Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Modified Encryption Scheme in PEPSI Architecture to Prevent Collusion

Er. Ravinder Singh, Er. Varinderjit Kaur
Ramgarhia Institute of Engineering & Technology,
Phagwara, Punjab, India

Abstract— With the proliferation of sensor-embedded mobile computing devices, democratic sensing is changing into common to gather data from and source tasks to taking part users. These applications take care of lots of non-public data, e.g., users' identities and locations at a particular time. Therefore, we'd like to pay a deeper attention to privacy and namelessness. However, from an information consumer's purpose of read, we wish to understand the supply of the sensing information, i.e., the identity of the sender, so as to judge what quantity the info is trusty. "Anonymity" and "trust" area unit 2 conflicting objectives in democratic sensing networks, and there aren't any existing analysis efforts that investigated the chance of achieving each of them at constant time. specialise in privacy protection in democratic Sensing and introduce an appropriate privacy-enhanced infrastructure. First, we offer a group of definitions of privacy necessities for each information producers (i.e., users providing detected information) and customers.

Keywords— Include at least 5 keywords or phrases

I. INTRODUCTION

In recent years, we've seen the large prevalence of mobile computing devices like smartphones and pill computers. These devices sometimes go along with multiple embedded sensors, like camera, microphone, GPS, measuring system, digital compass and gyro. attributable to these advancements, the democratic sensing model is changing into in style. Participants use their personal mobile devices to collect knowledge concerning near setting and build them out there for largescale applications. 2 samples of democratic sensing applications area unit Gigwalk [1] developed by a startup company and mCrowd [2] developed by University of Massachusetts Amherst. they supply a marketplace for sensing tasks that may be performed from smartphones. A requester of information will produce tasks that uses the final public to capture geo-tagged pictures, videos, audio snippets, or fill out surveys. Participants UN agency have put in the consumer apps on their smartphones will submit their knowledge and acquire rewarded. for instance, Microsoft Bing has been grouping photos mistreatment Gigwalk for bird's-eye 3-D chemical change of companies and restaurants in Bing Map. Sharing perceived knowledge labeled with spatio-temporal info may reveal lots of non-public info, like a user's identity, personal activities, dogmas, health standing, etc. [3], that poses threats to the taking part users. Therefore, democratic sensing needs a deeper attention to privacy and obscurity, and a mechanism to preserve users' location privacy and obscurity is obligatory. Another dimension {of knowledge|of knowledge|of information} security in democratic sensing is that the dependability of the perceived data. In democratic sensing applications, knowledge originates from sensors controlled by people, associated any participant with an fittingly organized device will simply submit falsified knowledge, thus knowledge trait becomes a lot of crucial than the normal wireless detector networks. there's associate inherent conflict between trust and privacy. If a democratic sensing system provides full obscurity to the participants, it's troublesome to ensure the trait of submitted knowledge. Finding an answer that achieves each trust and obscurity may be a major challenge in such systems [4]. The proliferation of mobile phones, at the side of their pervasive property, has propelled the number of digital knowledge created and processed everyday. This has driven researchers and IT professionals to debate and develop a unique sensing paradigm, wherever sensors don't seem to be deployed in specific locations, however area unit carried around by individuals. Today, many various sensors area unit already deployed in our mobile phones, and shortly all our gadgets (e.g., even our garments or cars) can plant a mess of sensors (e.g., GPS, digital imagers, accelerometers, etc.). As a result, knowledge collected by sensor-equipped devices becomes of utmost interest to alternative users and applications. as an example, mobile phones might report (in real-time) temperature or noise level; equally, cars might inform on traffic conditions. This paradigm is named democratic Sensing (PS) – generally additionally named as opportunist or urban sensing [3]. It combines the omnipresence of non-public devices with sensing capabilities typical of WSN.

II. PARTICIPATORY SENSING

PS is associate rising paradigm that focuses on the seamless assortment of knowledge from an oversized range of connected, always-on, always-carried devices, like mobile phones. notation leverages the wide proliferation of trade goods sensor-equipped devices and therefore the presence of broadband network infrastructure to produce sensing

applications wherever readying of a WSN infrastructure isn't economical or not possible. notation provides fine-grained observance of environmental trends while not the necessity to line up a sensing infrastructure. Our mobile phones square measure the sensing infrastructure and therefore the range and kind of applications square measure doubtless unlimited. Users will monitor gas costs (http://www.gasbuddy.com/), traffic data (http://www.waze.com/), accessible parking spots (http://spotswitch.com/), simply to cite a couple of. we have a tendency to refer readers to [4] for associate updated list of papers and comes associated with notation. What isn't democratic Sensing? notation isn't a mere evolution of WSN, wherever motes square measure replaced by mobile phones. Sensors square measure currently comparatively powerful devices, like mobile phones, with abundant larger resources than WSN motes. Their batteries may be simply recharged and cost constraints aren't as tight. they're extraordinarily mobile, as they leverage the walk of their carriers. Moreover, in ancient WSNs, the network operator is usually assumed to manage and own the sensors. On the contrary, this assumption doesn't match most notation eventualities, wherever mobile devices square measure tasked to participate into gathering and sharing native information. Hence, a detector (or its owner) would possibly select whether or not to participate or not. As a result, in notation applications, totally different entities co-exist and may not trust one another. democratic Sensing parts. A typical notation infrastructure involves (at least) the subsequent parties:

