ISSN:0975-9646

A Review on Privacy Enhanced Participating Sensing Infrastructure Architecture

Amandeep Kaur[1], Simarjeet Kaur[2]

[1]*M.Tech. Student, Department of Computer Science and Engineering*
Sri Guru Granth Sahib World University (SGGSWU)
Fatehgarh Sahib, Punjab, India.

[2]*Assistant Professor, Department of Computer Science and Engineering*
Sri Guru Granth Sahib World University (SGGSWU)
Fatehgarh Sahib, Punjab, India.

Abstract—The extreme use of mobile phones has magnified the quantity of digital knowledge created and processed on a daily basis. Participatory Sensing (PS) is associated paradigm that focuses on the collection of digital knowledge created from an oversized variety of connected, always-on, always-carried mobile devices. PS takes the advantage of fast movement of the sensor-equipped devices and therefore the omnipresence of broadband network infrastructure produces sensing applications wherever readying of a WSN infrastructure is not economical or impractical. It targets to provide high level of privacy and security in participatory sensing to knowledge producers like users. They focus on privacy protection in Participatory Sensing and introduce a suitable privacy-enhanced infrastructure.

***Keywords*— Participatory Sensing, Privacy, Mobile Node, Querier.**

I. INTRODUCTION

In recent years, the huge prevalence of mobile computing devices like smart phones and computers. These devices usually come with multiple embedded sensors, such as camera, microphone, GPS, accelerometer, digital compass and gyroscope. Because of these advancements, the participatory sensing model is becoming popular. Participants use their personal mobile devices to gather data about nearby environment and make them available for large scale applications. Two examples of participatory sensing applications are Gigwalk [1] developed by a startup company and Crowd developed by University of Massachusetts Amherst. They provide a market place for sensing tasks that can be performed from smart phones. A requester of data can create tasks that uses the general public to capture geo-tagged images, videos, audio snippets, or fill out surveys. Participants who have installed the client apps on their smart phones can submit their data and get rewarded. For example, Microsoft Bing has been collecting photos using Gigwalk for panoramic 3-D photosynthesis of businesses and restaurants in Bing Map. Sharing sensed data tagged with spatio-temporal information could reveal a lot of personal information, such as a users identity, personal activities, political views, health status, [3] which poses threats to the participating users. Therefore, participatory sensing requires a deeper attention to privacy and anonymity. A mechanism to preserve users location privacy and anonymity is mandatory. Another dimension of data security in participatory sensing is the reliability of the sensed data. In participatory sensing applications, data originates from sensors controlled by other people, and any participant with an appropriately configured device can easily submit falsified data. The data trustworthiness becomes more crucial than the traditional wireless sensor networks. There is an inherent conflict between trust and privacy. If a participatory sensing system provides full anonymity to the participants, it is difficult to guarantee the trustworthiness of submitted data. Finding a solution that achieves both trust and anonymity is a major challenge in such systems [4]. The proliferation of mobile phones, along with their pervasive connectivity, has propelled the amount of digital data produced and processed every day. This has driven researchers and IT professionals to discuss and develop a novel sensing paradigm, where sensors are not deployed in specific locations, but are carried around by people. Today, many different sensors are already deployed in our mobile phones, and soon all our gadgets (e.g., even our clothes or cars) will embed a multitude of sensors (e.g., GPS, digital images, accelerometers, etc.). As a result, data collected by sensor-equipped devices becomes of extreme interest to other users and applications. For instance, mobile phones may report (in real-time) temperature or noise level, similarly, cars may inform on traffic conditions. This paradigm is called Participatory Sensing (PS) – sometimes also referred to as opportunistic or urban sensing [3]. It combines the ubiquity of personal devices with sensing capabilities typical of WSN.

