Interference Detection System Using Android Emissary

Nitin Jagtap #1, Pravin.K.Patil #2

#1 Asst. Prof. Department of Information Technology, SSBT’s COET, Bambhori, Jalgaon
North Maharashtra University, Jalgaon.

#2 Asst. Prof. Department of Information Technology, SSBT’s COET, Bambhori, Jalgaon
North Maharashtra University, Jalgaon

Abstract—In the real world, every company, small firm and even educational institute focused on security of data. It is prime concern at everywhere so it is compulsory to protect the data from leaking outside. Leakage is very serious issues in the world. Authorised person having the sensitive data and handover the same to its responsible employees which can be detect through calculating guilt agent and like hood of the employee. But Nowadays Android mobile phones are used by company employee, firms employee, educational institute employee, and other organisation. In such a company’s security of the sensitive data such as source code, future plans, design specification, intellectual properties, copyright data, decision making report, product plans, trade secrets, students record and many other. Any responsible employee can leak this data and misuse it. Second he/she handover the sensitive data to the comptorator company’s employee in illegal manner in order to take over this, we are implemented the system “Interference Detection System using Android Emissary” which will keep track on user’s mobile such call, SMS, and its current Location through GPS.

Keywords: Android, GPS, SMS, Intrusion, Emissary.

I. INTRODUCTION

In enterprise, small firm or in educational institute authorised person must hand over sensitive data to responsible employee For example; financial data given to the financial employee for making balance sheet or for making financial transaction but that data was leaked out. Similarly, a company may have partnerships with other companies that require sharing customer data. We consider applications where the original sensitive data cannot be perturbed. Perturbation is a very useful technique where the data are modified and made “less sensitive” before being handed to agents. For example, one can add random noise to certain attributes, or one can replace exact values by ranges [13]. However, in some cases, it is important not to alter the authorised person data. Watermarks can be very useful in some cases, but again, involve some modification of the original data. In addition, watermarks can sometimes be broken if the data recipient is malicious [13].

In every enterprise, data leakage is very serious problem faced by it. An authorised person of enterprise has given sensitive data to its responsible employee but in most of the situation responsible employee leak the data. That leak data found in unauthorized place such as on the web of comparator enterprise or on laptop of employee of comparator enterprise or on comparators laptop. It is either observed or sometimes not observed by authorised person of the company. Leak data may be source code or design specifications, price lists, intellectual property and copy rights data, trade secrets, forecasts and budgets.

Android mobile phones are the important aspect of today’s digitized world, they are everywhere in the market but the impacts happening from it is necessarily considerable. In Company mostly all employee has the Android mobile phones in working hour. Employees may do make conversation, passion and gossips over the android mobile instead of doing their work. We can say some trusted responsible employee may leak the company’s sensitive data such as its source code or design specifications, price lists, intellectual property and copy rights data, trade secrets, forecasts and budgets, future plans, future work, decisions making, plant setup and revenue report even after maintaining security. To protect against the leaking of this sensitive data to the outside world is serious problem as per the company’s, small firm and educational institute’s privacy and security policies.[12] In some cases responsible employee may crossed the company physically in working hours or employee may enter in restricted zone where the company’s sensitive work is maintained or employee may enter in the other department without major permission for the interference and data stealing purpose which is also a serious problem in the company’s security point of view. So after considering this entire factor and to avoid such situation we implemented the system called “Interference Detection System using Android Emissary” which helps to avoid such problems. This system will tracks the Incoming call, Outgoing call, Incoming SMS, Outgoing SMS along with its content and other than this it will track the current location of the employee that where that employee is currently exists [10] [11]. This all task will be monitored by the authorised person of the company with valid authentication. As soon as the employee will receive the call from unknown or known number an alert will be sent to the authorised person’s mobile device and website for log
and analysis purpose. Also the responsible employee will make a call this alert will be also sent to the authorised person’s mobile in the form of mail. In this mail the content will be Call from, Call duration, Call date, Call time will be included for details and security purpose. If responsible employee crossed the specified ecological area or entered in confidential zone of the enterprise, small firm or in educational institute or we can say latitude and longitude of the enterprise, small firm or in educational institute then an alert will be sent to the Authorized person’s mobile. Actually and reasonably this system is very important in terms of security and privacy of the company. This system is not only inadequate to track over the responsible employee but also we can track the children’s location whether they are at college or outside or kidnapped by some criminals which major concern in parent’s point of view is. We can also track the location of the criminal [5] [6]. It plays an important role in government organization to track over the doubtful person in the organization and administrator can easily track the responsible employee’s activity with their mobile phones i. e. what kind of data is coming to mobile and what kind of data is going from their mobile phones. So this system is very important in terms of security and privacy of the company, organization, college and institute.

II. EXITING SYSTEM

Various organizations have taken a server regarding “Interference Detection System using Android Emissary”. They found that there is need to give a condition to track the responsible employee’s call, SMS, and current location but it all can be done over the Bluetooth technology and it has many of drawbacks. There are some drawbacks of the existing system approach:
1. Less dependability
2. Not able to gives the details of the calls, SMS, and Location
3. High cost
4. Platform dependent
5. Only one user can be track through the above approach, if multiple user can call and SMS at a same time the system is unable to give efficiency and proper output it get hanged.
6. Its mandatory that Bluetooth should be inbuilt in responsible person’s mobile device these drawbacks are overcome by our proposed system “Interference Detection System using Android Emissary” which is discussing in proposed approach.

