ISSN No: 2348-4845
International Journal & Magazine of Engineering,
Technology, Management and Research
A Peer Reviewed Open Access International Journal

Preserving Privacy in Participatory Sensing Applications

Thotla Varija
M.tech Student,
Department of Computer Science and Engineering,
VEMU Institute of Technology, Pakala, Chittoor Dist.

G.Lokesh
Assistant Professor,
Department of Computer Science and Engineering,
VEMU Institute of Technology, Pakala, Chittoor Dist.

Abstract:

Participatory Sensing is an emerging computing paradigm that enables the distributed collection of data by self-selected participants. It allows the increasing number of mobile phone users to share local knowledge acquired by their sensor-equipped devices, e.g., to monitor temperature, pollution level or consumer pricing information. While research initiatives and prototypes proliferate, their real-world impact is often bounded to comprehensive user participation. If users have no incentive, or feel that their privacy might be endangered, it is likely that they will not participate. We focus on privacy protection in Participatory Sensing and introduce a suitable privacy-enhanced infrastructure. First, we provide a set of definitions of privacy requirements for both data producers (i.e., users providing sensed information) and consumers (i.e., applications accessing the data). Then, we propose an efficient solution designed for mobile phone users, which incurs very low overhead.

Keywords:

Participatory Sensing, Privacy , WSN, .

1.INTRODUCTION:

In recent times, mobile phones have been riding the wave of Moore's Law with rapid improvements in processing power, embedded sensors, storage capacities and network data rates. The mobile phones of today have evolved from merely being phones to full-fledged computing, sensing, and communication devices. It is thus hardly surprising that over 5 billion people globally have access to mobile phones. These advances in mobile phone technology coupled with their ubiquity have paved the way for an exciting new paradigm for accomplishing large-scale sensing, known in literature as participatory sensing.

The key idea behind participatory sensing is to empower ordinary citizens to collect and share sensed data from their surrounding environments using their mobile phones. Mobile phones, though not built specifically for sensing, can in fact readily function as sophisticated sensors. The cameras on mobile phones can be used as video and image sensors. The microphone on the mobile phone, when it is not used for voice conversations, can double up as an acoustic sensor.The embedded GPS receivers on the phone can provide location information.

Other embedded sensors such as gyroscopes, accelerometers, and proximity sensors can collectively be used to estimate useful contextual information (e.g., if the is user walking or traveling on a bicycle). Further, additional sensors can be easily interfaced with the phone via Bluetooth or wired connections, e.g., air pollution or biometric sensors. Participatory sensing offers a number of advantages over traditional sensor networks which entails deploying a large number of static wireless sensor devices, particularly in urban areas.

- First, since participatory sensing leverages existing sensing (mobile phones) and communication (cellular or Wi-Fi) infrastructure, the deployment costs are virtually zero.
- Second, the inherent mobility of the phone carriers provides unprecedented spatiotemporal coverage and also makes it possible to observe unpredictable events (which may be excluded by static deployments).
- Third, using mobile phones as sensors intrinsically affords economies of scale. Fourth, the widespread availability of software development tools for mobile phone platforms and established distribution channels in the form of App stores makes application development and deployment relatively easy.
- Finally, by including people in the sensing loop, it is now possible to design applications that can dramatically improve the day-to-day lives of individuals and communities.

2. EXISTING SYSTEM:

A plethora of novel and exciting participatory sensing applications have emerged in recent years. CarTel is a system that uses mobile phones carried in vehicles to collect information about traffic, quality of en-route WiFi access points, and potholes on the road. Micro-Blog is an architecture which allows users to share multimedia blogs enhanced with inputs from other physical sensors of the mobile phone. Other applications of participatory sensing include the collection and sharing of information about urban air and noise pollution , cyclist experiences , diets, or consumer pricing information in offline markets.

