iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 5 Issue: XI Month of publication: November 2017

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

Automatic Identification and Notification of Threats in Text, Voice or Video Communication in Defence and Corporate Sectors

Miss. Elizabeth Pathipallil[1], Miss. Manisha Adarshe[2], Miss. Shayanika Hazarika[3], Master Shubham Vasekar[4], Prof. Sunil Rathod[5]
[1,2,3,4,5] *Computer Department, Dr D Y Patil School Of Engineering, Lohegaon Pune, Savitribai Phule Pune University, Maharashtra India*

Abstract*: Communication through various means has made human life simpler and faster but exponentially increased the threats in security of information getting transferred in any form like voice, text, audio, video or any other format. This paper proposes system for automatic identification and notification of threats in text, voice or video communication in defence & corporate sectors. The system is combining a Smartphone App, Global System for Mobile Communications (GSM) module and server which will track and check the device activities automatically and decides whether the call, text message going out of the organization is a security threat or not. The proposed system provides completely automatic solution and it provides an instant acknowledgement of the security threats to the organization without any human intervention or any external device for interception. This system uses Android based mobile phones for the software to be run. Nowadays Smartphone are equipped with built-in sensors and Application Program Interface (API). The proposed system uses GSM module to send the data to the server.

Keywords: Threat, Smartphone, Android, Security, Interception, GSM

I. INTRODUCTION

Employee monitoring systems are widely used by many companies nowadays. These systems allow company

Administrators/managers to monitor and supervise their employees from a central location, in which Manager should be always physically present to monitor their employees [1][3]. Some companies use mobile spy software for cell phones to log activities such as text messages , web history , Global Positioning System(GPS) locations etc[2].Such programs are installed on company computers to allow managers to take screenshots and monitor Emails, applications used, and even what keys were pressed[2]. With the development of the Smartphone, similar monitoring systems are available for company mobile phones. This development allows companies to monitor even mobile employees like field employees or drivers. Based on the experiences and findings of the field experiments, we propose a new systems and methods for automatic identification and notifications of threats in text voice or video communication. In our system the server decides the severity of the threat and decides the further activity to be performed such as blocking the device or blocking the SIM. An Android application is written with new and reusable application building blocks, such as activity; broadcast intent receiver, service, and content provider. After an application is written, it is deployed in a Zip-compatible archive, Application(apk) file, or the Android package file. An Android package file contains codes, resources, and a special XML file called the Android Manifest file. The manifest file contains basic information about an application such as the package name, component descriptions, and permission declarations. Android relies on Linux for system services such as security, memory management, process management, network stack, and driver model. Java Server pages (JSP) is being used at server side. Java Server Pages are built on top of the Java Servlets API , so like Servlets, JSP also has access to all the powerful Enterprise java APIs, including Java Database Connectivity(JDBC), Java API for XML Processing (JAXP) , etc. Any java class that follows certain design conventions is a JavaBeans component . JSP technology directly supports using JavaBeans components with standard JSP language elements. We can easily create and initialize beans and get and set the values of their properties. MySQL is a leading open source RDBMS. MySQL is also a multi-user, multithreaded database management system. MySQL is especially popular on web based server programming model. As it is free database server no licence key is required for the server based programming model.

II. LITERATURE REVIEW

New generation employee tracking system such as telephony manager tracks all incoming, outgoing calls and sms. Android mobile terminal is connected to high speed 3G network for effective data transfer between two mobile terminals. The tracking system is very secure due to implementation of Web Service Security (WSS).The system makes use of cloud technology to store and retrieve various telephony information using SOAP protocol. Some companies use employee monitoring software programs which allow companies to monitor every activity of the employees.

