ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Mobile Application based on Android Platform for Real Time Device Monitoring and Data Transfer

Sujit Ingale[1], Shrirang Bhat[2], Nikhil Chandratre[3], Vivek Ingale[4], Prof.V.S. Phad[5]

B.E, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, Maharashtra, India [1,2,3,4]

Assistant Professor, Dept. of Computer Engineering,, SKNCOE, Savitribai Phule Pune University, Pune, Maharashtra, India[5]

ABSTRACT: In this paper, we are proposing a system which can monitor the data belonging to the family or a small organization and provide file transfer between the same. The system performs monitoring based on the various data collected from the devices like call logs, location information, SMS information with parental monitoring for under-aged children. The data will be collected at the central server. Then the collected data will be used for monitoring user devices. Same central server can be used for providing utilities such as Data Transfer with in the users belonging to same family/organization.

KEYWORDS: Android, Global Positioning System, Google API, Parental Monitoring, Pull-Push data.

I. Introduction

Android Devices are very much popular these days. According to Gartner (2010) [7], Android[12] is poised to become second most used mobile operating system in the nearer future. Not only youngsters but most of the people belonging to each age group possesses an android device these days. Growing number of android users has increased difficulty in monitoring process. As we know some small organizations give their own devices to their employees for the means of communication. It is very difficult to ensure that those devices aren't being misused. The basic idea is to build a system which can periodically collect data from such devices belonging to a family or an organization and monitoring of collected data. By monitoring the data, the system can identify whether the devices are being misused. The system is also capable of data transfer among those devices belonging to the same family/organization.

II. Related work

It is an important task to maintain all the information related to an Android device. Since there are no efficient methods to implement this strategy it becomes a difficult task. For a secured transmission to be implemented, some of the most featured encryption algorithms like Message Digest-5 or SHA (Secured Hash Algorithm) is used. These algorithms can be used to encrypt the message and transmit it to a Server through which it can be again transmitted to the destination[1][5]. This is the efficient way to propose the secured message passing, But the problem with this system is that these algorithms should be implemented following a specific methodology. Users need not to be worried about the overhead of encryption and decryption that takes place while data is being transmitted. Specifically, it needs a PHP server if the implementation of Monitoring mechanism is Web based. The data is confidential which needs to be controlled in proper way [6]. Also, the location sharing is a basic function while monitoring a device geographically. Location sharing includes the Longitude and Latitude that determines the co-ordinates of the place. In Android based remote control system using VNC [3], it is proposed that user will be able to access and manipulate the desktops of remote computers through a VNC viewer that will be provided on the user's cell-phone.

In Remote Computer Access through Android Mobiles [4], the remote computer's desktop is accessed from the normal Android mobile phone. The Remote Control of Devices in Android [9] can be made wireless and can be

DOI: 10.15680/IJIRCCE.2017. 0502011

accessed from any part of the world. We can control the remote computer like our normal local computer by using a java enabled mobile phone.

Another part of implementation includes monitoring a windows desktop using an Android based smart phone. This kind of monitoring follows VNC (Virtual Network Computing) Architecture. VNC is basically a Desktop Sharing process carried out through network. In this, the Message is transmitted to an android device, is compressed using various Protocols. Then the compressed image is shared with the Android device [2]. The purpose of image compression is that the Desktop Interface needs to be adjusted according to the Screen size of the device. The protocol used for the compression is RFB (Remote Frame Buffer) [8].

This protocol is used to transfer information to and fro by the connected devices. Ports used during the transmissions are ranging from 5900-5906 using TCP/IP protocol. These systems are implemented using Android Device to monitor a desktop PC by requesting a Desktop Server [2]. Android devices can be easily hacked which proves their vulnerability while monitoring of any Device. Also, these techniques are basically focused on Controlling of devices rather than just monitoring.

Since expertise is required for the mentioned technologies to be implemented, simple thing to use is either a FTP server or a Google Drive API.

Disadvantages-

i) The system is only a controlling system. Any sort of monitoring of device is not provided.
ii) The data transfer is only limited to one network. Remote data transfer is not possible in the above system.
iii) Data bandwidth required for the system is much high. The system will fail in case of low data bandwidth.