1. Mobile Nodes square measure the union of a carrier (i.e., a user) with a detector put in on a movable or different transportable, wireless-enabled device. they supply reports and kind the idea of any notation application.
2. Queriers take data collected in an exceedingly notation application (e.g., "temperature in Irvine, CA") and acquire corresponding reports.
3. Network Operators manage the network accustomed collect and deliver detector measurements , e.g., they maintain GSM and/or 3G/4G networks.
4. Service suppliers act as intermediaries between Queriers and Mobile Nodes, so as to deliver report of interest to Queriers. Queriers will take the suitable Service supplier for one or a lot of sort of measurements.

For example, assume that Alice subscribes to "available parking spots on W sixteenth Street, New York", or Bob is inquisitive about the "temperature in common, New York". In turn, Mobile Nodes share native information either voluntary or reciprocally for a few profit—with one or a lot of Service suppliers, that create data accessible to Queriers. as an example, assume Carol' movable sends report "3 accessible parking spots on E 56th, New York", whereas John's device sends "74oF in common, New York". As Mobile Nodes and Queriers haven't any direct communication nor mutual information, 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. as an example, the Service supplier forwards John's temperature report back to Bob; Carol's parking report isn't sent to Alice because it refers to a distinct location.

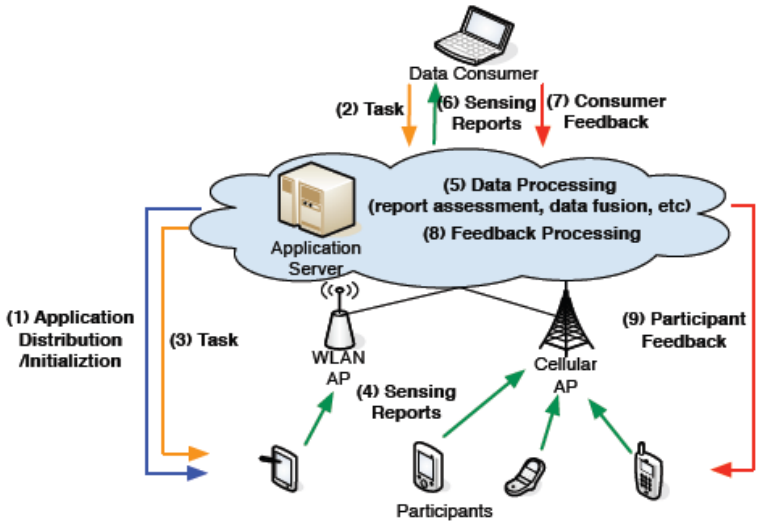

Fig. 1: Architecture of a participatory sensing system

III. ARCHITECTURE

PEPSI protects privacy victimization economical cryptanalytic tools. kind of like alternative cryptanalytic solutions, it introduces an extra (offline) entity, specifically the Registration Authority. It sets up system parameters and manages Mobile Nodes or Queriers registration. However, the Registration Authority isn't concerned in time period operations (e.g., query/report matching) neither is it trustworthy to intervene for safeguarding participants' privacy.

Figure one illustrates the Pepsi design. The Registration Authority will be instantiated by any entity accountable of managing participants registration (e.g., a phone manufacturer). A Service supplier offers PS applications (used, as an example, to report associated access pollution data) and acts as an intermediator between Queriers and Mobile Nodes. Finally, Mobile Nodes send measurements noninheritable via their sensors victimization the network infrastructure and Queriers area unit users or organizations (e.g., bikers) curious about getting reports (e.g., pollution levels).

PEPSI permits the Service supplier to perform report/query matching whereas guaranteeing the privacy of each mobile Nodes and Queriers. It aims at providing (provable) privacy intentionally, and starts off with shaping a transparent set of privacy properties.

Privacy Desiderata: The privacy desiderata of PS applications will be formalized as follows:
Soundness: Upon subscribing to a question, Queriers in possession of the acceptable authorization forever get the required question results.
Node Privacy: Neither the Network Operator, the Service supplier, nor any unauthorized inquirer, learn any data concerning the kind of activity or the info reported by a Mobile Node. Also, Mobile Nodes shouldn't learn any data concerning alternative nodes' reports. solely Queriers in possession of the corresponding authorization get reported measurements.
Query Privacy: Neither the Network Operator, the Service supplier, nor any Mobile Node or the other inquirer, learn any data concerning Queriers' subscriptions.
Report Unlinkability: No entity will with success link 2 or additional reports as originating from identical Mobile Node. However, as we have a tendency to discuss below, we have a tendency to don't pursue Report Unlinkability with relation to the Network Operator.
Location Privacy: No entity will learn the present location of a Mobile Node. (Again, excluding the Network Operator). In realistic eventualities, it seems unlikely – if not not possible – to ensure Report Unlinkability and placement Privacy with relation to the Network Operator. In fact, PS powerfully depends on the increasing use of broadband 3G/4G property. In these networks, current technology doesn't permit to produce user obscurity with relation to the Network Operator. Mobile Nodes area unit known through their International Mobile Subscriber Identity, and any technique for symbol obfuscation would result in service disruption (e.g., the device wouldn't receive incoming calls). Further, the regular usage of cellular networks (e.g., incoming/outgoing phone calls), likewise as heartbeat messages changed with the network infrastructure, irremediably reveal device's location. to produce Report Unlinkability/Location Privacy with relation to other parties, we'd like to trust the Network Operator (who routes Mobile Nodes' reports to Service Providers) to not forward any data characteristic the Mobile Nodes (e.g., the symbol, the cell from that 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.

