ISSN:0975-9646

A Research for Modified PEPSI Architecture

Shreya Ahuja[#1], Amninder Kaur Gill[*2]

[#1]PURCTIM Mohali
*[*2]PURCTIM Mohali*

***Abstract*— With the proliferation of sensor-embedded mobile computing devices, participatory sensing is becoming popular to collect information from and outsource tasks to participating users. These applications deal with a lot of personal information, e.g., users' identities and locations at a specific time. Therefore, we need to pay a deeper attention to privacy and anonymity. However, from a data consumer's point of view, we want to know the source of the sensing data, i.e., the identity of the sender, in order to evaluate how much the data can be trusted. "Anonymity" and "trust" are two conflicting objectives in participatory sensing networks, and there are no existing research efforts which investigated the possibility of achieving both of them at the same time. 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.**

***Keywords*— Include at least 5 keywords or phrases**

I. Introduction

In recent years, we have seen the massive prevalence of mobile computing devices such as smartphones and tablet 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 largescale applications. Two examples of participatory sensing applications are Gigwalk [1] developed by a startup company and mCrowd [2] developed by University of Massachusetts Amherst. They provide a marketplace for sensing tasks that can be performed from smartphones. 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 smartphones 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 user's identity, personal activities, political views, health status, etc. [3], which poses threats to the participating users. Therefore, participatory sensing requires a deeper attention to privacy and anonymity, and 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, hence 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 everyday. 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 imagers, 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. Our mobile phones are the sensing infrastructure and the number and variety of applications are potentially unlimited. Users can monitor gas prices (http://www.gasbuddy.com/), traffic information (http://www.waze.com/), available parking spots (http://spotswitch.com/), just to cite a few. We refer readers to [4] for an updated list of papers and projects related to PS. What isn't Participatory Sensing? 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. They are extremely mobile, as they leverage the ambulation of their carriers. Moreover, in traditional WSNs, 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. Hence, a sensor (or its owner) might choose whether to participate or not. As a result, in PS applications, different entities co-exist and might not trust each other. Participatory Sensing Components. A typical PS infrastructure involves (at least) the following parties:

1. 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.
2. Queriers subscribe to information collected in a PS application (e.g., “temperature in Irvine, CA”) and obtain corresponding reports.
3. Network Operators manage the network used to collect and deliver sensor measurements , e.g., they maintain GSM and/or 3G/4G networks.
4. Service Providers act as intermediaries between Queriers and Mobile Nodes, in order to deliver report of interest to Queriers. Queriers can subscribe to the appropriate Service Provider for one or more type of measurements.

For example, assume that Alice subscribes to “available parking spots on W 16th Street, New York”, or Bob is interested in the “temperature in Central Park, New York”. In turn, Mobile Nodes share local knowledge either voluntary or in return for some profit—with one or more Service Providers, that make information available to Queriers. For example, assume Carol’ mobile phone sends report “3 available parking spots on E 56th, New York”, while John’s device sends “74oF in Central Park, New York”. As Mobile Nodes and Queriers have no direct communication nor mutual knowledge, Service Providers route reports matching specific subscriptions to their original Queriers. In fact, Mobile Nodes ignore which Queriers (if any) are interested in their reports. For example, the Service Provider forwards John’s temperature report to Bob; Carol’s parking report is not sent to Alice as it refers to a different location.

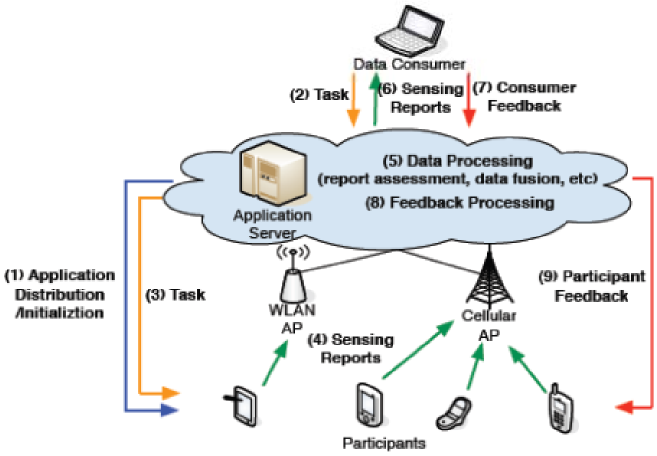

Fig. 1: Architecture of a participatory sensing system

III. ARCHITECTURE

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.