III. PROPOSED SYSTEM

The devices belonging to the same family or organization will get connected with the server using valid authentications. Once connected, the server will store provided data from devices. The data collected will be SMS logs, call logs, user location. Data will be transferred in text format only. Hence the data bandwidth required for the system is very low. Data sent from user devices will be collected by the server via internet. The admin will use this data to monitor the android devices belonging to his/her personal network. Another functionality provided by the system is of data transfer which is basically done with the help of push/pull request. The respective devices can push/pull the data which needed to transfer to/from server by using internet connection. Only devices connected to same family/organization can access that data.

A. *DEVICE MONITORING AND DATA TRANSFER SYSTEM ARCHITECTURE:*

Architecture shows N number of mobile devices forming a network, having a communication link to the server. The connection to server is formed via a common network gateway. Devices can be localized or can be remotely located. The main task performed by devices includes:

- Request the service: includes authenticating device itself for communication.
- Respond to server: responding to server queries for logs and locations.
- Push data to server: transferring files to the server over the network.
- Pull data from server: Requesting files from the server over the network.

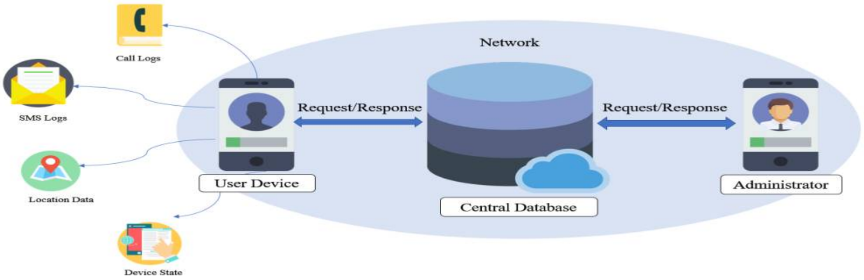

Fig. System Architecture

B. *BASIC TASKS PERFORMED BY THE SERVER SIDE:*

1. Authenticate the device requesting to connect.
2. Request the data to be collected from the devices.
3. Arrange the collected data in proper order and inform the system admin if data misuse is detected.

C. *MECHANISM TO PUSH/PULL DATA OVER THE NETWORK:*

To manage large volume of user data securely the system makes use of third party cloud storage i.e. Google Drive.Google Drive is a file storage and synchronization service created by Google. It has ability to store different types of media formats such as sheets, audio, video, images, documents etc.

To make use of services offered by google drive, system will be using a third-party API called google*Drive REST API*. This API is available for wide range of operating systems such as android, windows etc.

D. *MECHANISM TO TRACK USER'S LOCATION:*

Location tracking is one of the essential features provided by system. As devices are smarter and provides location based services based on the coordinates generated using GPS (Global Positioning System).

To make use of these coordinates and provide accurate user tracking and control facilities the third-party Google Maps API provides essential functionalities. It enables different views to track the user's locations such as satellite, earth view etc. The Maps API is suitable for cases where you want to maintain more control over the mapping experience

For an organization, an administrator can be high level authority person to monitor employee's activities. For a family, it can be a parent, monitoring activities of their children. The system has ability to perform parental control by assigning restrictions to user devices such as by scheduling shutdown timings, by putting limit on calling activities, by controlling access to explicit contents over the internet etc. For an organization, the collected data can be used to calculate employee's performance.

IV. SIMULATION AND RESULTS

The Simulation studies include Monitoring of the User device by collecting the data. The process will be initiated by user by registering through the User app. The User ID and Group ID that are required at the time of registration are provided by the Group Administrator, which will be monitoring the Device. Once registered, the Service is started automatically and the Data Collection process will be synchronized at certain time intervals. This Data is collected onto a central location i.e. Central Database. This Database will act as storage for all the information which is being fetched from the User Device. The Database will Store all the synchronized data and will transfer it to the Server i.e. Administrator. The Data, then, will be used to monitor the activities of the User Device.

The Central Database will also contain data that needs to be shared among the users of a Group. This Facility will be made usable by Administrator of the Group. Users can Upload/Download the Data as per their need.