II. PARTICIPATORY SENSING

PS is an emerging paradigm that focuses on the seamless collection of information from a large number of connected, always-on, always-carried devices, such as mobile phones. PS leverages the wide proliferation of commodity sensor-equipped devices and the ubiquity of broadband network infrastructure to provide sensing applications where deployment of a WSN infrastructure is not economical or not feasible. PS provides fine-grained monitoring of environmental trends without the need to set up a sensing infrastructure. The mobile phones are the sensing infrastructure and the number and variety of applications

are potentially unlimited. Users can monitor gas prices , traffic information , available parking spots , just to cite a few. They refer readers to [4] for an updated list of papers and projects related to PS. PS is not a mere evolution of WSN, where motes are replaced by mobile phones. Sensors are now relatively powerful devices, such as mobile phones, with much greater resources than WSN motes. Their batteries can be easily recharged and production cost constraints are not as tight. The traditional WSN, the network operator is always assumed to manage and own the sensors. On the contrary, this assumption does not fit most PS scenarios, where mobile devices are tasked to participate into gathering and sharing local knowledge. A sensor might choose whether to participate or not. As a result, in PS applications, different entities co-exist and might not trust each other. PEPSI architecture comprises of the following components:

1. Sensors installed on smart phone or other wireless enabled devices, emit data reports and form the basis of any participatory sensing infrastructure**.**

2. **Mobile Nodes** are the union of a carrier (i.e., a user) with a sensor installed on a mobile phone or other portable, wireless-enabled device. They provide reports and form the basis of any PS application. The data collected from sensors is also called report.

3.**Queriers** subscribe to information collected in a PS application (e.g., "temperature in Irvine, CA") and receiving sensor reports.

4. **Network Operators** manage the network used to collect and deliver sensor measurements , e.g., they maintain GSM and/or 3G/4G networks. It is responsible for the communication infrastructure.

5. **Service Providers** act as intermediaries between Queriers and Mobile Nodes, in order to deliver report of interest to Queriers. Service provider are cloud-based services that allow effective sharing of information between mobile nodes and queriers. Since mobile nodes and queriers have no mutual knowledge, service providers are key to participatory sensing applications. Service providers are responsible for data collection and dissemination to interested queriers[4]**.**

Assume that Alice subscribes to "available parking spots on W sixteenth Street, New York", or Bob is fascinated by the "temperature in green, New York". Mobile Nodes share native data either voluntary or reciprocally for a few profit—with one or a lot of Service suppliers, that create data obtainable to Queriers. For instance, assume Carol movable sends report "3 obtainable parking spots on E 56th, New York", whereas John device sends "74oF in green, New York". Mobile Nodes and Queriers have not any direct communication nor mutual data, Service suppliers route reports matching specific subscriptions to their original Queriers. In fact, Mobile Nodes ignore that Queriers (if any) have an interest in their reports. For instance, the Service supplier forwards John's temperature report back to Bob; Carol parking report is not sent to Alice because it refers to a different location.

III.ARCHITECTURE

PEPSI protects privacy victimization economical science tools. Similar to different sciences solutions, it introduces an extra (offline) entity, particularly the Registration Authority. It sets up system parameters and manages Mobile Nodes or Queriers registration. The Registration Authority is not involved in time period operations (e.g., query/report matching) neither is it sure to intervene for shielding participants privacy.

Figure 1 illustrates the PEPSI architecture. The Registration Authority can be instantiated by any entity in charge of managing participants 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).

PEPSI allows the Service Provider to perform report/query matching while guaranteeing the privacy of both mobile Nodes and Queriers. It aims at providing (provable) privacy by design, and starts off with defining a clear set of privacy properties.

