Indian Journal of Science and Technology, *Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102076, October 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Design Perspectives of People Centric Sensing Systems

K. R. Jansi[1]* and S. V. Kasmir Raja[2]

[1]Department of Computer Science and Engineering, SRM University, Kattankulathur, Chennai - 603203, Tamil Nadu, India; jansi.k@ktr.srmuniv.ac.in
[2]SRM University, Kattankulathur, Chennai - 603203, Tamil Nadu, India; svkr@yahoo.com

Abstract

Mobile devices play a vital role in our day to day life. The various sensing modalities available in mobile devices are identified and justify the growth of the capabilities on today's smart phones.Taking advantage of the sensing capabilities of the mobile devices paves way for a new era of network, referred as people centric sensing network. In this paper, a broad study about the applications, architectural components and the existing privacy and security architectures available are discussed. The applications of mobile sensing are categorized as personal, social and public sensing based on what they sense, how they share and infer. All these applications clearly depict the roles played by people. People may act as end users, as participants and as application administrators. Since people are in the loop, the basic privacy and security requirements are analyzed that can be realized as the need in the design of any mobile phone sensing systems. The possible threats that arise in this sensing context may be due to both internal and external entities. The strategies and types of adversarial models in the people centric sensing approach provides us light to how the framework works and solutions needed. Existing literature in terms of privacy preserving data aggregation schemes and security Frameworks are also discussed in detail. **Applications:** The model clearly portraits the importance of people who are no more only passive data users. More focus has to be given on privacy preserving models to make the system more acceptable by the people.

Keywords: Design, Mobile Sensing Systems, Participatory Sensing, People Centric Sensing, Privacy, System Model

1. Introduction

Enrichment of capabilities in today's smart phones in terms of communication, sensing and computation has paved way for variety of large scale mobile sensing applications. Now, smart phones are inseparable from our human life. A smart phone is a mobile phone offering advanced capabilities, often with PC- like functionality and sensing applications as depicted in Figure1.These smart phone capabilities and accessories can be used together to form a collaborative network providing scope for lot of mobile sensing applications. Every individual carry their own mobile devices and these devices can contribute sensory data related to the context of the people and their surroundings. Mobile phone sensing can create wider impact when the sensing tasks are assigned to a large group of people by crowd sourcing. Based on the approach used to collect the data and involvement of user in the sensing process, there are different dimensions in mobile phone sensing systems. These approaches are also called as Mobile phone sensing or People Centric Sensing (PCS)[1] either opportunistic or participatory sensing or mobile crowd sensing or citizen sensing or urban sensing. But the common factor that lays in the intersection of these approaches is people are in the loop of the network. Here people are both the data users and data contributors. So, concern for privacy and security of users is an open challenge in this area. Without deploying a sensor network, physical network is sensed using mobile devices carried by people. When people are directly involved in the active decision making of the sensing process, they are referred as Participatory sensing. When the expected

*Author for correspondence

context of the application matches with the environment then sensing ability is automatically triggered, they are referred as opportunistic sensing.

1.1 Traditional Wireless Sensor Networks

The characteristics of PCS are quite different from traditional wireless sensor networks (WSN). PCS is much suitable for large scale application. In PCS, the system device belongs to individuals with different interests. The system devices can be charged regularly and hence has more powerful energy resource. Sensing data are more related to interactions between people and between people and their surroundings. System node mobility is dynamic and people are not just data users but also active data contributors. In WSN, system devices are owned and managed by a single authority. Here, the sensor devices are not charged regularly and network is mostly static. The sensing data is related to some physical phenomena of interest like temperature, moisture etc. People are only passive users of the data generated by the sensors.

1.2 Classification of Applications

Mobile phone sensing application[2] can be categorized as personal, social and public based on the focus of the system. The day to day activity of persons or routine is monitored by an application; they are referred as personal sensing. These applications can be used to motivate individual and generate data for the consumptions of users themselves and not necessarily be shared with others. Social sensing applications focus on collecting and sharing social information about the custodians with their peers or community that share a common interest. Public sensing application focus on sensing and sharing environmental data of the custodians with everyone which can be used for the goodness of the public. The Figure 2 lists the various mobile phone sensing applications based on their category.

