ANONYMOUSLY SENSED DATA REPORTING

Prof. Anand N. Gharu, Kanchi S. Shah, Nayana V. Taskar, Pooja L. Jain, Wasim R. Shaikh

[1] *Department of Computer Engineering, P.V.G' s College of engineering, Nashik, Maharashtra, INDIA*
[2] *Department of Computer Engineering, P.V.G' s College of engineering, Nashik, Maharashtra, INDIA*
[3] *Department of Computer Engineering, P.V.G' s College of engineering, Nashik, Maharashtra, INDIA*
[4]*Department of Computer Engineering, P.V.G' s College of engineering, Nashik Maharashtra, INDIA*
[5] *Department of Computer Engineering, P.V.G' s College of engineering, Nashik Maharashtra, INDIA*

ABSTRACT

We are proposing an efficient anonymous data reporting protocol for participatory sensing. It provides strong 74privacy protection, data accuracy and generality. The protocol consists of two stages, namely message submission and encryption. In the message submission stage, each participant transmits a sensed data to the SQL server. The database maintain all records like smartphones IMEI number, smartphone identity name with sensed data from the sensors. It maintain those data but only application server has access to the database. In the Encryption phase, as per the request from the end user the Application Server will send the requested data but in encrypted format, which also not includes any identity information of the participants who sends those data. The encoded data to the End user do not contain any identity information, in such a way that the application server cannot link a data to a specific participant. With such a data reporting protocol, the link between the data and the participants is broken, and as a result, participant's privacy is protected.

Keyword: *Anonymity, Data reporting, Participatory sensing, Privacy*

1. Introduction

The ubiquitous sensor-rich mobile phones had promoted the emergence of a fast rowing people centric sensing paradigm, participatory sensing applications and thus have been playing an increasing important role in the evolution of the Internet of Things. The main idea behind participatory sensing is to use mobile phones as a platform for sensing research, by empowering citizens to collect and share data sensed from the environments using sensor equipped phones. Participatory sensing offers a number of advantages over traditional sensor networks such as reducing cost highly, unprecedented spatiotemporal coverage, easy deployment, and much more.

A typical participatory sensing application follows a client-server architecture, in which data collected by participant's phones are sent to a central server. The server processes all the data, & produces useful statistics report. The statistics may be published in various forms, such as graphical representations or maps showing the sensing results at individual and community scale. Based on the sensing scale, participatory sensing applications can be classified into three categories: 1] Personal sensing applications:-Which are designed for a single individual, such as personal health or sport experiences monitoring ; 2] Group sensing applications:-Which are designed for a set of individuals who share a common goal, concern, or interest, such as social media enhancing; and 3] community sensing applications:-Which conduct large-scale data collection, analysis, and sharing for the good of the community, such as environment and traffic monitoring. Participatory sensing campaigns will revolutionize many sectors of our society if a large number of participants or users are willing to submit their data. On the other hand,

participating in a participatory sensing task, especially a community scale task, could result in private information hacked. Some tasks require users to submit data containing sensitive information, for e.g. disease symptoms . Some applications do not directly use sensitive data, but still result in privacy leakage. For example in a power consumption monitoring application , from temporally fine-grained energy consumption reports submitted by users, household activities can be inferred easily. In addition, data in participatory sensing application are usually geo and time tagged.

From multiple data reported by a participant, an adversary can derive much sensitive information. Thus, users are reluctant to contribute to the sensing campaigns, if their privacy cannot be protected. This would diminish the impact and relevance of sensing campaigns deployed at large scale, as well as limiting the benefits to the users. Therefore, protecting privacy of participants is highly important. A variety of methods are proposed to protect the privacy of each participant or user for participatory sensing applications. The naive mechanism to protect the privacy is to use pseudonyms. However, as demonstrated, the use of pseudonyms does not necessarily guarantee privacy. Some privacy protection methods employ generalization or perturbation, both of which intend to allow the application server to determine community trends without disclosing individual data, by deliberately reducing the accuracy or precision of the sensed data. Nevertheless, this reduction of data accuracy or precision will inevitably degrade the derived statistics reports. Researchers also propose privacy protection methods for certain applications, such as data aggregation, regression modeling, or map generation. However, these methods are only applicable in specific applications & lack generality.

In existing methods, if the application server colludes with a global eavesdropper who can monitor the traffic across the network, it can link each data with its contributor. In this paper, we had proposed a privacy preserving data reporting protocol for participatory sensing application based on the anonymity. The key intuition is that, if we break the link between any data and the participant or user who reports the data, the participant's privacy can be protected, without degrading data accuracy. In this way, as long as the data itself does not contain identification information, it is sufficient to protect participants' privacy.