A typical participatory sensing application operates in a centralized fashion, i.e., the sensor data collected by the phones of volunteers are reported (using wireless data communications) to a central server for processing, as illustrated in Fig. 1. The sensing tasks on the phones can be triggered manually, automatically, or based on the current context. On the server, the data are analyzed and made available in various forms, such as graphical representations or maps showing the sensing results at individual and/or community scale. Simultaneously, the results may be displayed locally on the carriers' mobile phones or accessed by the larger public through web-portals depending on the application needs.

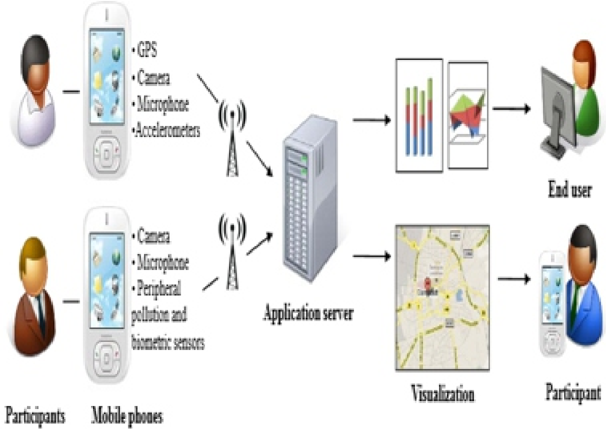

Figure 1: Architectural overview of a typical participatory sensing application

Current participatory sensing applications are primarily focused on the collection of data on a large scale. Without any suitable protection mechanism however, the mobile phones are transformed into miniature spies, possibly revealing private information about their owners.

Possible intrusions into a user's privacy include the recording of intimate discussions, taking photographs of private scenes, or tracing a user's path and monitoring the locations he has visited. Users are reluctant to contribute to the sensing campaigns, once they are aware of possible consequences. Since participatory sensing exclusively depends on user-provided data, a high number of participants is required. The users' reluctance to contribute would diminish the impact and relevance of sensing campaigns deployed at large scale, as well as limiting the benefits to the users. To encounter the risk that a user's privacy might be compromised, mechanisms to preserve user privacy are mandatory.

LIMITATIONS OF EXISTING SYSTEM:

» The mobile phones are behaving like spies, revealing the personal information of the participant.
» No privacy is concerned.
» The sensed reports are revealed to all.

3. PROPOSED SYSTEM:

In this paper, we present our novel solution for a Privacy Preserving Participatory Sensing Infrastructure (PPPSI). PEPSI protects privacy using efficient cryptographic tools. Similar to other cryptographic solutions, it introduces an additional (offline) entity, namely the Registration Authority. It sets up system parameters and manages Mobile Nodes or Queriers registration. However, the Registration Authority is not involved in real-time operations (e.g., query/report matching) nor is it trusted to intervene for protecting participants' privacy.

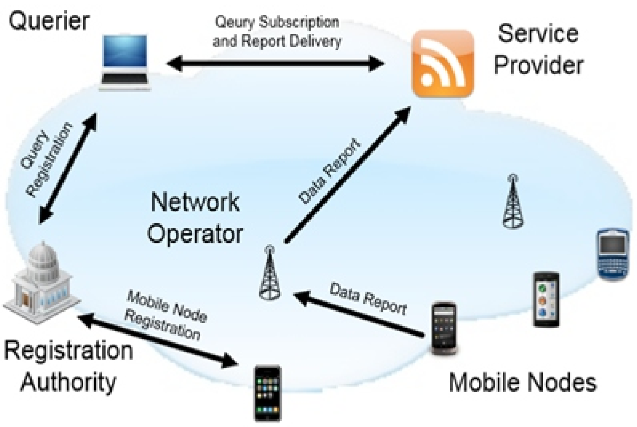

Fig.2: a Privacy Preserving Participatory Sensing Infrastructure (PPPSI).

