Volume 2, Issue 6 June 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

IRJIF IMPACT FACTOR: 3.01

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.01

"SECURITY ENHANCEMENT FOR USER PRIVACY AND DATA TRUSTWORTHINESS IN MOBILE CROWD SENSING"

DATTATRAY D.PHALLE, SHIVAJI M.RODE, KUNAL V. GANDHE & KEDAR G.BHEGADE
Department of Information Tech. NMIET, Talegaon, Pune. India

Abstract — ***Smartphones and other trendy mobile wearable devices are rapidly becoming the dominant sensing, computing and communication devices in peoples' daily lives. Mobile crowd sensing is an emerging technology based on the sensing and networking capabilities of such mobile wearable devices. MCS has shown great potential in improving peoples' quality of life, including healthcare and transportation, and thus has found a wide range of novel applications. However, user privacy and data trustworthiness are two critical challenges faced by MCS. In this article, we introduce the architecture of MCS and discuss its unique characteristics and advantages over traditional wireless sensor networks, which result in inapplicability of most existing WSN security solutions. Furthermore, we summarize recent advances in these areas and suggest some future research directions.***

Keywords — ***MCS, WSN, RS, USER PRIVACY, DATA TRUSTWORTHINESS.***

1. INTRODUCTION

Since the introduction of Apple's iPhone, mobile phones have evolved into *Smartphone's*. Supported by advances in mobile and wireless communication technologies such as third/fourth generation (3G/4G) and Wi-Fi, smart phones have better networking capabilities, allowing them to transmit data at higher rates. Moreover, they are equipped with more processing power and storage capacities. More important, they are programmable. A myriad of paid or free applications (often referred to as *apps*) are available to be downloaded in a convenient manner. Overall, this evolution makes mobile phones so powerful that many novel applications can be executed on them. Moreover, recently, devices equipped with similar capabilities are emerging as wearable accessories (e.g., Google Glass and Galaxy Gear). All together, they are referred to as mobile wearable devices.

Another important feature of mobile wearable devices is, as shown in Fig. 1, that they come with a growing set of powerful embedded sensors, such as gyroscope, accelerometer, microphone, digital comp-

pass, and camera. Based on these sensors, a variety of sensing applications can be executed on mobile wearable devices; among them mobile crowd sensing (MCS, also known as participatory sensing or people-centric sensing) is a prominent family. MCS relies on individual participants to collect data from their activities and surrounding environments by their wearable devices, and then upload the data to the application server via any available networking facility. The application server will process all data reported by the participants, extract the information in which queries are interested, and forward such information to the queries.

2. EXISTING METHODLOGY:

When searching for a place and nearest location, a user sends queries in the form of keyword. Nowadays Smartphones are used for query searching in the internet servers. Also users use Smartphones for posting or uploading some important reports into the server. Once the reports are uploaded, all other users get those results with the sensible information like location and time of the participant who uploads the reports. Participant may also upload some photos in social websites which may contain some information about his/her location. This leads to the leakage of participant's information to the queerer, one who performs search.

2.1 Merits of Existing System

- Empowerment Voting is the most powerful way for members to have a voice in the leadership and direction of their organization. When allowed to vote in fair and open elections, members will feel a greater sense of value, ownership, and responsibility. This is why it is important to reach as many members as possible with different election methods including online voting.
- Accessibility With the surge of mobile devices, online voting is a convenient option for many members, allowing them to access ballots anytime, anywhere.
- Cost effectiveness online elections are cost effective, especially when considering production costs of printing, postage, and mailing ballots.
- Security and confidentiality A properly designed online voting system has safeguards in place to assure security of ballots and protection of voter identities.
- Transparency Online elections, particularly those run by a third-party, eliminate the chance of election mismanagement or fraud. An audible trail helps increase voter confidence.
- Accuracy and expedience since online voting utilizes electronic ballots, there are no rejected, mismarked, or invalid votes. Results are automatically calculated, eliminating the need for manual tabulation.

2.2 Demerits of Existing System

- Proposes mobile phone intermediate e-voting system uses the extended encryptions system.
- This system is used to enforce the cut of the choose method to exclude the computational zero
- Knowledge evidences and shows the effectiveness of the system. Proposed system is probably safe in simulation-based prototype.
- Propose GSM based mobile phone voting system is used to cast vote without registering for voting in advance and going to polling booths.
- System prevents repetition voting but It has big Disadvantage to security, proposes system does not used any cryptographic algorithm.
- Proposed mobile phone voting system based on public key encryption algorithm RSA.

3. MOBILE CROWD SENSING ARCHITECTURE OF MCS:

Note that different MCS applications may have Different system models. To make it more general, Here we consider a typical MCS architecture as shown in Fig. 1,

Figure 1. Sensors on typical mobile wearable devices.