In [1], authors propose a monitoring system which allows managers to watch and interrupt all incoming and outgoing calls, texts and multimedia messages. Managers can also monitor their employees' location and access a history of where they have been. Managers receive SMS alerts if the employee is going outside an approved geographical zone or if he/she is receiving texts or calls from unapproved numbers. The system is not providing any privacy protection as managers can view the entire call history of the corresponding employee with the help of the cloud service. This system does not use any controller. The only processing unit in this system is the Smartphone itself. This may lead to high resource consumption

Another system [2], Mobile Spy employee monitoring software for cell phones is installed onto the company owned Smartphone to log activities such as text messages, web history, GPS locations, social media and more. The employee monitoring software then sends the information to your private viewing account that you can access online from anywhere. The log may include the following information like Text Message Logging -Logs all text messages sent and received on the monitored mobile phone, Social Networking Logs- Logs activity from Facebook, WhatsApp and Twitter messaging, YouTube Videos-See what YouTube videos are being watched on the phone with link to video, Phone Call -Logs information on each incoming and outgoing phone call, Email-View emails sent and received. The alert system will notify you about when prohibited activities occur. Activities will now be logged and rapidly inserted to your mobile monitoring account. You can login to your account by visiting the Login Page anytime.

In [3], a smart driver monitoring system combines sensors, Smartphone and embedded microcontroller. This system guarantees a comprehensive monitoring for driver performance during work and a full privacy protection. The system uses an Android App developed using Magnet Code 3.0 Smartphone Controller platform which is developed by Bizchip Technology Centre. The platform is built to run on Android OS. HC-05 FC-114 Bluetooth communication module is used to connect the Smartphone with the embedded microcontroller PIC16F777

The embedded Microcontroller Unit(MCU) module, which is already installed in the car, is switched on as the driver starts the car. The driver should open the Android App on the Smartphone. The App will prompt the user to enable the Bluetooth function in the mobile phone. Driver is then instructed to start the secured connection which is done by choosing "Run" from the setting. As long as the driver is in the mission the MCU continuously checks the Light Dependent Resistor(LDR), the door sensor and the temperature sensor. Also, it commands the Smartphone to send the charging status and GPS information. The MCU then evaluates the acquired data. If any unauthorized or illicit act is detected, the MCU saves log data including the kind and level of action, date and time. It also sends a command to Smartphone to take photos. Then it commands the Smartphone to set subject for Email and SMS, criteria and attachment list, and to send Email and/or SMS to the people in charge of monitoring.

The system will give the driver a period of time to stop the unauthorized act before sending the information to administrators again. A counter will increase as long as the unauthorized act is repeated. The administrators, according to the received data, can take the suitable reaction when the driver reaches the final destination, the GPS data are used to decide the end of the task. When the task is ended, the MCU commands the Smartphone to save the last report on "end of task" log data including date and time and to send the final Email and/or SMS to the administrators.

III.PROPOSED SYSTEM

There are semi-automated systems or manually controlled devices available for monitoring, tracing and intercepting the information passed on communication media in various possible forms.

The proposed systems and methods are providing completely automatic solution for monitoring, tracing and intercepting the information passed on communication media where there is less human intervention or even no human intervention