Figure 2 illustrates the PPPSI architecture. The Registration Authority can be instantiated by any entity in charge of managing participant's registration (e.g., a phone manufacturer). A Service Provider offers PS applications (used, for instance, to report and access pollution data) and acts as an intermediary between Queriers and Mobile Nodes. Finally, Mobile Nodes send measurements acquired via their sensors using the network infrastructure and Queriers are users or organizations (e.g., bikers) interested in obtaining reports (e.g., pollution levels). PPPSI allows the Service Provider to perform report/query matching while guaranteeing the privacyof both mobile Nodes and Queriers. It aims at providing (provable) privacy by design, and starts off with defining a clear set of privacy properties.

3.1 PPPSI OPERATIONS:

Figure 3 shows how PEPSI work. The upper part of the figure depicts the offline operations where the Registration Authority is involved to register both Mobile Nodes and Queriers.

Querier Registration:

In the example, Querier Q (the laptop on the right side) picks "Temp" among the list of available queries and obtains the corresponding decryption key (yellow key).

Mobile Node Registration:

Similarly, Mobile Node M (the mobile phone on the left side) decides to report about temperature in its location and obtains the corresponding secret used for tagging (grey key).

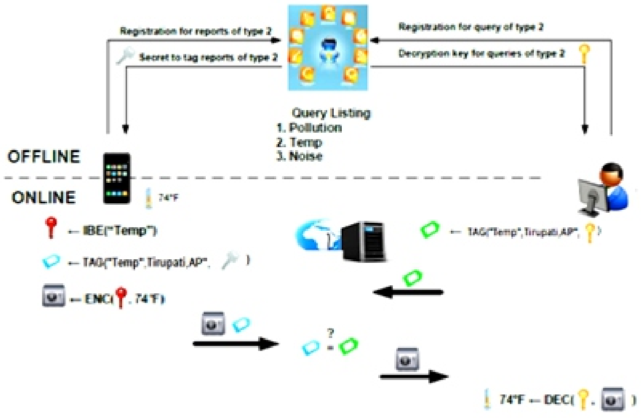
Registration for reports of type 2
Secret to tag reports of type 2
Registration for query of type 2
Decryption key for queries of type 2
Query Listing
1. Pollution
2. Temp
3. Noise
OFFLINE
ONLINE
74°F
← IBE("Temp")
← TAG("Temp",Tirupati,AP",)
← ENC(, 74°F)
← TAG("Temp",Tirupati,AP",)
?
=
74°F ← DEC(,)

Fig. 3: PPPSI Operations

The bottom part of Figure 3 shows the online operations where the Service Provider is involved.

Querier Subscription:

Q subscribes to queries of type "Temp" in "Tirupati, AP" using these keywords and the decryption key acquired offline, to compute a (green) tag; the algorithm is referred to as TAG () . The tag leaks no information about Q's interest and is uploaded at the Service Provider.

Data Report:

Any time M wants to report about temperature, it derives the public decryption key (red key) for reports of type "Temp" (via the IBE() algorithm) and encrypts the measurement; encrypted data is pictured as a vault. M also tags the report using the secret acquired offline and a list of keywords characterizing the report; in the example M uses keywords "Temp" and "Tirupati, AP". Our tagging mechanism leverages the properties of bilinear maps to make sure that, if M and Q use the same keywords, they will compute the same tag, despite each of them is using a different secret (M is using the grey key while Q is using the yellow one). As before, the tag and the encrypted report leak no information about the nature of the report or the nominal value of the measurement. Both tag and encrypted data are forwarded to the Service Provider.

Report Delivery:

The Service Provider only needs to match tags sent by Mobile Nodes with the ones uploaded by Queriers. If the tags match, the corresponding encrypted report is forwarded to the Querier. In the example of Figure 3 the green tag matches the blue one, so the encrypted report (the vault) is forwarded to Q. Finally, Q can decrypt the report using the decryption key and recover the temperature measurement.

5. CONCLUSION:

Participatory Sensing is a novel computing paradigm that bears a great potential. If users are incentivized to contribute personal device resources, a number of novel applications and business models will arose. In this paper we discussed the problem of protecting privacy in Participatory Sensing. We claim that user participation cannot be afforded without protecting the privacy of both data consumers and data producers.

