of day, your location, the power situation, or just your preference. Multiple User Mode is the ability to give the phone to another person, let them log in with their own account information, and any changes they make are done under their account. They give the phone back to you, and you'll have none of their clutter, photos, emails, or apps on your account. This enables you to give your phone to a relative to play with at a picnic and not get it back with 10,000 pay apps downloaded via Google Play, and all your email and icons deleted.

G)To change the airplane mode :

Sure, Android users don't have fingerprint scanners (well, maybe one), but that doesn't mean you're stuck when it comes to security. Here are some of the best apps you can download to boost security on your phone without buying all-new hardware. Of course, it's worth pointing out that any airplane mode security is only a stumbling block. Securing your data on your phone should be done with a complete remote wipe solution (Google even has its own already associated with your account).

At best, any airplane mode security will keep curious eyes or clumsy thieves out from unwanted misbehaviour while attending a call.

H)To retrieve the Call logs from Mobile :

To get the call logs which is may be Incoming call logs or Out going call logs or missed call logs. If suppose the user want to get the recent call logs then he send the SMS to the current working android mobile and he get the recent contact logs that may have incoming call logs otherwise outgoing call logs or it may have missed call logs.

I)G-Mail Module

This module is designed to get the details through g-mail when internet connection is available in user's mobile.

IV.CONCLUSION AND FUTURE ENHANCEMENT

In this paper simply we put our idea of the communication of mobile phone to mobile phone. The important part of this paper is that,we can access the mobile phone data from basic mobile phone .That paper includes call logs, messages,call divert,sound profile mode and location tracking. The proposed model facilitates accessing of the device from a remote location using any other mobile terminal. The system has been designed in such a way that the mobile terminal used for accessing the remote android device, need not be an android device.

REFERENCE

1. Bilal Shebaro, Oyindamola Oluwatimi, Elisa Bertino "Context-based Access Control Systems for Mobile Devices" DOI 10.1109/TDSC.2014.2320731, IEEE Transactions on Dependable and Secure Computing

2. Bhushan Sonawane, Sagar Sonawane, Pradip Nikalje, Sandip Nagare "Remote Windows Mobile Function Controlling Through SMS

3. Deepak Kumar and Mohammed Abdul Qadeer "SMS Based Emerging Technique For Monitoring And Controlling android mobile" IACSIT International Journal of Engineering and Technology, Vol. 4, No. 6, December 2012

4.K.S.Kuppusamy, Senthilraja.R ,G.Aghila "A model FOR REMOTE ACCESS AND PROTECTION OF SMARTPHONES using Short Messeages Service"

International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012

5. Ann Skudlark, AT&T Labs "Characterizing SMS spam in a large cellular network via mining victim spam reports" 2600 Camino Ramon San Ramon, CA 94583.

6. Jayvant H. Devare, Sonali D.Kotkar, DipaliN.Nilakh, Priyanka S.Solat "iMobile: Remote Access for Android Phones" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 4 April, 2014 Page No. 5360-5363.
7. Hossein Falaki, Ratul Mahajan Srikanth Kandula, Dimitrios Lymberopoulos, Ramesh Govindan, Deborah Estrin: Diversity in smartphone usage, Proceedings of the 8th international conference on Mobile systems, applications, and services, ISBN: 978-1-60558-985-5
8. Bo Li and Eul Gyu Im: Smartphone, promising battlefield for hackers, Journal of Security Engineering , vol: 8 no: 1, 2011, pages 89-110
9. Karsten Sohr, Tanveer Mustafa, and Adrian Nowak. 2011. Software security aspects of Java-based mobile phones. In Proceedings of the 2011 ACM Symposium on Applied Computing (SAC '11). ACM, New York, NY, USA.
10. J. F. Jerome, Android a programmer's guide, MGH Publisher, Second Editon.
11. R. Meier and Wrox, Professional Android Application Development, First Editon.
12. N. Park, et al., "The security consideration and guideline for open LBS using XML security mechanism," ASTAP 04/FR08/EG.IS/06, 2004.
13. H. Srivatsa, "Location-based services," IBM Paper, November 2002.
14. Mohammad Zahaby, Ganesh D. Bhutkar, M. L. Dhore, "An Improved GPS Location Tracking with Kalman Filter and Velocity Renovation", ICCNS 2008, Pune, India, pg 475-478.
15. Hyunkyu Yu, Student Member, IEEE, GoohyunPark,Student Member, IEEE, Hangyu Cho, Student Member, IEEE,Changeon Kang, Senior Member, IEEE, and Daesik Hong, Member, IEEE, "SNR-Independent Methods for Estimating Maximum Doppler Frequency", IEEE SIGNAL PROCESSING LETTERS, VOL. 12, NO. 5, MAY 2005.