Issue 9 vol 3 ISSN: 2321-8134

IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

SECURE COMMUNICATION IN MOBILE CROWD SENSING NETWORK

Pallavi Walke[1], Vaishnavi Naygaonkar[2],Rushabh Uttarwar[3], Ashish P.Nanotkar[4]

[1]*Student, computer engineering department, J.D.I.E.T, Yavatmal, pallaviwalke05@gmail.com*
[2]*Student, computer engineering department, J.D.I.E.T, Yavatmal, naygoankarvaishnavi40@gmail.com*
[3]*Student, computer engineering department, J.D.I.E.T, Yavatmal, rushabhuttarwar@gmail.com*
[4]*Guide, computer engineering department, J.D.I.E.T, Yavatmal, ashishnanotkar@gmail.com*

ABSTRACT

In today's era everyone is using smart phones with *different applications installed in that. Mobile crowd sensing is one of them which is a rising technology which helps to find different environmental details or any type of information easily. The devices which contain these practical applications and technology are called as mobile wearable devices. The smart phones may find these details using the sensing property of the phone and smart device. The mobile crowd sensing application can be used in many* different *areas like healthcare, medical, transportation which helps to increase the quality of life of people. When the user used these applications they may give their personal details to the server because hacker will hack there personal details. So* there are *two problems may be arrived like data trustworthiness and user privacy. So in this paper we will discuss Mobile crowd sensing architecture and second these two issues.*

Keywords— *MCS, Smartphones, Data trustworthiness, User privacy.*

1. INTRODUCTION

Many rising technologies have been evolved into smart phones which consists more processing power and storage capacity. In today's world the evolution of mobile phones is increasing rapidly which makes them so powerful that many novel applications can be run them..These devices consists of powerful embedded sensors like gyroscope, camera, microphone etc. using these sensors many sensing applications can run on wearable devices so MCS is one of the example of them. MCS depends on the user to collect information from the surrounding environments using the sensors, and then upload the data to application server using the network. Then the application server will process the data and extract the useful information and forward that information to the user.Supported by advances in mobile and wireless communication technologies such as third/fourth generation (3G/4G) and Wi-Fi, smartphones have better networking capabilities, allowing them to transmit data at higher rates. Moreover, they are equipped with more processing power and storage capacities. Mo re important, they are programmable.

For instance:Environment when the user wants to find the current environment status of the particular location at that time using his mobile application he will get logged in and then the current position all these are user privacy and data trustworthiness..so this issue be resolved data is sent to the server and then server will process that data and extract that useful information like temperature,time, date, location, climate condition and then these information is sent back to the user. Usually MCS focuses on upcoming new applications and solution of data collection. But MCS faces mainly two problems that.

2. PROPOSED WORK

2.1 Mobile crowd sensing

First of all the user has to get registered with the mobile crowd sensing application with the appropriate credentials. After the registration process the user become the participant of this application. Then the user may fire the queries which they need . After the registration process has been done the user can upload there queries using sensors in their mobile phones. The service provider handles all the mobile sensing data to the system and after the whole registration of the users and participants the confirmation is given to the mobile users then only if they have given their valid information. Then the data is transmitted to application server after receiving the query the application server informs all the nodes about the query. Then the nodes collects the information about the query and sends reply to the application server. The application server collects the data from each and every nodes but here without disclosing the identity of the node the application server gives reply of the query to the appropriate querier.

User privacy

Mobile Crowd Sensing application contains large amount of data collection from different areas. As the participants upload their personal information on the web that information may get hacked by the another person on the internet. Sometimes the hackers may expose their location or sometimes they may hack there important information. The different type of attacks on user privacy may be like user identification attack in which ID and time or date may get hacked. another one may be the Sensitive location tracking in which the IP address and location may get disclosed. The third one may be the sequential tracking attack in which all of the above information may get loosed. As the result people may get afraid of taking part into the MCS or get afraid of using MCS. So this issue needs to be addressed immediately.