2. Participatory Sensing Application

Users actively participate in participatory sensing applications by contributing sensory data generated from their device. Degree of user involvement is high in participatory sensing applications. Figure 3 shows an architectural overview[3]of participatory sensing applications. The Roles played by people are as end users, participants and administrators. End users are people who actually use the application or web portal to view the results or inferences summarized by the system. The results are also presented using visualization techniques like maps, graphs and charts to enable the user interpret them. Users can query the application server for the data that fits the context of the application. Participants are the custodians of the mobile devices and active data contributors for the system. They push the data to the server through standard communication capabilities like Wi-Fi or 3G/4G or Bluetooth standards. Participants can also act as end users and access the data inferred. Participants are also users and get incentives or rewards for their contribution. They also get benefited in terms of data inferences derived from their peer community who share a common interest. Administrators are the community head or organizations who design applications and make it available for people to download and get benefitted. They process

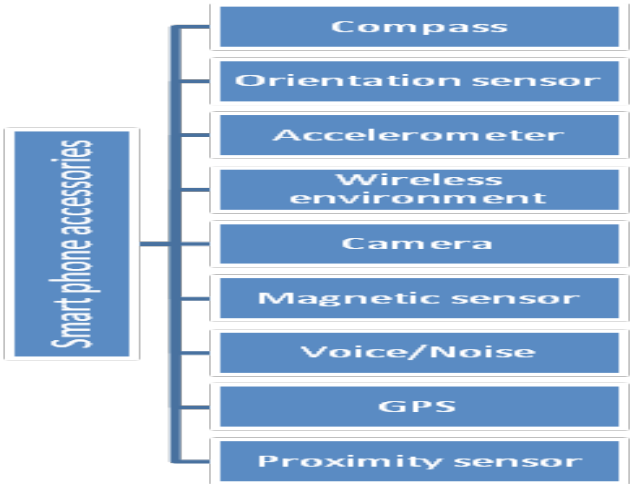

Figure 1. Smart phone accessories.

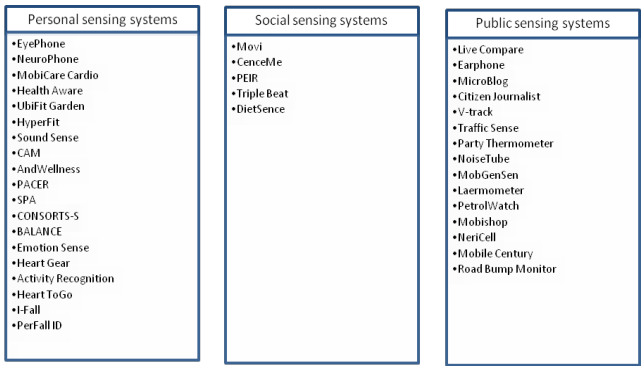

Figure 2. Mobile phone sensing System applications.

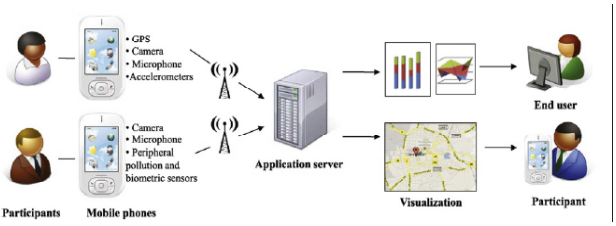

Figure3. Typical participatory sensing application.

the data contributed by the participants and infer results and present it for end users. Administrators maintain the application servers and provide incentives for the participants. They are the task initiators and direct the query to the appropriate mobile nodes available in a region through aggregation servers. Sensing, Processing, Storage and Reporting are the task component involved with the mobile phones. The application servers are responsible for tasking, Storage, Processing and Presentation.

2.1 Basic Privacy and Security Requirements

Users should participate in sensing tasks without revealing their identity. The identity in terms of user specific data and device specific data has to be hidden. Users should receive credits and rewards for their participation without associating themselves with the data or the tasks they contributed. The incentive mechanism should be resilient such that users cannot exploit them to increase their benefits. All the participating entities should be authenticated during every join in the network. The data communicated by the participants should not be disclosed to or altered by any unauthorized persons. Thus communication integrity and confidentiality need to be maintained. Proper access control policy defined by administrators has to be in place. Data contributed by users should be validated and ensure proper mechanisms to assess the trust of the data. Users should be held accountable for any misleading actions that disturb the proper functioning of the system. The Figure 4 depicts the consolidated view of privacy and security requirements[4].