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.

Privacy Desiderata: The privacy desiderata of PS applications can be formalized as follows:

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. Also, 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 Unlinkability: No entity can successfully link two or more reports as originating from the same Mobile Node. However, as we discuss below, we do not pursue Report Unlinkability with respect to the Network Operator.

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 Unlinkability and Location Privacy with respect to the Network Operator. In fact, PS strongly relies on the increasing use of broadband 3G/4G connectivity. In these networks, current technology does not allow to provide user anonymity with respect to the Network Operator. Mobile Nodes are identified through their International Mobile Subscriber Identity, and any technique for identifier obfuscation would lead to service disruption (e.g., the device would not receive incoming calls). Further, the regular usage of cellular networks (e.g., incoming/outgoing phone calls), as well as heartbeat messages exchanged with the network infrastructure, irremediably reveal device’s location. To provide Report Unlinkability/Location Privacy with respect to other parties, we need to trust the Network Operator (who routes Mobile Nodes' reports to Service Providers) not to forward any information identifying the Mobile Nodes (e.g., the identifier, the cell from which the report was originated, etc.).

IV. OPERATIONS

Figure 2 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 NodeM(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.

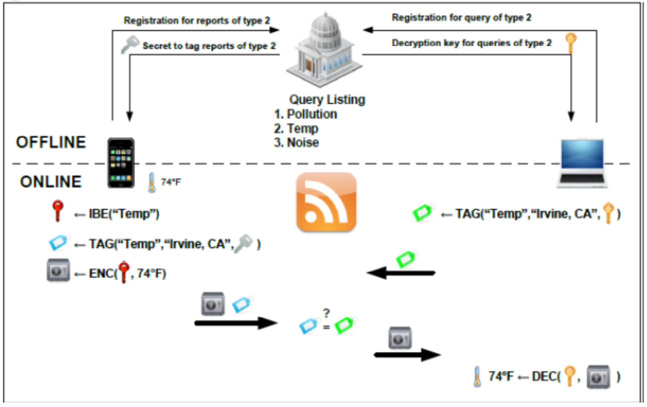
Registration for reports of type 2
Secret to tag reports of type 2
Registration for query of type 2
Decryption key for queries of type 2
Query Listing
1. Pollution
2. Temp
3. Noise
OFFLINE
ONLINE
74°F
← IBE("Temp")
← TAG("Temp","Irvine, CA",)
← ENC(, 74°F)
← TAG("Temp","Irvine, CA",)
?
=
74°F ← DEC(,)

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's interest and is uploaded at the Service Provider. Data Report. Any timeMwants 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. Malso tags the report using the secret acquired offline and a list of keywords characterizing the report; in the exampleMuses keywords "Temp" and "Irvine, CA". Our tagging mechanism leverages the properties of bilinear maps to make sure that, ifMand 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.