Data trustworthiness

It is also called as an reliability of the uploaded data. Whenever the user sends data to the application server there the data owner saves that data to the database but he is not confirmed whether the data faulty or true data. So this issue should also be resolved.

2.2 System Architecture

The entities of the mobile crowd sensing application are as follows:

Participant

Participants or mobile node register properly with the application server managed by Mobile Crowd Sensing operator. Once the registration is confirmed by authority, he or she can upload that reports with the help of mobile sensors in their smart phones.

Service provider

The service providers handle the mobile phone sensing information to the system. After getting all the user registration of participant and querier the confirmation for the mobile nodes are given, only when they have given their valid details. Then all the collected reports from mobile nodes are verified. When the querier queries, the reports for their query is transmitted to the querier with the encrypted details of participant.

Querier

Queriers are the mobile users, who queries according to their needs. They too have a valid registration with the registration authority. They get the reports according to their queries with encrypted details of participants. Also the location is shown in Google maps.

The architecture consists of three main phases which are as follows as:

A. *Sensing phase*:

Before the mobile wearable device would use the MCS application the user first should download the corresponding app and should get properly registered with MCS application by providing all the valid own personal details then only the user may become the participant of the MCS application.Whenever the user fires an query the service provider informs all the participants about the sensing task. After that only the appllication starts collecting data with the help of the sensors.

B. Learning and mining phase

There are two models in this phase the first one consists of participants whose role is important who decides when to report data and in another one is mobile wearable devices satisfies task requirements. The sensed data is uploaded to the application server with the help of wi-fi or internet. Then the sensed data is processed from which important data is extracted with the help of techniques like machine learning and data mining.

C. Disseminating phase

In this phase the output which has been generated are finally organized into a suitable forms and then given back to the users**.**

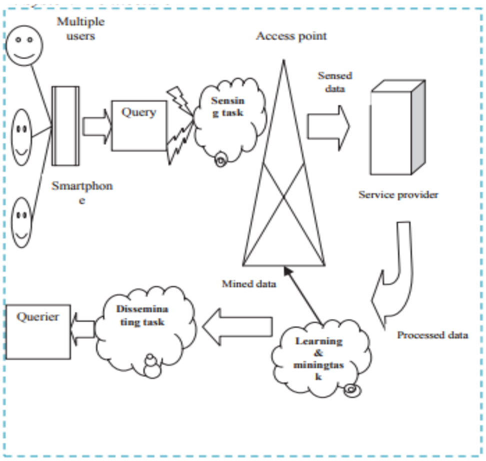

Figure: 4.1 Systeam Architecture Of MCS

The architecture of McSense has two main components:

(1) The server platform accept that particular tasks from clients and schedules the individual tasks for execution at mobile providers.

(2) The mobile platform (at the providers) that accepts individual tasks from the server, performs sensing, and submits the sensed data to the server. The communication relate to all these components takes place over the Internet. Next we will discuss the overall process.

User Registration:

The McSense application on the smart phones shows a registration screen for first time users, prompting them to enter an email address and a password. During the registration process, the user phone’s MEID (Mobile Equipment IDentifier) is captured and saved in the server’s database along with the user’s email address and password. We choose to store the phone’s MEID in order to restrict only one user registration per device. In addition, the server also avoids duplicate registrations when users try registering with the same email address again

Posting new sensing tasks:

New sensing tasks can also be posted by clients using a web interface running on the McSense server. The sensing task details are entered on this web page by the client and then submitted to the server’s database. Once a new task is posted, the background notification service running on the provider’s phone identifies the new available tasks and notifies the provider with a vibrate action on the phone. Providers can check out the notification and can open the McSense application

For to view the new available tasks. When the application is loaded, the providers can see four tabs (Available, Accepted, Completed and Earnings). The providers can view the list of tasks in the respective tabs and can click on each task from the list to view the entire task details such as (type, status, verbal description, accepted time, elapsed time, completion time, payment amount).