2.2 System Model

The basic system model in PCS is depicted in Figure 5. Here the users who has the custody of the mobile device are called the Mobile Nodes (MN).The MN's contribute sensory information to the Aggregation Server (AS) where the aggregation statistics is computed for the

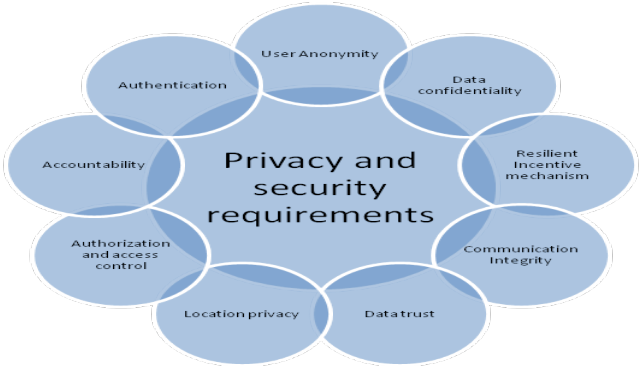

Figure 4. Privacy and security requirements.

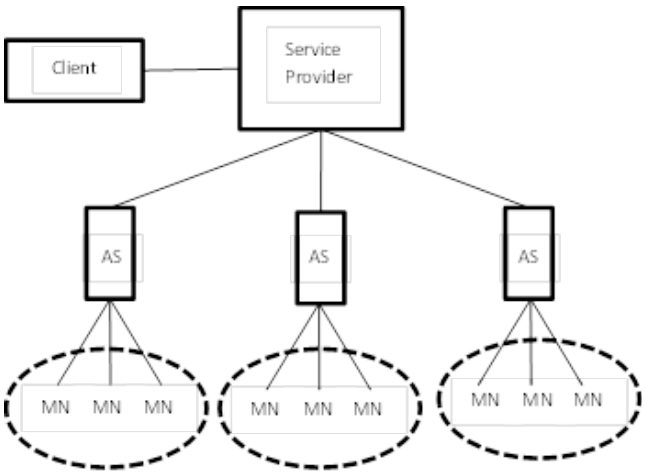

Figure 5. System model.

request received from the corresponding service provider. Each AS is in charge of certain region called as area and interacts with the nodes available in the area. The service provider is the entity which processes the request given by the client and directs it to the AS. The Peer-to-Peer communication and communication between AS and MN are possible through WIFI or Bluetooth standards. In PCS, client requests may be handled by various third party entities and aggregation server which creates a threat to the user's sensitive data contributed by the mobile nodes. The service provider needs to provide extra incentives to motivate user participation.

2.3 Threat Model

There are two types of attacks either internal or external attacks. If the adversary is a system entity then it is referred as internal attacks. A node and the aggregation server may be curious, malicious or both. If the adversary

is not the system entity, it is referred as external attacks. They might be a third party entity who is interested with the data shared by the community. An adversary may eaves drop the communication between mobile node and the aggregation server. Encryption schemes can be used to provide security to the system. False data injection attack, forgery attack can cause damage to the data integrity and data accuracy. Differential attacks have to be considered during the privacy preserving data aggregation. In mobile phone sensing applications each user has to contribute the sensor data of their device. The assumption of Trusted Platform Module [5] in the device ensures the integrity of the data generated by the sensors and the users. Thus the data trust worthiness can be achieved in the system.

2.4 Adversarial Model and Strategies

To address the threats discussed in the above section, analysis about the adversaries[6] and their approach towards the system is necessary.

2.4.1 Resident Adversary[6]

When the adversary exists always on the network it is called as resident adversary. The adversary controls the sensors during the sensing, dissemination and query phase of the network. Privacy and security is harder to achieve during such circumstances.

