IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

# User Privacy and Data Trustworthiness in Mobile Crowd Sensing

**Ms. T. Sharadha[1], Dr. R. Vijaya Bhanu[2]**

MCA, Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India [1]

Assistant Professor, Department of Computer Science , Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India [2]

**Abstract:** "Mobile crowd sensing" is an evolving technology based on the sensing the networking capabilities of mobile wearable devices. Mobile Crowd Sensing (MCS) has shown great potential in improving peoples' quality of life, including healthcare, transportation, and environmental monitoring. User privacy and data trustworthiness are two critical challenges faced by MCS. In MCS, the private information such as IP addresses and location tracking are prevented by user privacy concern. The main objective of trustworthiness is to hide reports of sensed data and queries from unconcerned parties. In this work, MCS technology will provide wireless sensor network security solution by user privacy and trustworthiness in traffic and event management.

**Keywords:** Mobile Crowd Sensing (MCS), User Privacy, Data Trustworthiness, Wireless Sensor Network security (WNSs).

## I. INTRODUCTION

Nowadays the trending smart phones and other mobile wearable devices are rapidly growing. These smart phones are not only used for computing and communication but also smart in sensing the data [3]. Mobile Crowd Sensing (MCS) is an evolving technology based on the sensing the networking capabilities of mobile wearable devices. Two major issues faced by MCS are user privacy and trustworthiness which are secured with Wireless Sensor Network security solution [15].

MCS relies on individual participants to collect data from their surrounding environments by their wearable devices or smart phones, and then upload the data to the application server through networking facility [16]. The application server will process all data reported by the participants, extract the information in which queriers are interested, and forward such information to the end users. MCS application can be used under different categories such as healthcare, business, environment, transportation, and social networking.

This MCS application collects data across wide geographical areas, spatial-temporal information where there are possible threats to the participants who uploaded their data such as the collected data may disclose their locations and trajectories.

Here the major security issue of MCS is the reliability of the uploaded data which are reported by participants, which could possibly be falsified [9]. Hence, this raises the issue of data trustworthiness which is used to hide reports of sensed data and queries from unconcerned parties.

### A. Mobile Crowd Sensing

Mobile Crowd Sensing involves a very large number of users or crowd sensors in the sensing tasks by collecting and delivering the local data obtained through their sensor-enabled mobile devices to a data collection center [16].

### B. User Privacy

User privacy is defined how the information is collected, used, and distributed as follows

- Information user creates using some combination of applications, such as the e-mail, financial records, and so on.
- Information about user, such as user name, address, personal interests, and so on, collected by an application in order to provide services to user.
- Information about the machine and/or network connection users are using, such as an IP address, collected by an application in order to provide services to the user [16].

### C. Data Trustworthiness

Presenting that the evidence for the data results reported is true and when the argument made based on the results is strong which means the data reported should not be falsified [16].

## II. MCS ARCHITECTURE

MCS applications may differ to different system models. A typical MCS architecture as shown in Fig. 1, which has three stages: sensing, learning and mining, disseminating.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

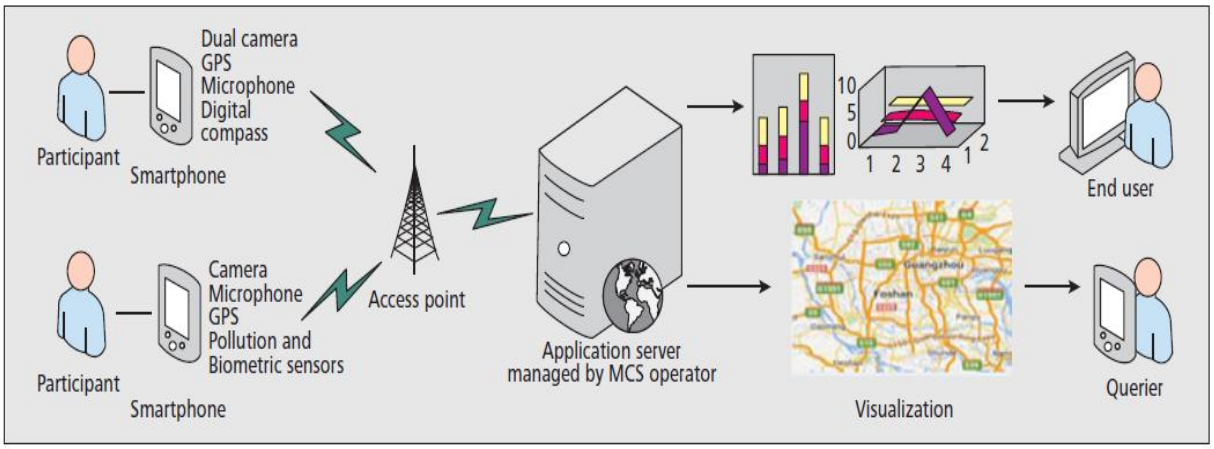


Fig 1.The architecture of a typical mobile crowd sensing application [15]