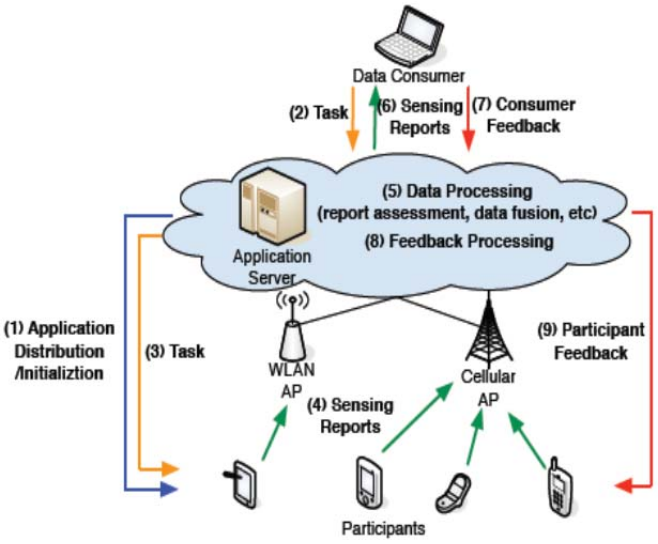


Figure1: Architecture of a participatory sensing system

IV. APPLICATIONS

The applications of PS are explained below:

Soundness: Upon subscribing to a query, Queriers in possession of the appropriate authorization always obtain the desired query results.

Node Privacy*:* Neither the Network Operator, the Service Provider, nor any unauthorized Querier, learn any information about the type of measurement or the data reported by a Mobile Node. Mobile Nodes should not learn any information about other nodes reports. Only Queriers in possession of the corresponding authorization obtain reported measurements.

Query Privacy*:* Neither the Network Operator, the Service Provider, nor any Mobile Node or any other Querier, learn any information about Queriers subscriptions.

Report Unlink ability: No entity can successfully link two or more reports as originating from the same Mobile Node.
Location Privacy: No entity can learn the current location of a Mobile Node. (Again, excluding the Network Operator).
In realistic scenarios, it appears unlikely – if not impossible – to guarantee Report Unlink ability and Location Privacy with respect to the Network Operator.

V. OPERATIONS

Figure 2 represents the working of PEPSI. The upper part of this figure depicts the offline operations where the Registration Authority is involved to register both Mobile Nodes and Queriers.
Setup: In this phase, the RA generates all public parameters and its own secret key.
Querier Registration: Queriers approach the appropriate RA and request an authorization to query the participatory sensing application and order to obtain a specific type of data reports. 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: Users register their sensor-equipped device to the RA and install participatory sensing software. The Mobile Node may also fetch the list of data reports types for which it will later provide reports. A public list of report types may be available from either the SP or the RA. 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). The bottom part of figure 2 shows the online operations where the Service Provider is involved.

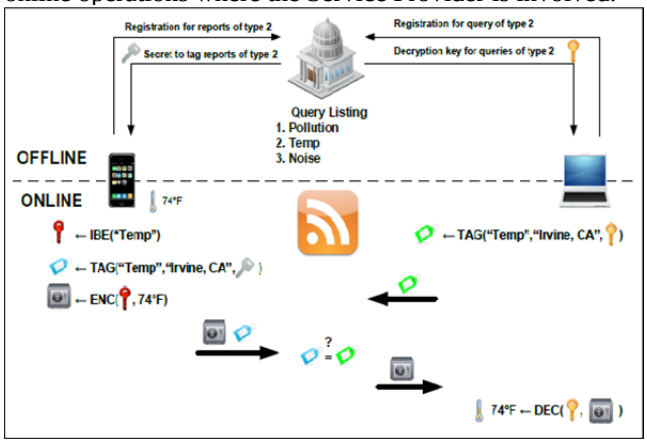


Figure 2: PEPSI operations.