2.4.2 Non Resident Adversary[6]

In this model, adversary is not always on the network. It releases the sensors at times. It corrupts the sensors only after certain phases and releases the sensors often to go undetected. Higher degree of privacy and security aspects can be achieved compared with the resident model.

Adversaries may select the sensors to compromise based on the following approaches.

2.4.3 Randomly Distributed Adversary[6]

The adversary may select the nodes for compromise randomly. No particular strategies are followed to take control of the nodes.

2.4.4 Local Adversary[6]

The adversary may follow a strategy to corrupt the nodes. It may focus on a specific region of the network or any grid like network structure.

3. Privacy Preserving Data Aggregation Schemes in People Centric Sensing System

3.1 PRISENSE[7]

To meet the privacy requirements of People centric sensing systems, in Suggests a scheme based on the idea of data slicing and mixing. PRISENSE supports additive and non-additive aggregations. Three novel cover node selection strategies are used to tackle the user dynamics and dynamic nature of the network. They are random cover selection, one hop scheme and h-hop scheme.

3.2 VPA[8]

VPA is based on data slicing and mixing method. It addresses the user privacy and integrity of the data. VPA is designed for both additive and non-additive aggregation function. Here the idea is to divide the aggregation process in to two phases. In the first phase every node computes a homomorphic MAC of its original data and submits it to the aggregation server. The homomorphic property enables aggregation server to generate desired statistics without recovering the original data contributed by the user. In the second phase, using data slicing and mixing technique each user share their own data with the selected peers and then submit the mixed data to the AS. The aggregation server is now able to verify the integrity of the data shared by the user with the data submitted in the first phase. Hence VPA requires multiple rounds of bidirectional communication between the aggregation server and mobile nodes which leads to long delays. VPA is not suitable for time series data and also not fault tolerant to failure of mobile nodes. VPA+ is designed for non-additive aggregation functions through a unique combination of the binary search and verifiable privacy preserving count queries. VPA is not resistant to differential attacks. In Focus on query and data privacy. The sensed data should be protected against unauthorized access and also the queriers might not be willing to reveal their interests. Adversarial models and strategies are discussed with the preferred dissemination method for the data. In non-resident adversary model, the adversary is not always present in the network but it corrupts after both the sensing and dissemination phase have been completed. A resident adversary is always on the network and controls the sensors at all times. Privacy is harder to achieve in the presence of resident adversary.

The adversary selects the sensors to compromise based on two strategies. If the adversary is randomly distributed over the network, it controls m randomly selected sensors. Otherwise adversary focuses on a specific region of the network. Though the degree of privacy is higher in a non-resident adversary, they incur higher message overhead. The various dissemination strategies suitable for the adversarial model are discussed and analyzed. The proposed distributed privacy preserving technique for each type of adversarial models rely on generating replica of the sensed data. Replication not only achieves privacy but also enhances data reliability and fault tolerance. In [9] Propose an efficient protocol to achieve sum aggregate that uses the additive homomorphic encryption technique. The straw man construction algorithm for key generation is extended to reduce the computation overhead at the aggregator. The derived key management technique supports large plain text space and also achieves better security. The sum aggregate protocol is also extended to support time series data. This protocol does not require bidirectional communication between the aggregator and mobile users in every aggregation period there by reducing the communication overhead. The protocol protects the privacy of the user's data in the presence of untrusted aggregator and hence supports strong adversarial model. In mobile sensing applications, dynamic addition and removal of users may occur frequently. So, redundancy technique for assigning security parameters for users is used to address the user dynamics. The sum aggregation scheme has much less communication overhead and need to be extended to support other aggregation statistics.

3.3 Secure and Privacy Related Work

General purpose security and privacy architecture for PCS is proposed in AnonySense[10]. Statistical K-Anonymity is achieved where individuals cannot be identified within a set of k users assumed to reside in the same area at a given moment in time. It also prevents Report linkability problem. Group signatures are used to achieve user anonymity. PoolView[11] is a privacy preserving scheme which uses data perturbation technique to preserve the identity of the user data. It considers only privacy of data streams and also achieves accuracy in deriving the statistics over the perturbed data. TAPAS[12] ensure privacy preserving participatory sensing framework and considers data trust worthiness. Redundancy model is used to ensure the higher degree of trust of user's data. PEPSI[13] focus on the privacy of the data queriers and prevents unauthorized entities from querying with a security solution. PEPPer[14] also protects the privacy of the parties querying mobile nodes. Generally, the privacy and confidentiality aspect can be achieved using homomorphic encryption schemes[15].