The advantage of our protocol includes: 1] Participants can report its original sensed data to the application server, with which the server can produce statistics with the highest accuracy. 2] The protocol is general to all kinds of sensing applications as the reported data are non-altered original data, the application server can use the data freely for any kind of data processing and produce any statistics report. 3] Even if the application server colludes with a global eavesdropper, it can't link any data with its contributor.

Specifically, our anonymous based data reporting protocol operates in two phases, slot reservation phase & data submission phase. In slot reservation stage, a group of participants collaborate to construct a vector which contains a set of slots, each of same length. Each slot contains a reservation message from a participant or user, which consists of a pseudonym and the length of the data that the participant or user will submit in the data submission stage. Thus the vector denotes a schedule that all participants will follow when submitting the data. The vector is constructed in such a way that other than the slot owner no one will get to knows the owner of the slot. The data submission stage might includes multiple rounds. In each round, based on the schedule established in the slot reservation stage, each participant submits a bit of stream to the application server, who then XOR all participant's bit streams together to yield a concatenation of all participant's raw data each at its slot. As all the bit streams are encoded with multiple secrets & have the same length, an adversary cannot ascertain which data belongs to which of the participant.

Our contributions can be summarized as follows:-

- We introduce the notion of anonymous data collection for participatory sensing, where anonymous indicates unlinkable, that is, an adversary cannot link any piece of data to the participant who reports that data.

- We present a two-stage protocol for anonymous data reporting, which provides us strong privacy, data accuracy and generality.
- We propose an anonymous slot reservation schemes for the first stage & an efficient XOR based data submission scheme for the second stage of the anonymous data reporting protocol.
- We give the theoretical analysis on correctness and anonymity property of our protocol.
- We provide experimental results to measure practical efficiency of our solutions, which show that the proposed protocol is applicable to small scale that is with tens of participants and periodically sampling applications.

2. Design and Implementation Details

2.1. Modules

1. Participant Module
2. Application Server
3. End User

2.1.1. Modules Description

(A) Participant Module

Users should register in the application to get access into it. Each user will be assigned a separate ID and their IMEI number will be taken and stored in SQL server Database. Once a user successfully registered in the app. He can login using is UserID and password. Once he logged in successfully two tabs will be shown on the samescreen.

(A) Tab-One : User Details will be shown ie; User Name, Device Name,IMEI Number etc,
(B) Tab-Two : Sensor readings that are supported by your android device. This screen will contain a Button to send sensor data to the server. Every 5 minutes data will be send to the server once user quite the app. Application automatically stops from sending data to the server.

(B) Application Server

Administrator is a web portal. So that he can login using is userid and password. Once he logged in he can view all the registered user from the android application. To view the data of the user he can simply select a user from the left side,
so that he can get the sensor data for the particular user. He can also see all the user data at the same Time.

(C) End User

User can view the online reports and give the feed backs according to the type of posts.

3. Problem Formulation

3.1 System Architecture

Privacy protection is an important issue in participatory sensing. We propose an anonymous data reporting protocol for participatory applications to protect user privacy.

- The intuition behind the protocol is that, if the data itself does not contain identification information, and we can break the link between the data and the participant that reports the data, the users privacy can be protected.
- The anonymous data reporting protocol is divided into two stages, a slot reservation stage and a data submission stage.

- In the slot reservation stage, a group of participants collaborate to construct a vector which contains a set of slots, all with the same length. Each slot contains a reservation message from a participant, which consists of a pseudonym and the length of the data that the participant will submit in the data submission stage.
- Thus, the vector denotes a schedule that all the participants will follow when submitting data. The vector is constructed in such a way that other than the slot owner, no one knows the owner of the slot.
- The data submission stage may include multiple rounds. In each round, based on the schedule established in the slot reservation stage, each participant submits a bit stream to the application server, who then XOR all participants' bit streams together to yield a concatenation of all participants' raw data, each at its slot.
- As the entire bit streams are encoded with multiple secrets and have the same length, an adversary cant ascertain which data belongs to which participant.

Smartphones sensors like Proximity, Gravity, Magnetometer, etc., are used to collect data. We are going to use these sensors because most of the smartphones having such sensors in build with them. As Figure 5.1 shows, the application first involves a android module which send sensed data to the Application server after every fixed time interval. Initially all the sensed data from all smartphones will be stored in the SQL server for further processing. We consider that Application Server is the coordinator for collecting the data with applying the encryption to the sensed data. Identity information is not used while encryption, which results in hiding the identity of the participants. These encrypted data is send to the End User for generating the statistical reports.

