Surveillance and Securing the Mobile Information on Context Based Approach

B.Hema[1] , Assistant Professor / IT
R.Narmatha Devi[2] , M.Indhu[3] , B.Tech / IT
Department of Information Technology
Velammal Insitute Of Technology,Chennai

Email: [1]baluhema@gmail.com , [2]narmathadeviramar@gmail.com , [3]indhumailss@gmail.com

Abstract:-Context based Mobile Information Catalog Surveillance is a mobile phone based communication application.The Short Message Service (SMS) allows text-based messages to be send from mobile telephones on a GSM network. .Many applications need the ability to do real-time notification when events occur. Often the people who need to be kept aware of events are in a remote location. Here the same is to giving the notification to the user when ever they want to communicate with their mobile virtually.To find the contact log from the Android mobile devices whenever we required the contact and change the profile mode of the device for our convenient. This application proved to get the recent call logs details when you sent a message to the device. Then you may want to see contact list those which are think from your mind alphabetical contacts you can get from your mobile. And you change the profile mode for your mobile and if you want Switch off your mobile you can. It is used on Business point of view surveillance and Security. Real time example if the user forgot his mobile at his home and context is very important to access the last moment data received by his mobile. Here context is nothing but the surrounding situation. If you need business point of view you need to access the last moment message otherwise to access the recent call logs which may be important or you need to access the contacts in alphabetical order. In that situation you need to give a privacy to your mobile device you can change your mobile to change the profile mode or to lock the screen. If suppose in your mobile is in silent mode you need anybody to want to access your mobile in your mobile surroundings you can change the mobile device into the normal mode.

Index Terms:-Context-based access control, smartphone devices, security and privacy, policies, mobile applications

———————————————————————————————————————*****——

1. INTRODUCTION

SMS is very common and widely used way of communication. Now-a-days we do most of the communication with SMSs. Today in the era of technology we want most of the things to be automated. Imagine that it would be great if we could perform various functions in our mobile phones even if it is far from us or it could respond automatically like an intelligent device. So now this can be achieved by our SMS software application which is developed for android mobile platform. By using this application we can operate many functions via sending a SMS to the mobile phone which is far from us without interception of operator and in this way our android mobile phone will act as intelligent device. This application establish client-server relationship between mobile phones in which the mobile requesting operations by sending SMS will act as client and mobile serving those operations will act as server. Various operations that can be performed by this application are listed as storing and fetching contact numbers, fetching the device's location, sending SMS to other mobile phones through our remote mobile, auto responding to the incoming messages, finding and fetch the details about SIM and mobile like and we can also switch off our mobile via sending a SMS to it. This application makes the use of both traditional and advance technology like telephony and location based services (LBS). These services are also used in various applications but we are presenting them in very different way from there conventional use.

There are some issues that have gotten more attention like convenience to the user, security which is very important and necessary aspect of this application and efficiency. To use this software application we have some fixed formats of SMSs that are needed to be sending on the android mobile on which application is installed. These formats are discussed later sections in this paper.

2. OBJECTIVE: Here objective defines whenever you want to access your device virtually and get some details dynamically ,this apps will satisfies your need for your convenience. To find the contact lag from the Android mobile devices whenever we required the contact and change the profile mode of the device for our convenient. This application proved to get the recent call logs details when you sent a message to the device. Then you may want to see contact list those which are think from your mind alphabetical contacts you can get from your mobile.

3. SCOPE OF THE PROJECT : Main scope of the projects is to give the surveillance to our mobile device through the SMS. Give the SMS details to the destination mobile and it will compare the SMS information and it will send the more relevant information to the user.

4. PROBLEM DEFINITION : Now we access that all above information only within the mobile or we should keep the contact details with our dictionary or dairy. We can't access the information wherever we want for our own requirements.

5. EXISTING SYSTEM : Mobile learning with cell phones offers a unique response to our need. .It can retrieve the data

from already define database in offline and it does not communicate with other mobile devices. And we cannot retrieve the data from other android device.

DISADVANTAGES :

1. We cannot communicate with other mobile without need any intruder.

2. We can't make remote access the prior information through the SMS for our own mobile device.

3. We can't save the mobile in remote access and can't make the business view for our mobile in remote access.

6. PROPOSED SYSTEM : 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. If it is highly confidential then we can shout 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.

ARCHITECTURAL DIAGRAM :
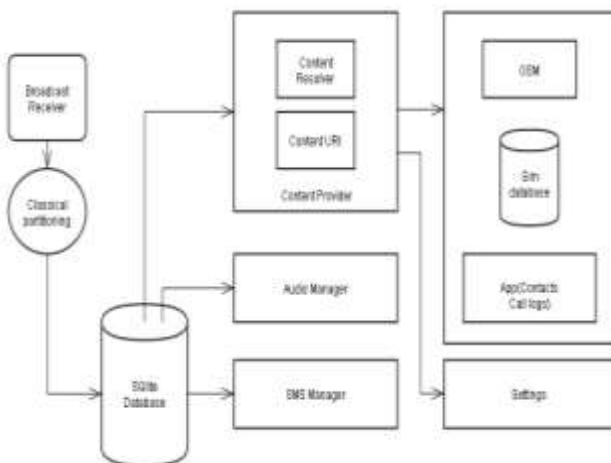
7. IMPLEMENTATION:

1. Database read the Message Body
2. To retrieve the Contacts from Mobile
3. To retrieve the Incoming Call logs from Mobile
4. To retrieve the outgoing Call logs from Mobile
5. To retrieve the Missed call logs from Mobile
6. To retrieve the Message from Mobile
7. To change the Profile Mode

7.1. 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 send DataMessage() method to send SMS at the specified mobile number as below:

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

7.2.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 onReceive method, which receives Context and Intent parameters. You can find all additional information on the Android developer documentation site.