4. Conclusion

A people centric sensing system leverages the use of existing infrastructures and avoids the deployment cost available in the traditional wireless sensor networks. It has paved way for large scale urban sensing applications. This paper discusses the architectural and tasking components involved in the participatory sensory applications. Thus, the model depicts the importance of participants who are no more only passive data users. This significant difference motivates researchers to focus on designing a secured privacy preserving framework for mobile phone sensing systems. A resilient incentive mechanism also to be considered to encourage users to contribute data and get benefitted with rewards. Trust management has to be incorporated with existing PCS framework for substantial growth expected in this domain. Existing Literature on privacy preserving data aggregation model clearly focuses on achieving data integrity, data confidentiality by reducing the communication and computation overhead. More focus has to be given on privacy preserving models to make PCS more acceptable by the people.

5. References

1. Campbell AT, Eisenman SB. The rise of people-centric sensing. IEEE Internet Computing. 2008 Jul–Aug; 12(4):12–21.
2. Khan WZ, Xiang Y. Mobile phone sensing systems: A survey. IEEE Communication Surveys and Tutorials. 2013 Feb; 15(1):402–27.
3. Christin D, Reinhardt A, Kanhere SS, Hollick M. A survey on privacy in mobile participatory sensing applications. The Journal of Systems and Software. 2011 Nov; 84(11):1928–46.
4. Thanassisgiannetsos, Gisdakis S, Papadimitratos P. Trustworthy people centric-sensing: Privacy, security and user incentives road-map. Annual Mediterranean Adhoc Networking Workshop. 13th Annual Mediterranean;2014 Jun. p. 39–46.
5. Padma RS. An efficient strategy to provide secure authentication on using TPM. Indian Journal of Science and Technology. 2015 Dec; 8(35):1–8.

6. De Cristofaro E, Di Pietro R. Adversaries and countermeasures in privacy-enhanced urban sensing systems. IEEE Systems Journal. 2013 Jun; 7(2):311–22.
7. Shi J, Zhang Y, Liu Y. Prisense: privacy-preserving data aggregation in people-centric urban sensing systems. INFOCOM, Proceedings IEEE; 2010 Mar. p. 1–9.
8. Zhang R, Shi J, Zhang Y. Verifiable privacy-preserving aggregation in people-centric urban sensing systems. IEEE Journal on Selected Areas in Communications. 2013 Sep; 31(9):268–78.
9. Li Q, Cao G, La Porta T. Efficient and privacy-aware data aggregation in mobile sensing. IEEE Transactions on Dependable and Secure Computing. 2014 Mar–Apr; 11(2):115–29.
10. Cornelius C, Kapadia A, Kotz D, Peebles D, Shin M, Triandopoulos N. Anonysense: privacy –aware people centric sensing. Proceedings of the 6th International Conference on Mobile Systems, Applications and Services, Breckenridge: USA; 2008. p.211–24.
11. Ganti RK, Pham N, Tsai YE, Abdelzaher TF. Pool view: Stream privacy for grassroots participatory sensing. Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems Sensys'08, Raleigh, NC: USA; 2008. p. 281–94.
12. Kazemi L, Shahabi C. TAPAS:Trustworthy Privacy Aware Participatory Sensing. Knowledge and Information Systems. 2013 Oct; 37(1):105–28.
13. DeCristofaro E, Soriente C. Extended capabilities for a Privacy Enhanced Participatory Sensing Infrastructure (PEPSI).IEEE Transactions on Information Forensics and Security. 2013 Dec; 8(12):2021–33.
14. PEPPer: Aquerier's Privacy Enhancing Protocol for Participatory sensing [Internet]. [Cited 2012]. Available from: http://ioanniskrontiris.de/publications/queryPrivacyMobiSec2012.pdf.
15. Suveetha K, Manju T. Ensuring confidentiality of cloud data using homomorphic encryption. Indian Journal of Science and Technology. 2016 Feb; 9(8):1–7.