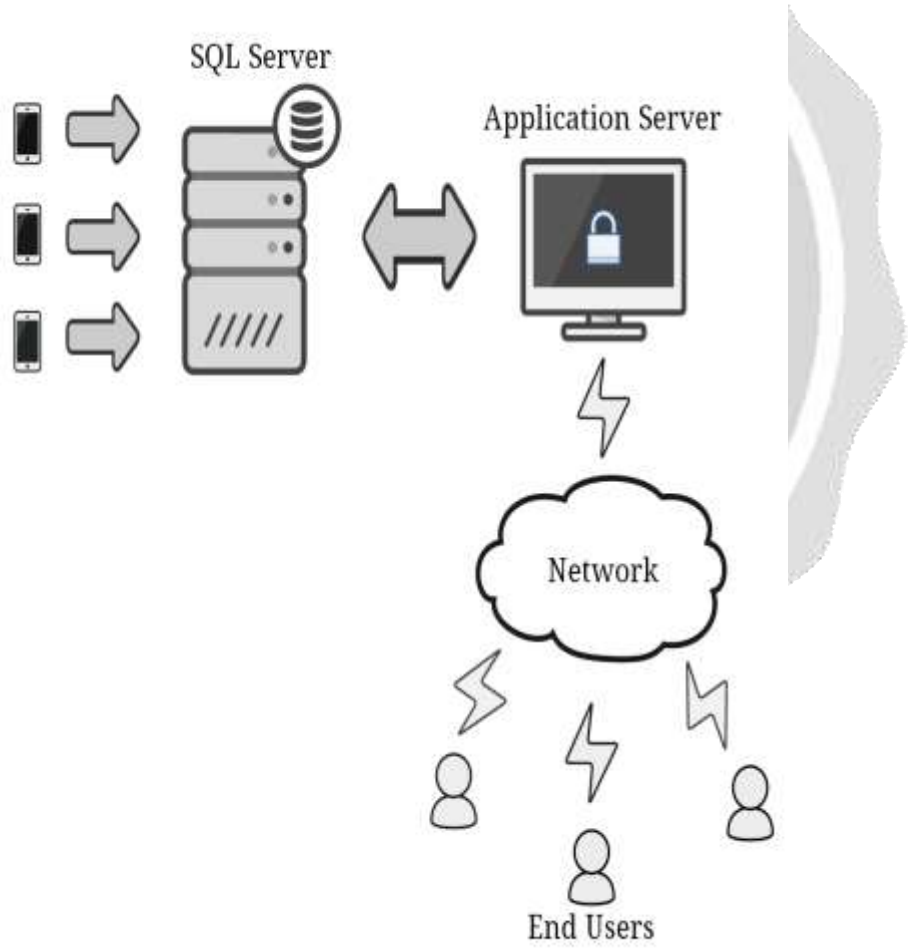

Fig -1: System Architecture

4. Algorithm

4.1 Lamport's Algorithm

Lamport was the first to give a distributed mutual exclusion algorithm as an illustration of his clock synchronization scheme. Let Ri be the request set of site Si (MobileApp) ,i.e. the set of sites from which Si needs permission when it wants to enter CS Critical Section (Application Server). In Lamports algorithm Every site Si keeps a queue, request queuei, which contains mutual exclusion requests ordered by their timestamps. This algorithm requires messages to be delivered in the FIFO order be tween every pair of sites.

A. The Algorithm Requesting the critical section:

1. When a site Si wants to enter the CS, it sends REQUEST (tsi, i) messages to all the sites in its request set Ri and places the request on request queuei (tsi is the timestamp of the request).
2. When a site Sj receives the REQUEST(tsi, i) message from site Si, it returns a timestamped REPLY message to Si and places site Sis request on request queuej

B. Executing the critical section:

Site Si enters the CS when the two following conditions hold:

L1: Si has received a message with timestamp larger than (tsi, i) from all other sites.

L2: Sis request is at the top request queuei.

C. Releasing the critical section:

1. Site Si, upon exiting the CS, removes its request from the top of its request queue and sends a time stamped RELEASE message to all the sites in its request set.
2. When a site Sj receives a RELEASE message from site Si, it removes Sis request from its request queue. When a site removes a request from its request queue, its own request may come at the top of the queue, enabling it to enter CS. The algorithm executes CS requests in the increasing order of timestamp

4.2 RSA Algorithm

RSA encrypts messages through the following algorithm, which is divided into 3 steps:

1. Key Generation
2. Encryption

(a) Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.

3. Decryption

Why RSA Encryption is secure?