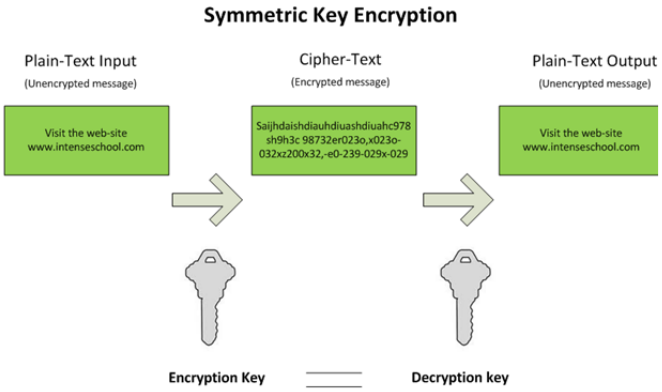
Querier Subscription: Q subscribes to queries of type "Temp" in "Irvine, CA" using these keywords and the decryption key acquired offline, to compute a (green) tag; the algorithm is referred to as TAG(). The tag leaks no information about Q interest and is uploaded at the Service Provider**.**
Data Report: 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 "Irvine, CA". 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 2 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[1].

VI. ENCRYPTION TECHNIQUES

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. In case of PEPSI architecture following encryption schemes are used.
AES: AES is predicated on the Rijndael cipher developed by Belgian cryptographers, Joan Diemen and Vincent Rijmen, United Nations agency submitted a proposal to office throughout the AES choice method. AES may be a symmetric-key algorithmic rule, which means identical secret is used for each encrypting and decrypting the information. AES is predicated on a style principle referred to as a substitution-permutation network, combination of each substitution and permutation and it is quick in each software package and hardware. In contrast to its forerunner DES, AES does not use a Feistel network. AES may be a variant of Rijndael that features a fastened block size of 128 bits, and a key size of 128, 192, or 256 bits. In contrast, the Rijndael specification in and of itself is nominal with block and key sizes that will be any multiple of thirty two bits, each with a minimum of 128 and a most of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, though some versions of Rijndael have a bigger block size and these have extra columns within the state. The key size used for Associate in Nursing AES cipher specifies the quantity of repetitions of transformation rounds that convert the input, known as the plaintext, into the ultimate output, known as the cipher text.
AES is a symmetric key encryption algorithm, which essentially means that the same key is used for the encryption and decryption of the data. A computer program takes clear text and processes it through an encryption key and returns cipher text. If the data needs to be decrypted, the program processes it again with the same key and is able to reproduce the clear text. This method required less computational resources for the program to complete its cipher process, which means lower performance impact.

AES encryption is a good method to protect sensitive data stored in large databases.

AES is fast and works best in closed systems and large databases

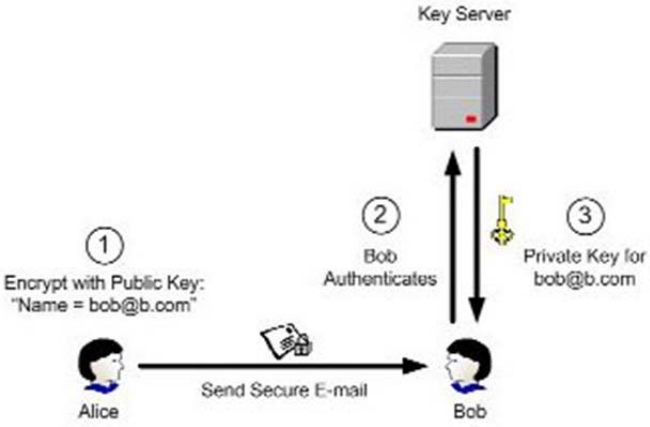


IBE:PEPSI main building block is Identity-Based Encryption (IBE), specifically, the construction given by Meiklejohn [34]. The main advantage in using IBE, as opposed to standard public-key cryptography, is to enable non-interactivity in our protocol design. Participatory sensing scenarios, where MNs and queriers have no direct communication nor mutual knowledge. IBE enables asymmetric encryption using any string ("identity") as a public key. IBE, anyone can derive public keys from some unique information about recipient's Identity-based encryption (IBE)is used as a standard public key cryptography in PS. IBE is a certificate less alternative to public key encryption, allows encrypting messages under textual strings, instead of public keys. Such a string originally refers to the identity of a recipient. Identity-based approach requires the availability of a complete list of all intended recipients. It allows realizing encryption that is partly suitable for one-to many settings, by describing a group by a single textual string. IBE can derive public keys from some unique information about the recipient identity. Private decryption keys are generated by a third -party, called the Private Key Generator.