We also proposed the architecture of a privacy-preserving Participatory Sensing infrastructure and introduced an efficient cryptographic solution that achieves privacy with provable security. Our solution can be adopted by current Participatory Sensing applications to enforce privacy and enhance user participation, with little overhead.This work represents an initial foray into robust privacy guarantees in PS, thus, much remains to be done. Items for future work include (but are not limited to):

1.Protecting query privacy with respect to the Registration Authority.

2.Protecting node privacy with respect to the Network Operator. Current technology does not allow hiding users' locations and identities from to the Network Operator. Hence, it is an interesting challenge to guarantee node anonymity in broadband networks.

3.Addressing collusion attacks, where multiple entities might collaborate in order to violate the privacy of Mobile Nodes or Queriers

REFERENCES:

[1] E.S. Cochran and J.F. Lawrence and C. Christensen and R.S. Jakka, the Quake Catcher Network: Citizen Science expanding seismic horizons, Seismological Research Letters, vol. 80, 2009, pp. 26-30.

[2] C. Cornelius and A. Kapadia and D. Kotz and D. Peebles and M. Shin and N. Triandopoulos, Anony- Sense: Privacy-aware people-centric sensing, 6th International Conference on Mobile Systems, Applications, and Services (MobiSys), 2008, pp. 211-22.

[3] Emiliano De Cristofaro and Claudio Soriente, Participatory Privacy: Enabling Privacy in Participatory Sensing, IEEE TRANSACTIONS ON NETWORKING VOL.27 NO.1 YEAR 2013.

[4] E. De Cristofaro and C. Soriente, Privacy-Preserving Participatory Sensing Infrastructure, http://www.emilianodc.com/PEPSI/.

[5] P.T. Eugster and P.A. Felber and R. Guerraoui and A.M. Kermarrec, The many faces of publish/ subscribe, ACM Computing Surveys, vol. 35, no. 2, 2003, pp. 114-131.

[6] R.K. Ganti and N. Pham and Y.E. Tsai and T.F. Abdelzaher, Pool View: stream privacy for grassroots participatory sensing, 6th International Conference on Embedded Networked Sensor Systems (SenSys) 2008, pp. 281-294.

[7] P. Gilbert and L.P. Cox and J. Jung and D.Wetherall, Toward trustworthy mobile sensing, 11thWorkshop on Mobile Computing Systems and Applications (Hot Mobile), 2010, pp. 31-36.

[8] M. Ion and G. Russello and B. Crispo, Supporting Publication and Subscription Confidentiality in Pub/Sub Networks, 6th Iternational ICST Conference on Security and Privacy in Communication Net- works (SecureComm), 2010, pp. 272-289.

[9] D.H. Kim and J. Hightower and R. Govindan and D. Estrin, Discovering semantically meaningful places from pervasive RF-beacons, 11th International Conference on Ubiquitous Computing (Ubi- Comp), 2009, pp. 21-30.

[10] S. Kuznetsov and E. Paulos, Participatory sensing in public spaces: activating urban surfaces with sensor probes,ACM Conference on Designing Interactive Systems (DIS), 2010, pp. 21-30.

[11] B. Longstaff and S. Reddy and D. Estrin, Improving activity classification for health applications on mobile devices using active and semi-supervised learning, 4th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2010, pp. 1-7.

[12] N. Maisonneuve and M. Stevens and M.E. Niessen and L. Steels, NoiseTube: Measuring and mapping noise pollution with mobile phones, 4th International ICSC Symposium on Information Technologies in Environmental Engineering (ITEE), 2009, pp. 215-228.

[13] E. Paulos and R.J. Honicky and E. Goodman, Sensing Atmosphere, Sensing on Everyday Mobile Phones in Support of Participatory Research (SenSys workshop), 2007, pp. 1-3.

[14] J. Shi and R. Zhang and Y. Liu and Y. Zhang, PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems, 29th IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 758-766.

[15] K. Shilton, Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection, Communications of the ACM, vol. 52, no. 11, 2009, pp 48-53.