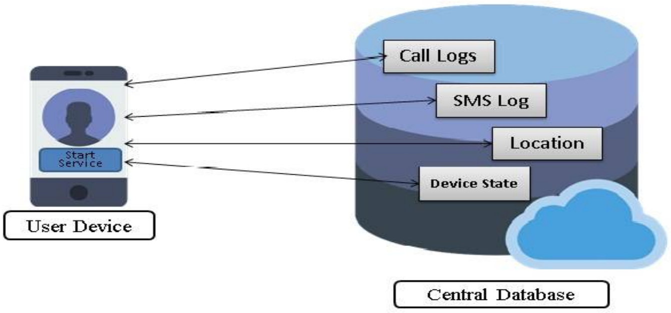

Fig.1. Initiation Process

Description Fig.1:

Firstly, the user of device will need to register its credentials with the Administrator through the application. User ID and Group ID will be assigned to User by Administrator of that particular group. Registering will make the user able to sign in to App. After user signs in to app, the process to synchronize data will be started automatically. The Data will be then uploaded to the Database and will be available to Administrator for Monitoring. A notification will be displayed to user when the Service has started.

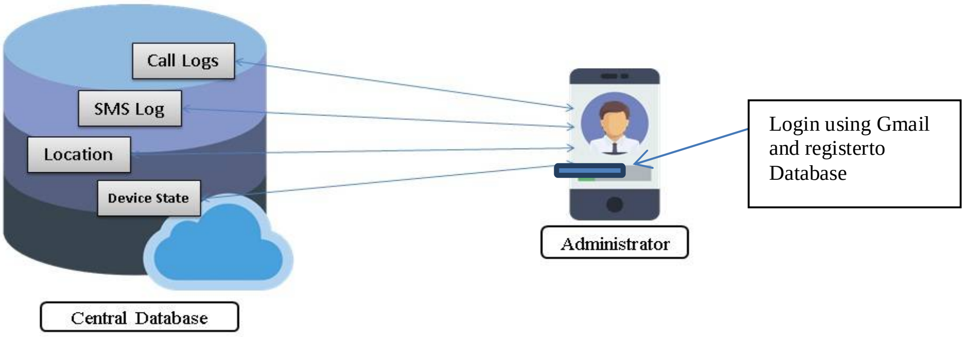

Fig.2. Data Monitoring

Description Fig.2:

The Administrator starts the monitoring of devices after successfully signing up on the Admin Application. Admin is required to sign in by using their Gmail credentials and then signing up for the Database Facility. Once this process is performed positively, Admin will be able to monitor all the available data from the Admin Application. After signing up, Admin should create a group of devices which is intended to be monitored. Each Device is required to be given a User ID, which can be used by User while logging into User App, is assigned by Admin.

As number of users are added to a Group, their data is collected on central database and will be fetched by Admin App for Monitoring. Admin can manage all the groups under its observation by selecting them as needed. Users can be viewed through 'My Groups' section in the App. The information related to any user can be accessed by selecting the Group and viewing option for the user available in the list.

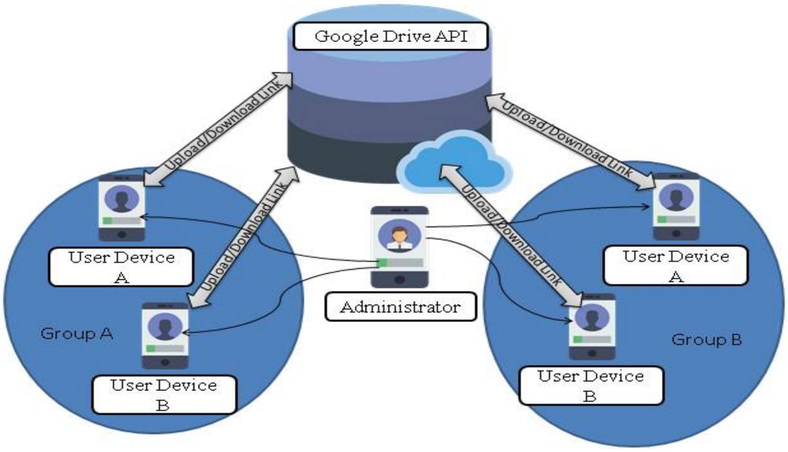

Fig.3. Data Transfer

Description Fig.3 :

We have provided an extra functionality for user application, which is Data Transfer. Important files can be shared by the users on this API. Basically when user logs in to the application, data synchronization starts in the background while in the foreground, user can upload files and download the files that are available. Administrator creates a Google Drive API after logging in to Administrator Application and when the users are added to groups, they are given permission to access the API for uploading and downloading of the files over the Internet. Any Group under same Admin can access the data shared over the Google API.