Which has three stages: *sensing, learning and mining, disseminating*. In the sensing stage, before the owner of a mobile wearable device can participate in an MCS application, he/she first needs to download the corresponding app published by end users from the appropriate channel, e.g., Apple's App Store or Google's Play Store. After installing and running the app, he/she becomes a participant. For a certain query, the application server informs all participants about their sensing tasks. Then, the app starts collecting data using the relevant sensors. 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 whenever the state of the mobile wearable device satisfies the tasks' requirements. So, the sensed data are uploaded to the application server through Wi-Fi or cellular networks. The application server then processes the sensed data to extract the desired information using techniques such as machine learning and data mining. In the disseminating stage, the results are formatted into suitable forms and made available to queries.

4. SCOPE

Process enables voters to cast a secure and secret ballot over the android application. In the framework, an e-voting process may fall in one of the following categories:

- Public elections and/or referenda at state and/or local level
- Internal elections and similar decision procedures.
- Advisory polls for decision-making and advisory referenda.
- Mobile Based polls.
- Privacy Preservation using E-Aadhar No and Email supported OTP.
- RESULT DECLARATION

5. PROBLEM STATEMENTS ON USER PRIVACY:

In a typical MCS application, the sensing data uploaded by participants are invariably tagged with important contextual information such as sensing location and time. Clearly, disclosure of this information can have serious implications on participants' privacy. Moreover, multiple reports from the same participant can be linked to extract more private information such as the location of his/her home and/or office.

6. PROPOSED SYSTEM

1. A novel approach to user privacy and data trustworthiness when they use mobile sensors to sense and share information to the server.

2. In MCS, privacy concerns arise due to the disclosure of private information such as participant's identities, IP addresses, locations, trajectories, and lifestyle-related information.

3. MCS applications even aggravate the privacy problem because they make large volumes of information easily available through remote access. Thus, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk and anonymous manner.

4. Remote access also allows a single adversary to monitor multiple users simultaneously. We consider users location information as an example. Since MCS allows any voluntary participant to contribute data, the application server is exposed to erroneous or even malicious data. For example, participants may inadvertently put their wearable devices in an undesirable position while collecting sensor readings (e.g., Galaxy Gear kept in a pocket while sampling street-level noise). Moreover, malicious participants may deliberately contribute bad data. Both behaviors result in erroneous contributions, which need to be identified and eliminated to ensure the reliability of the computed summaries

6.1 BENEFITS OF PROPOSED SYSTEM

1) Live tracking is possible.
2) Mapping.
3) Continuous live tracking.
4) Maintaining database.

7. RELATED WORK

7.1. Pseudonyms or suppressing user identity:

These are basic and simple methods to make participants anonymous by replacing their identification information with pseudonyms or suppressing users' identities. However, these methods may not always work. For example, from a user's movement pattern, it is straightforward for an adversary to de-anonymize his/her reports. To address this challenge, some methods with the connection anonymization concept have been proposed in recent years for securing user privacy in MCS systems.

7.2 .Connection anonymization:

Such methods can be used to avoid some tracing attacks (e.g., network-based tracing attacks based on IP addresses). In [9], the authors attempted to achieve anonymity of users by using Mix Networks. A Mix Network is a statistical-based anonymizing infrastructure achieving the *k*-anonymity property, which ensures that the operator cannot identify the originator of each sensing record from a group of *k* or more participants. It routes reports via multihop transmission, adding delays and mixing with the data between different sources and destinations. It aims to prevent an adversary from linking all reports of a mobile node, identifying which mobile node sent the report, and learning when and where the reports were generated. Unfortunately, Mix Networks are unsuitable for many MCS settings. On one hand, they do not attain provable privacy guarantees. On the other hand, the degree of confidentiality is relatively limited: reports are encrypted under the public key of the so-called report server (RS) — a trusted party collecting reports and distributing them to queriers. In that case, the RS may learn both sensors' reports and the interest of queriers.

8. METHODOLOGY

8.1 HARDWARE IMPLEMENTATION

1) ***GPS Satellite:*** Global Positioning System (GPS) is a network of satellites that continuously transmit location information, which makes it possible to precisely identify locations on earth by measuring distance from the satellites.[3]
2) ***GSM:*** This GSM can accept any Global System for Mobile communication (GSM) network operator SIM card and act just like a mobile phone with its own unique phone number. It is a wireless MODEM and can send and receive data through the GSM network It requires a SIM card and connectivity to the GSM network. It can also be used in GPRS mode to connect to the internet and use all the applications for data logging.
3) ***LCD Display Unit:*** This system has a LCD display module for displaying Distance Time and Date.
4) ***Power Supply Unit:*** The power supply unit has to provide a regulated D.C supply to all sections

of the system. As it is essential to operate the instrument on batteries since it is used with the person while moving. It consists of rechargeable batteries, filter capacitors and voltage regulators.

8.2 SOFTWARE IMPLEMENTTAION

1) ***Server*:** Server, the Server serves its basic necessity even though it lacks a few major functionalities. It consists of Victim's Database features and Device Information. Also manages all devices.
2) ***Android Application for Device Tracking:*** The crucial part of the application is the tracking of device. Unlike the mobile version, this is achieved precisely by showing the locations of the victim on the map. Thus the android version of tracking application depicts a clear view of the real time positions on the map based on the indoor mapping.