In the sensing stage, the user first needs to download the corresponding app from the appropriate channel, e.g., Apple's App Store or Google's Play Store. After installing and running the app, the user becomes a participant. Then, the app starts collecting data using the relevant sensors and the application sever informs the participants about the sensing task according to the queries [10]. In the learning and mining stage, there are two possible data collection models. In the first model, participants play an active role by deciding when to report data. In the second model, reporting occurs when the sensed data are uploaded to the application server through networks which processes the sensed data to extract the desired information using mining techniques [6]. In the disseminating stage, the results are converted into suitable forms and made available to the desired queriers. The role of each entity of an MCS architecture system is summarized in Table 1.

**Table 1.**Roles of entities of an MCS system. [15]

| | |
|---|---|
| Participants | Measuring the required data about a subject of interest using mobile wearable devices. |
| End users or queriers | Requesting data through tasks and then utilizing the information acquired by participants. |
| MCS operator | Distributing tasks to participants who meet the requirements of applications. In certain architectures, end users or queriers can also act as MCS operators. |

## III. PROPOSED SYSTEM

The work entitled "User Privacy and Data Trustworthiness in Mobile Crowd Sensing" will provide Wireless Sensor Network security (WSNs) solution by user privacy and trustworthiness. In Mobile Crowd Sensing (MCS), the private information such as IP addresses and location tracking are prevented by user privacy concern and the data trustworthiness is used to hide reports of sensed data and queries from the unconcerned parties.

## IV. SYSTEM WORK FLOW

The workflow goes through the following stages, as shown in Fig 2.

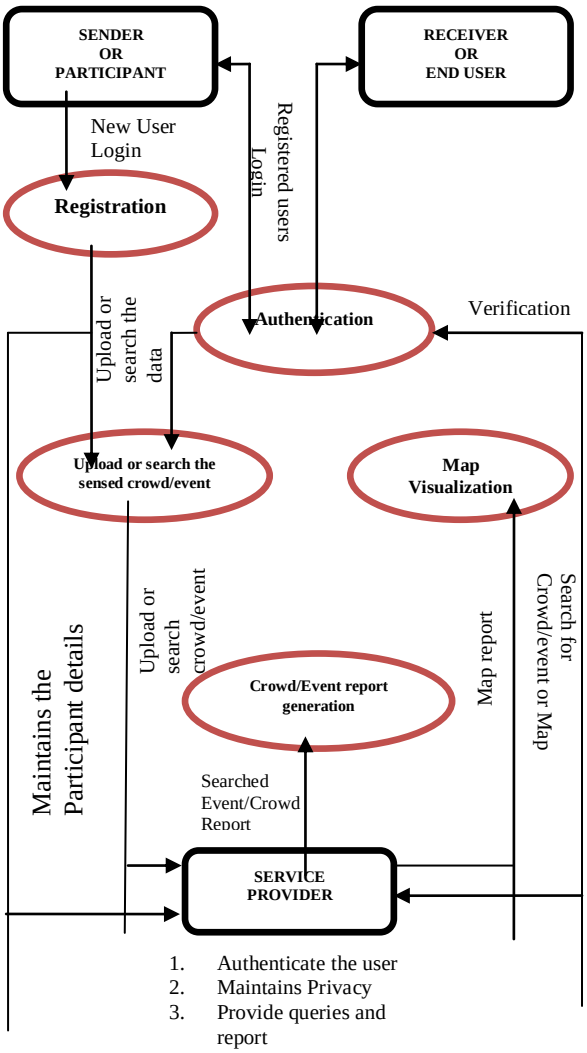


**Fig 2.**Workflow

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

## V. SYSTEM DEVELOPMENT

System development is a series of operations performed to manipulate data to produce output from a computer system. The principle activities performed during the development phase can be divided into a major related sequence, this project has four modules are as follows [16]

A. Participant or Mobile Node

Login**:** In Participants or Mobile node, the user or the participants has to login with the appropriate username and password managed by MCS operator. The MCS operator authenticates the authorized person to access the details for security purpose. After successful login, the user is allowed to access the home page where the user can upload an event or search an event.

Registration: In Participants or Mobile node, if the user or the participant is new, their personal details has to be given with valid username and password. These unique username and password are managed by the MCS operator. The MCS operator authenticates the authorized person by successful login dialog box.