V. PROPOSED APPROACH

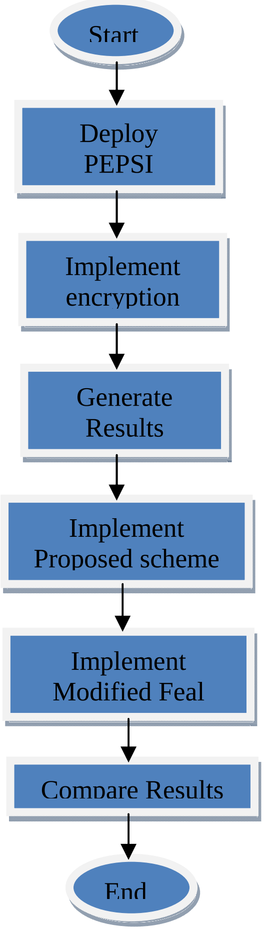

Figure 3: Flow Chart for implementation

VI. RESULTS AND DISCUSSION

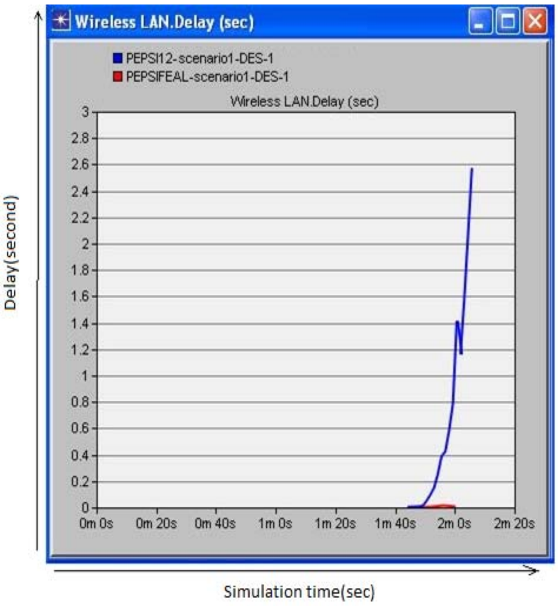

Figure 3: Delay

Figure 3 defined about the delay possessed by the existing and proposed approach. Proposed approach has much lesser delay than that of AES.

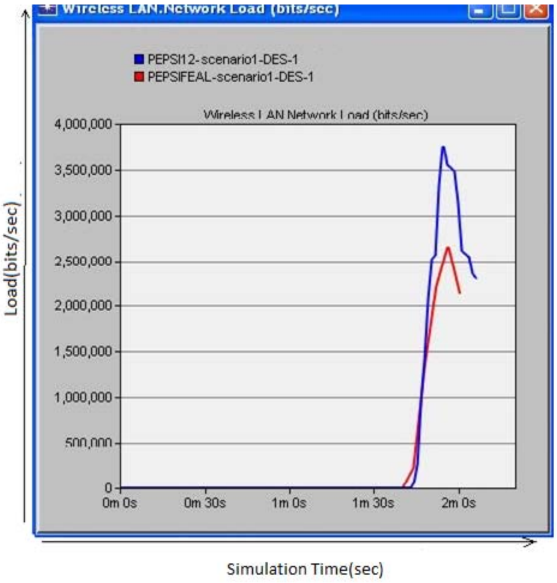

Figure 4: Load

Load defined in figure 4 is quite better in case of FEAL as compared to the AES.

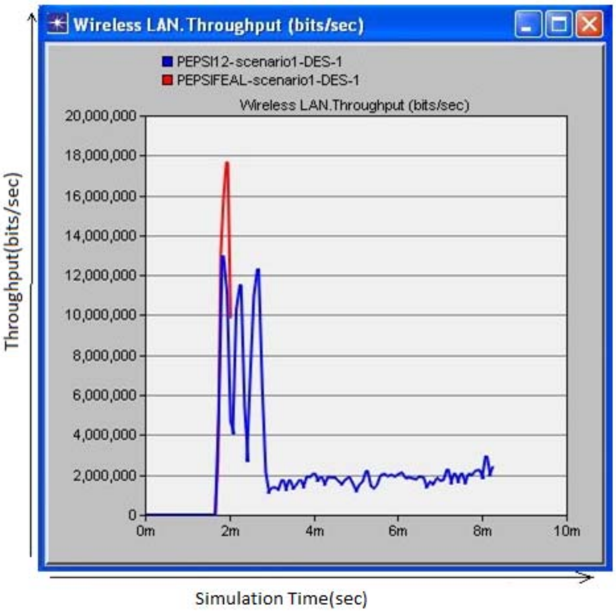

Figure 5: Throughput

Throughput in the proposed approach is higher than that of existing approach.

VII. 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 article 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.

REFERENCES

[1] E.S. Cochran and J.F. Lawrence and C. Christensen and R.S. Jakka, The QuakeCatcher 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. 211-224.

[3] D Cuff and 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, 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, PoolView: 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 (HotMobile), 2010, pp. 31-36.

[8] M. Ion and 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 (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 (UbiComp), 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.