2.3 Life cycle of a task:

The life cycle starts from the Available tasks tab. After this When a provider selects an available task and clicks on the Accept button, the task is moved to the Accepted tab. Once a task is accepted, then that task is not available to others anymore .When the accepted task is completed according to its their requirements, the task is moved to the Completed tasks tab. At last, the providers view their aggregated total dollars earned for successfully completed tasks under the Earnings tab. If suppose that accepted task expires before completing successfully according to its requirements, it is moved to the Completed tasks tab and marked as unsuccessfully completed. The providers do not earn money for the tasks that are accomplished unsuccessfully. Background services on phone: Suppose When the network is not available, a completed task is marked as pending upload. A background service on the phone periodically checks for the network connection. When the connection becomes available, the awaiting data is uploaded and finally these tasks are marked as successfully completed. If the provider phone is restarted manually or due to the mobile OS crash, then all the in progress sensing tasks are automatically resumed by the Android's Broadcast Receiver service registered for the McSense application. Furthermore, the Accepted and the Completed tab's both task lists are cached locally and are synchronized with the server. If suppose server is not reachable, then the users can still see the tasks that were last cached locally.

3. Application, Advantage & Disadvantage

3.1 Application

Smart Cities

Cities with high population density and a very large number of interconnected issues make effective city management a challenging task. There several significant government and industrial research efforts are currently underway to exploit the full potential of the sensing data by initiating smart city systems to improve city Efficiency by deploying smarter grids, water management systems and ultimately the social progress.

Marketing/Advertising:

Real-time location or mobility traces can be used by vendors/advertisers to target certain categories of people. They can run context-aware surveys (function of location, time, etc.).

Road Transportation:

Departments of transportation can collect fine grain and large scale data about traffic patterns in the country/state using location and speed data provided by GPS sensors embedded in cars. These data can then be used for traffic engineering, construction of new roads, etc. Drivers can receive real-time traffic information based on the same type of data collected from smart phones.

Healthcare & Wellbeing:

1. Wireless sensors worn by people for heart rate monitoring and blood pressure monitoring can communicate their information to the owners' smart phones. Mobile sensing can leverage these existing data into large scale healthcare studies that seamlessly collect data from various groups of people, which can be selected based on location, age, etc.
2. The phones can perform activity recognition and determine the level of physical exercise done by people, which was proven to directly influence people's health. So as per the study in a city, the municipality may decide to create more bike lanes to promote people to do more physical activities.

3.2:Advantages

a. Location Accuracy
b. It is highly accurate and reliable
c. It help in faster direction Of input sensor.
d. It reduce the extra consumption of electricity.

3.3 Disadvantages

a. Short battery Life.
b. Small screen Display.
c. Speed of internet is slow as compared to PC'S

4. CONCLUSION

We have seen the architecture of mobile crowd sensing in which how the user may get all the necessary details by using the Mobile crowd sensing appllication in their mobile phones. While using this appllication they upload their personal information which should be protected by the hackers. There may be two problems faced user privacy and data trustworthiness so these two issues should be get overcome to keep the MCS app evergreen without getting any hesitation to use this application.

REFERENCES

[1] Madhuri Bhandalkar and A.B.palve"Location Based Secure Communication In Mobile Sensor Network", IEEE,Mar.2016

[2] E. De Cristofaro and C. Soriente, "Participatory Privacy: Enabling Privacy in Participatory Sensing", IEEE Network, vol.27, no.1, Jan.Feb.2013, pp.32-36

[3] I. Boutis and V. Kalogeraki, "Privacy Preservation for participatory Sensing Data", IEEE

[4] PerComm, Mar.2013, pp.103-13.

[5] K. L. Huang. S. S. Knahere, "Are you contributing trustworthy data? The case for reputation System in participatory sensing", Proc.ACM MSWiM, 2010,pp.14-22.