-The idea of making one of your own encryption algorithms public on the internet seems very strange at first. However, this is actually one of the most important steps in RSA encryption. If Person C intercepts your message to Person B, they already know the encryption key (exponent e, modulus n). However, what he/she does not have is the decryption exponent d. Since you encrypted your message with Person B's encryption key, only Person B has the decryption key (exponent d, modulus n) to decrypt it. Person C is only missing one piece of information, exponent d, which turns out to be the hardest piece of information to find.

5. CONCLUSION

Privacy protection is an important issue in participatory sensing. We propose an anonymous data reporting protocol for participatory applications to protect user privacy. The intuition behind the protocol is that, if the data itself does not contain identification information, and we can break the link between the data and the participant that reports the data, the user's privacy can be protected. The anonymous data reporting protocol is divided into two stages, a slot reservation stage and a data submission stage. An anonymous slot reservation scheme based on public key encryption & message shuffle & a data submission scheme based on efficient XOR operation has been proposed in this paper. The theoretical analysis verifies the correctness and the anonymity of the protocol. The experiments demonstrate that, for small-scale applications with only tens of participants where data is collected in a periodic manner, the proposed protocol is efficient and applicable.

6. REFERENCES

[1]. Delphine Christina, Andreas Reinhardt, Salil S. Kanhere, Matthias Hollick. A survey on privacy in mobile participatory sensing applications.
The journal of Systems and Software, 2011, 84(11): 1928-1946
[2]. T. Denning, A. Andrew, R. Chaudhri, C.Hartung, J. Lester, G. Borriello, G. Duncan. BALANCE: towards a usable pervasive wellness application with accurate activity inference. In Proc. 10th workshop on Mobile Computing Systems and Applications (HotMobile), 2009, pp. 5:1–5:6.
[3]. Rana, R., Chou, C., Kanhere, S., Bulusu, N., Hu, W., Ear-Phone: anend-to-end participatory urban noise mapping system. In Proc. 9th ACM/IEEE Int. Conference on Information Processing in Sensor Networks (IPSN), 2010, pp. 105–116.
[4]. Mohan, P., Padmanabhan, V., Ramjee, R., Nericell: rich monitoring of road and traffic conditions using mobile smartphones. In Proc. 6th ACM Conference on Embedded Network Sensor Systems (SenSys), 2008, pp.
[5] Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, D. Irwin. Private memoirs of a smart meter, in Proc. of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, BuildSys., 2010, pp. 61–66.
[6] M. Wernke, P. Skvortsov, F. Dürr, K. Rothermel. A classification of location privacy attacks and approaches. Personal and Ubiquitous Computing, 2014, 18(1): 163-175.
[7] Z. Huang, W. Du, B. Chen. Deriving private information from randomized data. In Proc.2005 ACM SIGMOD International Conference on Management of Data (SIGMOD), pp. 37–48.
[8] L. Kazemi, C. Shahabi. A privacy-aware framework for participatory sensing. ACM SIGKDD Explorations Newsletter, 2011, 13(1): 43-51.
[9] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, N. Triandopoulos, AnonySense: a system for anonymous opportunistic sensing. Journal of Pervasive and Mobile Computing, 2010(7): 16–30.
[10] R. Ganti, N. Pham, Y. Tsai, T. Abdelzaher. PoolView: stream privacy for grassroots participatory sensing. In Proc. 6th ACM Conference on Embedded Network Sensor Systems (SenSys), 2008, pp. 281–294.
[11] [15] S.Aoki, H. Kobayashi, M. Iwai, K. Sezaki. Perturbation with General Tendency for Mobile Community Sensing. In Proc. 2nd International Conference on Mobile Services, June 2013, pp. 23-30
[12] Qinghua Li, Guohong Cao. Efficient privacy-preserving stream aggregation in mobile sensing with low aggregation error. In Privacy Enhancing Technologies, January 2013, pp. 60-81
[13] Kai Xing, Zhiguo Wan, Pengfei Hu, Haojin Zhu, Yuepeng Wang, Xi Chen, Yang Wang, Liusheng Huang. Mutual Privacy-Preserving Regression Modeling in Participatory Sensing. In proc. 32rd Annual IEEE International Conference on Computer Communications (INFOCOM), April 2013
[14] Xi Chen, Xiaopei Wu, Xiang-Yang Liy, Yuan He, Yunhao Liu. Privacy-Preserving High-Quality Map Generation with Participatory Sensing, in proc. 33rd Annual IEEE International Conference on Computer Communications (INFOCOM), April 2014
[15] Z. Yang, S. Zhong, and R. Wright. Anonymity-preserving data collection. In Proc. 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining (KDD), 2005, pp: 334–343
[16] J. Brickell, V. Shmatikov. Efficient anonymity-preserving data collection. In Proc. 12th ACM SIGKDD international conference on Knowledge discovery and data mining, August 2006, pp. 76-85.