IBE algorithm consist of four operations:

1. **Setup:** generates global system parameters and a master key.
2. **Extract:** uses the master-key to generate the private key corresponding to an arbitrary public key string.
3. **Encrypt:** encrypts messages using the public key ID.
4. **Decrypt:** decrypts messages using the corresponding private key.

Identity Based Encryption was to simplify certificate management in e-mail systems. When Alice sends mail to Bob at bob@company.com she simply encrypts her message using the public key string "bob@company.com". There is no need for Alice to obtain Bob's public key certificate. When Bob receives the encrypted mail he contacts a third party ,which call the Private Key Generator (PKG). Bob authenticates himself to the PKG in the same way he would authenticate himself to a Centre of Authentication (CA) and obtains his private key from the PKG. Bob can then read his e-mail.



VII. Comparison Between AES And IBE

AES	IBE
1.AES is a symmetric key encryption algorithm, which means that the same key is used for the encryption and decryption of the data.	IBE is a asymmetric key encryption algorithm which used the different key for the encryption and decryption of the data.
2.AES doesnot use the master key generation.	IBE uses the master key generation.
3.It is supports larger key sizes.	It is supports short lived public key and their corresponding private keys.
4. Online.	Online or offline.
5. AES encryption is a good method to store the data in large database.	IBE store the data in small databases.

VIII. Conclusion

Participatory Sensing is a novel computing standard and also tolerate a good potential. It is a technique in which a sensor node can share its information. It is also isolated from the network i.e. a node has privacy in spite of sharing its information with the other nodes of the network. In this paper a review on the PEPSI is done on the various encryption schemes. Identity-based encryption (IBE), which allows encrypting messages under textual strings, instead of public keys and Advance Encryption System that is used to encrypt the sensor data which is to be shared. Such a string originally refers to the identity of a recipient where as AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. So in the end it can be said that both the encryption schemes have their own advantages that can-not be correlated and they have to be used separately in PEPSI architecture.

References

[1] E.S. Cochran, J.F. Lawrence, 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 , A. Kapadia , D. Kotz and D. Peebles , M. Shin and N. Triandopoulos, Anony-Sense: Privacy-aware people-centric sensing, 6th International Conference on Mobile Systems, Applications, and Services (Mobile Sys), 2008, pp. 211-224.

[3] D Cuff , M.H. Hansen and J. Kang, Urban sensing: out of the woods, Commun. ACM, vol. 51, no. 3, 2008, pp. 24-33.
[4] E. De Cristofaro and C. Soriente, Privacy-Preserving Participatory Sensing Infrastructure.
[5] P.T. Eugster , P.A. Felber, 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 , N. Pham ,Y.E. Tsai and T.F. Abdelzaher, PoolView: stream privacy for grassroots participatory sensing, 6th International Conference on Embedded Networked Sensor Systems (SenSys) 2008, pp. 281-294.
[7] P. Gilbert , L.P. Cox , 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 , G. Russello and B. Crispo, Supporting Publication and Subscription Confidentiality in Pub/Sub Networks, 6th International ICST Conference on Security and Privacy in Communication Networks (Secure Comm), 2010, pp. 272-289.
[9] D.H. Kim , J. Hightower , R. Govindan and D. Estrin, Discovering semantically meaningful places from pervasive RF-beacons, 11th International Conference on Ubiquitous Computing (Unicom), 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 , 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 , M. Stevens , 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 , R.J. Honicky and E. Goodman, Sensing Atmosphere, Sensing on Everyday Mobile Phones in Support of Participatory Research (SenSys workshop), 2007, pp. 1-3.