B. Service Provider Module

User Authentication**:** The service providers sense the information from mobile to the server system. It verifies the username and password, and authenticates the user whether the user is eligible to login or not.

Query and Report generation**:** After verification is done, the service provider processes the queries and report that has been uploaded by the user. The collected queries are processed by the service provider and transmitted to the user in the form of report and can be visually viewed in the map format.

Maintains Privacy**:** The main work of the service provider is to maintain privacy of the user details. The user details like participants' identities, IP addresses, locations, trajectories etc., are to be hidden for privacy concern.

C. Querier Module

Upload an event: Queriers are the mobile users, who can upload the details if there is an event or crowd sense in a particular location. The uploaded details are stored in service provider to keep track for crowd in a particular location.

Search an event: The Querier searches the location and if there is any crowd sense or event in the particular area, the events are listed with the details of the user who uploaded the event with privacy concern. The query event can be visually viewed in map.

Event Details: User gets the reports according to their queries with details of participants along with location in Google maps. The Event details like tag of the event, area of the event, the user name that uploaded the event, latitude and longitude of the event can be viewed. Here the user details like participants' identities, IP addresses, locations, trajectories etc., are hidden for privacy concern.

D. Map Services

Google map is embedded into the application to view the locations and set the map information for the user. The map can be embedded in the application with the Meta Key and SHA1 fingerprint of the IDE software [18].

## VI. RESULTS AND DISCUSSION

The work has been done in Eclipse as Integrated Development Environment (IDE) with Java as coding language and SQLite as backend database. The results of the work done are discussed in following figures.

The Login Screen has the inputs for Username and Password for the registered users which are shown in Fig 3.Login Screen.

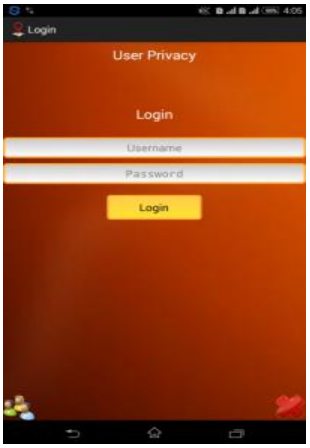


**Fig 3.**Login Screen

By authenticating the Username and Password the Login Success screen is displayed with the output as Login Success which is shown in Fig 4.Login Sucess.

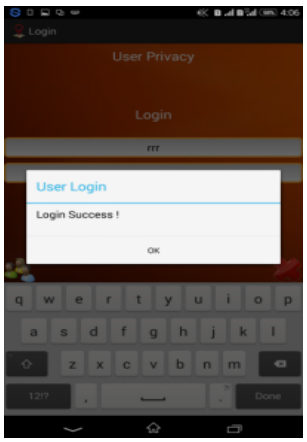


**Fig 4.**Login Success

The new user can register their details as inputs in this New User Registration Screen like

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

- Username
- Password
- Email
- Address

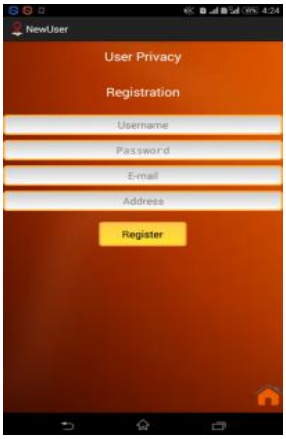


**Fig 5.**New User Registration

After the successful login, the Home Screen will be displayed with options like Search, Upload and Logout which is shown in Fig 6.Home Sreen.

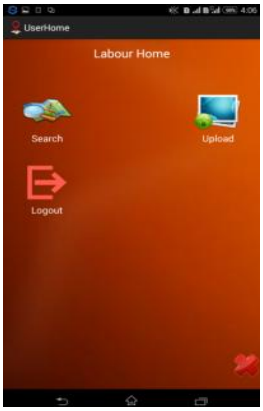


**Fig 6.**Home Screen

The sensed event/crowd can be uploaded as inputs in the Upload an event screen like

- Event/Crowd Place
- Event/Crowd tag
- Details of the event/Crowd


**Fig 7.**Upload an event

The event/crowd can be searched as outputs in Search an event screen which is shown in Fig 8.Search an event.

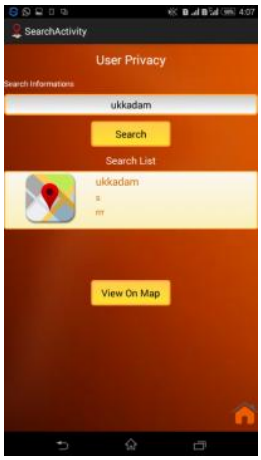


**Fig 8.**Search an event

The user can view the details of the event/crowd and the view who uploaded the details in Details of the event screen which is shown in Fig 9.Details of the event.