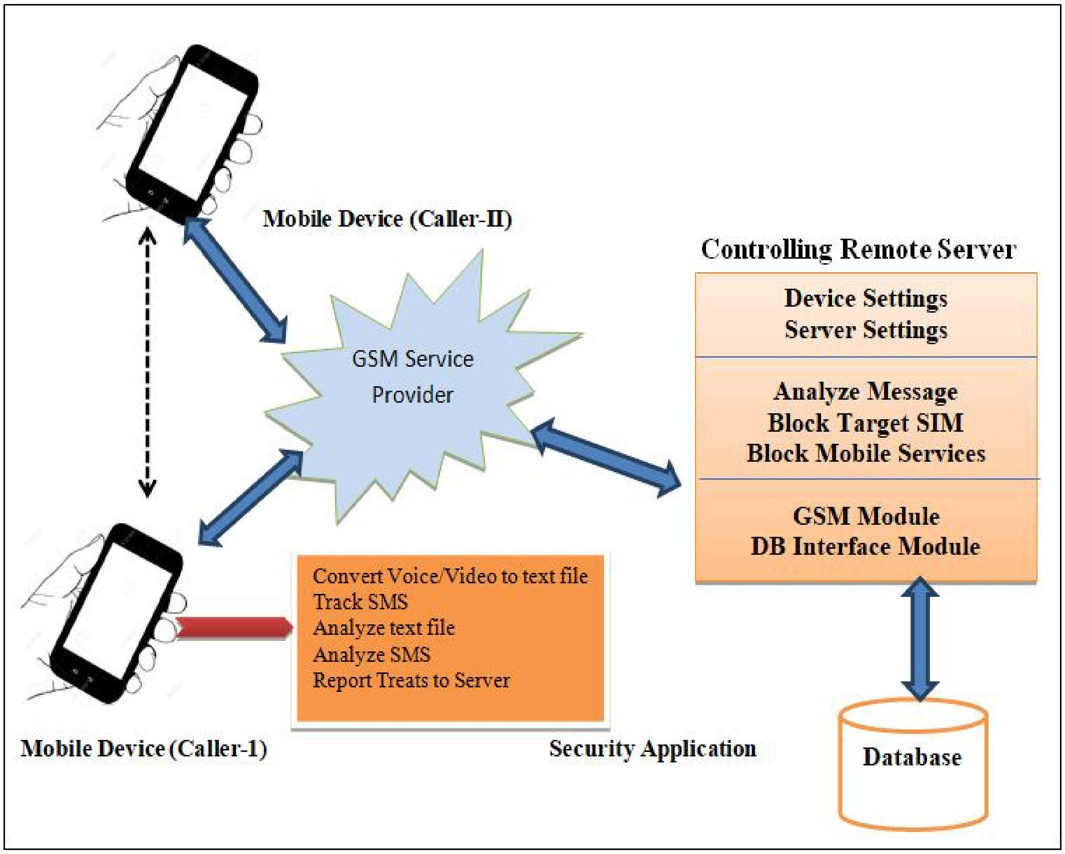

Fig. 1 Proposed System Architecture

As shown in fig 1. a mobile device will be used for tracing and tracking ongoing calls and messages and with Voice/Video to Text file conversion module for an incoming or outgoing call first we will check the type of call if it is a voice call record it and convert to text file, if it is video call extract voice from the recorded file and convert it into text file.

Now through Text Analysis Module read the text file which is converted of the call, check each word of the text file and compare it with the dictionary of objectionable words and set a counter and increment the counter on repetition of same word till word found is end of file repeat the same process and if and when found suspicious words (threats),text file will be transferred to the remote controlling server through GSM module , At Server side there will be automatic inspection of records once again by an algorithm and depending on severity of threats in records server will further send the record with all details of user to respective authority as well as store the same in a database. The Server will block SIM or mobile on command of the authority. If at Server side obtained record is not severe and just suspicious Server will just alert the concerned authority through Alert message analysis module.

IV. CONCLUSION

This paper proposes an integrated new system software for automatic identification and notification of threats in text, voice or video communication using Android Smartphone App. Using this system it is possible to intercept messages, video and voice calls of employee without any human intervention. It is also possible for the server to block the device depending upon the severity of the threat. Using the Smartphone app, the proposed new system can adapt to different fields such as Corporate and Defence sectors.

REFERENCES

[1] R. Anand, G. Arun Kumar and S. Murthy, "Mitter – Bitter Monitoring System Using Android Smartphone's," In Proc. Of International Conference on Computing, Communication and Applications (ICCCA), pp. 1-4, Tamilnadu, India, 2012.

[2] Mobile Spy: monitoring software : http://www.mobile-spy.com/employeemonitoring.html

[3] Mohammed HayyanAlsibai, Hoon Min Siang, "A Smart Driver Monitoring System Using Android Application and Embedded System" 2015 IEEE International Conference on Control System, Computing and Engineering, 27 - 29 November 2015, Penang, Malaysia