7.3. 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.

7.4. 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

982

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.

7.5.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

7.6.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.

7.7. TO CHANGE THE AIRPALNE 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.

7.8.TO RETRIEVE THE INCOMING 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.   **7.9. TO RETRIEVE THE OUTGOING 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.

7.10.TO RETRIEVE THE MISSED 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.

8. OVERALL DIAGRAM:
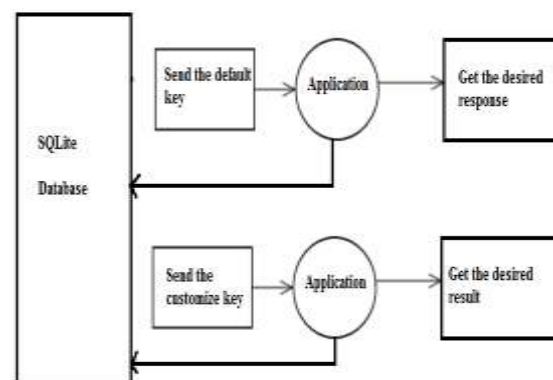
9. ADVANTAGES:
1. Can access our contact details when ever we want through remote access.
2. To provide the security for our android devices because we should change the profile mode through remote access.

3. Main objective is to give the surveillance to our android mobile.

4. Business point of view it is efficient to handle the situation and problems.

10. SYSTEM REQUIREMENTS:

SUPPORTED OPERATING SYSTEMS : The operating systems that the ArcGIS Runtime SDK for Android supports are the same as those listed for the Android SDK developed by Google. Generally, development is supported on Mac OS X (Intel), Linux, and Windows-based operating systems.

SOFTWARE AND PLATFORM REQUIREMENTS : The apps you build will run on Android phones and tablets with the Android platform version 2.3.3 (API level 10) and above.

ANDROID SDK SUPPORT : The following is required before you can develop with the ArcGIS Runtime SDK for Android in any IDE.Java Development Kit (JDK) 6is required. A Java runtime environment (JRE) is not enough for development Depending on which developer IDE you choose, you may need to download the Android SDK separately. Please refer to Get the Android SDK to determine if you need the SDK.Integrated Development Environment (IDE) support

ECLIPSE: Esri provides tools for the Eclipse IDE with the Android Developer Tools (ADT) plug-in. This is the best supported IDE to use when developing with the for ArcGIS Runtime SDK for Android.

INTELLIJ IDEA : Esri does not provide any tooling for IntelliJ IDEA with this release. However, we do provide everything you need to setup an IntelliJ IDEA developer environment for developing ArcGIS Runtime SDK for Android applications. Please refer to the install document to get your IntelliJ IDEA environment set up.

ARCGIS FOR SERVER AND ARCGIS FOR PORTAL VERSIONS AND PLATFORMS : To connect your app to ArcGIS for Server data or services, use ArcGIS for Server version 10.0 or later. To use ArcGIS for Server data when your app is offline, use ArcGIS for Server version 10.2.2 or later. You can use ArcGIS for Portal version 10.2 or later with your app.

CONCLUSION AND FUTURE WORK :

In this work, we proposed a modified version of the Android OS supporting context-based access control policies. These policies restrict applications from accessing specific data and/or resources based on the user context. The restrictions specified in a policy are automatically applied as soon as the user device matches the pre-defined context associated with the policy. Our experimental results show the effectiveness of these policies on the Android system and applications, and the accuracy in locating the device within a user-defined context. Our approach requires users to configure their own set of policies; the difficulty of setting up these configurations require the same expertise needed to inspect application permissions listed at installation time.

However we plan to extend our approach to give network administrators of organizations the same capabilities once a mobile device connects to their network. In this way, network administrators are able to block malicious application accesses to resources and services that may affect the security of their network.

We believe that such an approach is critical for assuring security of corporate networks when organizations allow users to "bring their own devices".

12. REFERENCES

[1]   R. Meier and Wrox, Professional Android Application Development, First Editon

[2]   Android.   [Online].   Available: http://www.android.com

[3]   N. Park, et al., "The security consideration and guideline for open LBS using XML security mechanism," ASTAP 04/FR08/EG.IS/06, 2004.

[4]   M. Tuisku, "Wireless java-enabled MIDP Devices as peers in grid infrastructure," Helsinki Institute of Physics, ERN.

[5]   H. Srivatsa, "Location-based services," IBM Paper, November 2002.

[6]   J. F. Jerome, Android a programmer's guide, MGH Publisher, Second Editon

[7]   Code. [Online]. Available: http://google.com/android

[8]   J. R. Cuellar, Location Information Privacy. B. 2002.

[9]   Srikaya (Ed.), Geographic location in the internet, Kluwer Academic Publishers, pp. 179–208.

[10]   S. Ravi, M. S. Chathish, and H. Prasanna, "WAP and SMS based emerging techniques for remote monitoring and control of a process plant," in Proc.2004 7th International Conference on Signal Processing.