V. CONCLUSION

Device Monitoring and Data Transfer System provides monitoring and data transfer mechanism among devices based on android platform. The system makes use of textual data so the bandwidth required is considerably less as compare to discussed systems in this paper. Previous systems that are controlling the devices require higher bandwidth. The device monitoring mechanism requires internet connection on devices and thus allows remote communication among these devices across globe. This system is very much practical for any sort of user wishing to monitor devices belonging to his/her family /organization to prevent any misuse. Our system aims to minimize efforts by providing device state information periodically.

VI. ACKNOWLEDGEMENT

This work was supported by STES's SKNCOE for providing all necessary facilities and their constant encouragement and support. We are ending this acknowledgement and are thankful to our friends who have helped us.

REFERENCES

1. Sushant A. Patinge, Pravin ," Secure Instant Message and Location Sharing System for Android using Cryptanalysis.",IJAIEM, Vol.3, issue 3, P.332, 2014.
2. BasuShreejita, KulkarniPranita, PawaniPriyanka," Remote Desktop Monitoring Using Android.", IJRITCC, Vol.3, Issue.3, P.1547, 2015.
3. Rashmi A. Kalje, Prof. S. P. Kosbatwar," Android Based Remote Control of Mobile Devices Using VNC System.",IJCSIT, Vol.5, P.5090, 2014.
4. Jaya Bharathichintalapati, SrinivasaRao T.Y.S.," Remote computer access through Android mobiles", IJCSI, Vol.9, Issue 5, P. 368, 2012.
5. Ramesh Shrestha, Yao Aihong, "Design of Secure Location and Message Sharing System for AndroidPlatform", IEEE International Conference on Computer Science and Automation Engineering, pp. 117-121,2012.
6. S. M. Diesburg and A.-I. A. Wang, "A survey of confidential data storage and deletion methods,"*ACM Comput.Surv.*, vol. 43, pp. 2:1–2:37, December 2010
7. Sandeep Kumar, Mohammed Abdul Qadeer, ArchanaGupta ,"Location Based Services using Android", IEEE,P.2, 2009.
8. "Granter",available:http://betanews.com/2011/02/09/gartner-android-smartphone-sales-surged-888-8-in-2010, [Online; accessed 28-sep-2013]
9. Tristan Richardson RealVNC Ltd (formerly of Olivetti Research Ltd AT&T Labs Cambridge), The RFB protocol, Version 3.8, 2010.
10. Angel Gonzalez Villan and JosepJorbaEsteve, "Remote Control of Mobile Devices in Android Platform",arXiv,P.4,2013.
11. "Uploading Files, Drive REST API":*https://developers.google.com/drive/v3/web/manage-uploads*
12. Android Developer (2011). What is Android?http://www.android.com/about/
13. Android Service, Android Apps that runs in background,http://developer.android.com/reference/android/app/Service.html

BIOGRAPHY

1. Sujit Ingale is a student pursuing Bachelor of Engineering degree in Computer Engineering Department from Smt. KashibaiNavale College of Engineering,SavitribaiPhule Pune University. He Received Diploma in Computer Engineering Degree in year 2014 from MAEER's MIT's Shree SavitribaiPhule Polytechnic, Pune, India.

2. Shrirang Bhat is a student pursuing Bachelor of Engineering degree in Computer Engineering Department from Smt. KashibaiNavale College of Engineering,SavitribaiPhule Pune University. He Received Diploma in Computer Engineering Degree in year 2014 from MAEER's MIT's Shree SavitribaiPhule Polytechnic, Pune, India.

3. Nikhil Chandratre is a student pursuing Bachelor of Engineering degree in Computer Engineering Department from Smt. KashibaiNavale College of Engineering,SavitribaiPhule Pune University. He Received Diploma in Computer Engineering Degree in year 2014 from Sandip Foundation's Sandip Polytechnic, Nashik, India.

4. Vivek Ingale is a student pursuing Bachelor of Engineering degree in Computer Engineering Department from Smt. KashibaiNavale College of Engineering,SavitribaiPhule Pune University. He Received Diploma in Computer Engineering Degree in year 2014 from Smt. VenutaiChavanPolytechnic, Pune, India.

5. Prof. V. S. Phad is an Assistant Professor in Computer Engineering Department, Smt. KashibaiNavale College of Engineering, SavitribaiPhule Pune University.