III. PROPOSED SYSTEM

We proposed the system called “Interference Detection System using Android Emissary”. These overcome the drawback of Bluetooth technology by wireless Wi-Fi technology. This system tracks the movement from responsible employee’s mobile phone and sent through Wi-Fi to the authorised person. In this proposed system we are dealing and programming with the android operating system which provides the better indoctrination litcheness [3]. “Interference Detection System using Android Emissary” provides more dependability, if many user call, SMS at a one time the system does not fails and provides proper output to the authorized person’s in the form mail alert.

In this system Incoming call, outgoing call, responsible employee’s current location can be tracked and sent to the authorized person’s mobile. For this we implemented the Android Emissary which will be concealed in the responsible employee’s mobile phone and runs in the backdrop and constantly sends the alert to the administrator from employee’s mobile device [11]. If responsible employee crosses the company’s location say latitude and longitude then an alert will be sent to the authorized person of company with exact location, name, and mobile number of responsible employee. For gathering these all services, we proposed the system entitled “Interference Detection System using Android Emissary”.

IV. IMPLEMENTATION

Following figure shows the graphical representation of the “Interference Detection System using Android Emissary”.

![Architecture of Interference Detection System using Android Emissary](image_url)

Fig. 1 Architecture of Interference Detection System using Android Emissary.

In this system we developed following modules
1. Android Emissary
2. Tracking of responsible employee call and SMS (Incoming and outgoing)
3. Tracking of responsible employee’s Location
4. Mail alert

All these modules keep track of the Call, SMS, and current Location of the responsible employee. In the (1) module we implemented the android Emissary which is be installed in the responsible employees’ mobile device which runs in the backdrop movement on the android operating system. This android emissary is kept tracks on the ongoing movement in the mobile device of responsible employee so far and sent an alert of call, SMS, and location of responsible employee to the specified website address and mail. In (2) module the tracking of call can be done using (1) module in which caller number, call time, call duration, call date will be tracked and sent to the administrator’s mobile device. This is really beneficial for the company is the doubtful and frequent caller number is found then action strict action will be taken against that particular responsible employee if he found impostor, at the same time logs is being maintained on the website server and again module tracking of SMS of responsible employees has done using (1) module in which incoming SMS. Outgoing SMS along with the material of the SMS, also verifying the number is right or wrong. This type of analysis has done and as soon as the SMS sent or received by the employee’s android mobile phone an alert with above information will be sent to the authority of the company. If the SMS content found sensitive the further action will be taken against the responsible person. In (3) module tracking of responsible employee’s current location has specified. If responsible employee crosses the specified threshold or geographical area or restricted zone of the enterprise, small firm or in educational institute an alert will be sent to the authorized employee’s mobile phone and also on the website of the company, this is really helpful for the responsible employee which is not crossed the geographical area of the company.

In (4) module an alert sent to the authorized person using (1) module and also the logs maintained in the centralized web server of the company for analysis and security purpose. For implementing the above six module we required following permission of Android programming such as
1. android.permission.READ_SMS
2. android.permission.WRITE_SMS
3. android.permission.RECEIVE_SMS
4. android.permission.SEND_SMS
5. android.permission.CALL_PHONE
6. android.permission.READ_PHONE_STATE
7. android.permissionINTERNET
8. android.permission.ACCESS_FINE_LOCATION
9. android.permission.RECEIVE_BOOT_COMPLETED
10. android.permission.READ_CONTACTS
11. android.permission.ACCESS_NETWORK_STATE

After including this permission in AndroidManifest.xml we will able to get the all alerts regarding call, SMS, and Location of the employee [3][10].

V. RESULT AND DISCUSSION

We found the following results by implementing the system. This is our main movement showing in fig.1 hello world which keep track of the call, SMS, and current location of the responsible employee. This .apk file install in responsible employee’s android mobile phones and its consent will be hidden from the responsible employee of the small firm, enterprise or the educational institute. This android emissary will send the all position as an alert to the authorized employee’s mobile phone. This fig 3 is an alert received by the authorized employee’s when responsible employee has an incoming call on his mobile phone. Similarly when responsible employee made call an alert will be sent to the administrator’s mobile with its complete details such as shown above employee’s number, department, call from, Time, and Call duration.
This all information will be maintained to the server also that authorized employee can logged into server and check also if he failed to receive an alert from a responsible employee. Same alert used by the authorized person when he when responsible person has an incoming SMS on his mobile phone. Same alert used by the authorized person responsible employee has an outgoing SMS on his mobile phone. In this way alert can be received by the authorized person through which can Interference can be stopped and we can easily find the doubtful one in the company.

VI. CONCLUSION

The above system is very important name as Interference Detection System using Android Emissary as per as security and privacy of the security are concern. It is based on the android operating system. This system tracks the movement of responsible employee’s day to day through the movement of their mobile phone by tracing incoming and outgoing call, SMS of responsible employee of the company. The above movement has done by the authorized person by handling alter. This is very helpful for the government agencies to track the movement of the person who are having criminal background.

REFERENCES