**Fig 9.**Details of the event

The user can view the sensed event/crowd in map visualization format in Map Visualization screen which is shown in Fig 10.Map Visualization.


**Fig 10.**Map Visualization

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

## VII. CONCLUSION

Mobile Crowd Sensing is a computing paradigm that can lead to a wide range of novel applications relating to environmental monitoring, transportation, business etc. In this project, the two important challenges of MCS are user privacy and data trustworthiness which are the two major barriers to the success and massive deployment of MCS systems. Thus, we can sense the traffic and event management in MCS over Wireless Sensor Network (WSNs) by using user privacy and data trustworthiness.

## VIII. FUTURE SCOPE

The developed system has many possibilities for the future enhancements. We also improve this project in other new mobile operating system like ios and microsoft.

Future work can be focused on, how to employ some simple cryptographic operations to transfer a reputation value without the involvement of any trusted third party and high communication overheads. If participants are malicious, they would provide falsified data, and it is difficult to identify them, especially when different task actions are not linked due to privacy protection.

## REFERENCES

[1] S. Gaonkar et al., "Micro-Blog: Sharing and Querying Content Through Mobile Phones and Social Participation," Proc. ACM MobiSys, 2008, pp. 174–86.
[2] P. Narula et al., "Security in Mobile Ad-Hoc Networks Using Soft Encryption and Trust Based Multi-Path Routing," Comp. Commun., vol. 31, no. 4, Mar. 2008, pp. 760–69.
[3] I. Boutsis and V. Kalogeraki, "Privacy Preservation for Participatory Sensing Data," Proc. IEEE PerCom, Mar. 2013, pp. 103–13.
[4] K. L. Huang, S. S. Kanhere, and W. Hu, "Are You Contributing Trustworthy Data? The Case for a Reputation System in Participatory Sensing," Proc. ACM MSWiM, 2010, pp. 14–22.
[5] L. K. Huang, S. K. Salil, and H. Wen, "A Privacy-Preserving Reputation System for Participatory Sensing," Proc. IEEE LCN, 2012, pp. 10–18.
[6] A. Dua et al., "Towards Trustworthy Participatory Sensing," Proc. USENIX HotSec., 2009, pp. 1-6.
[7] D. Christin et al., "IncogniSense: An Anonymity-Preserving Reputation Framework for Participatory Sensing Applications," Pervasive and Mobile Computing, vol. 9, no. 3, 2012, pp. 353–71.
[8] Q. Li, G. Cao, and T. La Porta, "Efficient and Privacy- Aware Data Aggregation in Mobile Sensing," IEEE Trans. Dependable Sec. Comp., vol. 11, no. 2, Mar.–Apr. 2014, pp. 115–29.
[9] C. Cornelius et al., "AnonySense: Privacy Aware People-Centric Sensing," Proc. ACM MobiSys., 2008, pp. 211–24.
[10] S. Gao et al., "TrPF: A Trajectory Privacy Preserving Framework for Participatory Sensing," IEEE Trans. Info. Forensics Security, vol. 8, no. 6, June 2013, pp. 874–87.
[11] R. Caceres et al., "Virtual Individual Servers as Privacy- Preserving Proxies for Mobile Devices," Proc. MobiHeld Wksp., 2009, pp. 37–42.
[12] 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.
[13] J. Shi et al., "PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems," Proc. IEEE INFOCOM., 2010, pp. 1–9.
[14] R. Ganti et al., "PoolView: Stream Privacy for Grassroots Participatory Sensing," Proc. ACM SenSys., 2008, pp. 281–94.
[15]http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7054716
[16] http://jpinfotech.org/user-privacy-data-trustworthiness-mobile-crowd-sensing-2/
[17] http://www.lemenizinfotech.com/2015/android/User%20Privacy%20and%20Data%20Trustworthiness%20in%20Mobile%20Crowd%20Sensing.pdf
[18] http://www.slideshare.net/IISTech2015/user-privacy-and-data-trustworthiness-in-mobile-crowd-sensing

## BIOGRAPHIES

**Sharadha. T** is doing her Master's Degree in Computer Applications (MCA), Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She had completed her Bachelor's Degree in Computer Application in 2011. Her areas of interests are Android Application Development and Java.

**Dr. R. Vijaya Bhanu** is an Assistant Professor in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She has completed MCA and M.Phil and Ph.D in Computer Science at Avinashilingam University. Her thesis is in the area of Soft Computing. She has published 11 papers in International Journals and presented four papers at International conferences.