9. RECENT WORKS ON DATA TRUSTWORTHINESS:

Trust systems for data reliability have been widely used for a wide range of networks such as the Internet, mobile ad hoc networks, peer-to-peer networks, and WSNs. However, most of them are inapplicable for MCS systems due to the special characteristics of MCS systems mentioned earlier. Recent research on data trustworthiness in MCS can be found in [4–8]. These systems focus on how to evaluate the trustworthiness of the shared data and how to maintain the reputation of data processing network entities. In particular, Huang *et al.* [4] proposed a reputation system based on the Gompertz function to compute reputation scores of devices to measure the trustworthiness of the contributed data. However, it does not take privacy preservation into account.

More recently, several reputation schemes that are privacy-aware have been proposed [5–8]. Some of the approaches [5, 6] rely on the existence of a trusted third party, but the establishment and maintenance of this entity in a distributed environment is not trivial. In the scheme of [5], multiple pseudonyms are assigned for each participant. A trusted server is required to manage the mapping between the real identity of a participant and his/her pseudonyms, and transfer reputation values between different pseudonyms. Compared to other methods, this method does not require expensive cryptographic operations and has low communication overheads. Also, Dua *et al.* [6] proposed and implemented a trusted platform module (TPM), which is a micro-controller embedded within each mobile device, to attest the integrity of sensor readings. However, TPM chips are not yet widely adopted in mobile devices. Some methods that do not rely on the existence of a trusted third party have been proposed. In [7], an anonymity-preserving reputation solution called

Incognisense was proposed. It generates periodic pseudonyms using blind signatures, and cloaks exact reputation values dynamically into reputation groups. The assumption that the manager of reputation and pseudonym must be trusted is eliminated. However, additional management overhead is incurred.

9.1 FUTURE DIRECTIONS:

The problems of user privacy and data trustworthiness are quite new. Notwithstanding the recently proposed works, much remains to be done. Some future directions for each problem are suggested below.

9.2 USER PRIVACY:

• Protecting query privacy with respect to the registration authority.

• Protecting node privacy with respect to the network operator. With the current technology, users' locations and identities are not allowed to be hidden from the network operator.

• Addressing collusion attacks, which invade the privacy of mobile nodes or quarries through collaboration. While available cryptographic techniques support simple aggregate function evaluation over encrypted data, enabling efficient evaluation of complex predicates is still an open challenge.

9.3 SYSTEM ARCHITECTURE:

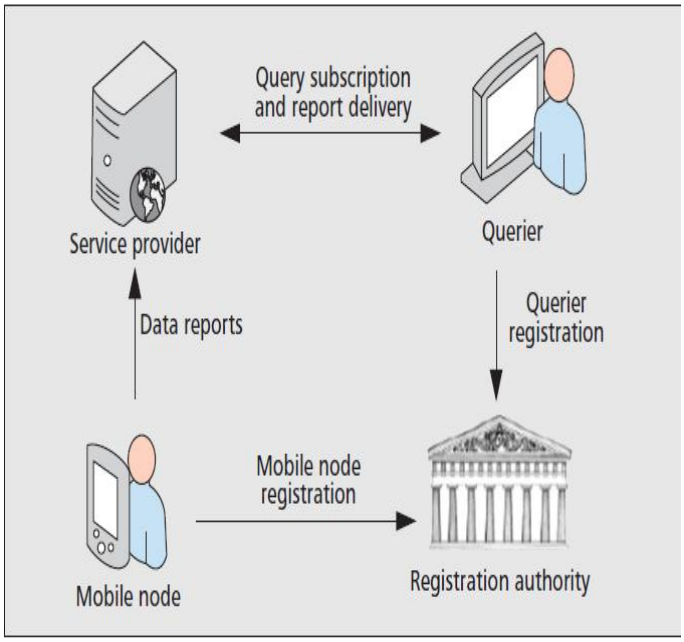

Figure 3. The architecture of PEPSI.

10. CONCLUSION

MCS is an innovative computing paradigm that bears great potential and can lead to a wide range of novel applications relating to, for example, environmental monitoring, transportation, and entertainment. In this article, we have presented the advantages of MCS over traditional WSNs. At the same time, we have also identified two important challenges of MCS, user privacy and data trustworthiness. They are the two major barriers to the success and massive deployment of MCS systems. It is important to overcome these challenges in order to move this field forward.

ACKNOWLEDGMENT

Each project big or small is successful largely due to the effort of a numerous wonderful people who have always given their precious advice or lent a helping hand. I sincerely appreciate the inspiration; support and guidance of all those people who have been instrumental in making this project a success.

We would also like to thank all the faculty members of NMIET for their critical advice and guidance without which this project would not have been possible.

REFERENCES

[1]. Boutsis and V. Kalogeraki, "Privacy Preservation for Participatory Sensing Data," Proc. IEEE Per Com, Mar. 2013, pp. 103–13.

[2] L. K. Huang, S. K. Salil, and H. Wen, "A Privacy -Preserving Reputation System for Participatory Sensing," *Proc. IEEE LCN*, 2012

[3] A. Dua *et al.*, "Towards Trustworthy Participatory Sensing," *Proc. USENIX HotSec.*, 2009, pp. 1-6.

[4] 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.

[5] 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.

[6] 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.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301 Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com