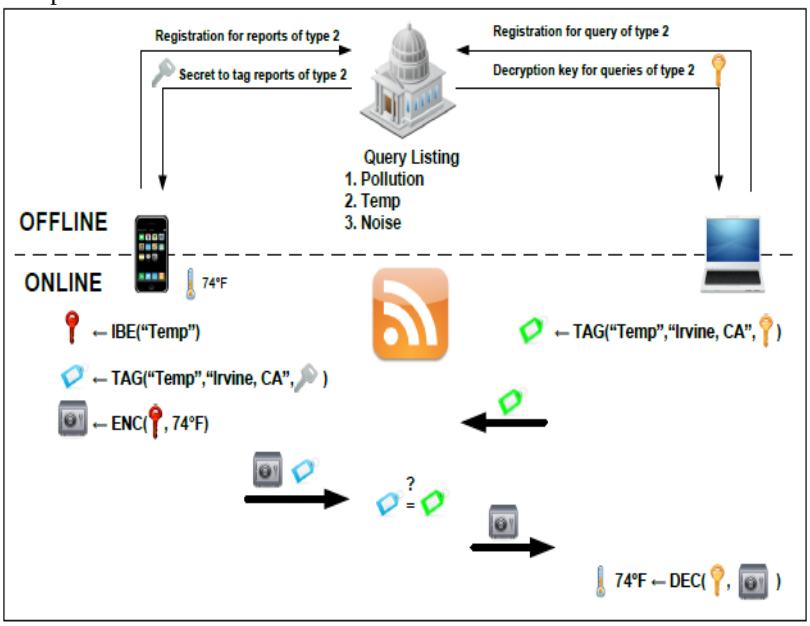

Figure 2: PEPSI operations.

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

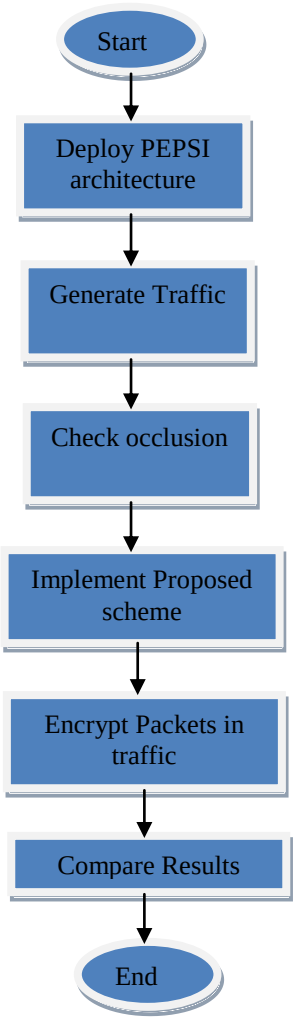

Figure 3: Flow Chart for implementation

VI. RESULTS AND DISCUSSION

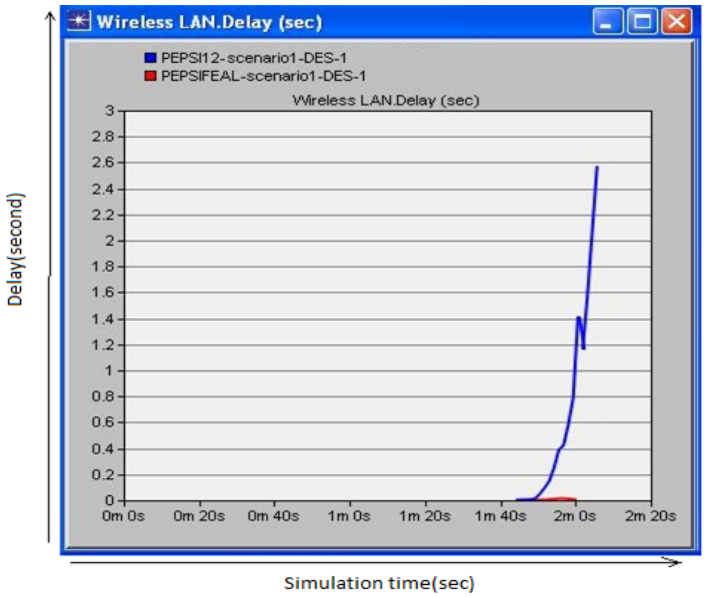

Figure 3: Delay

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

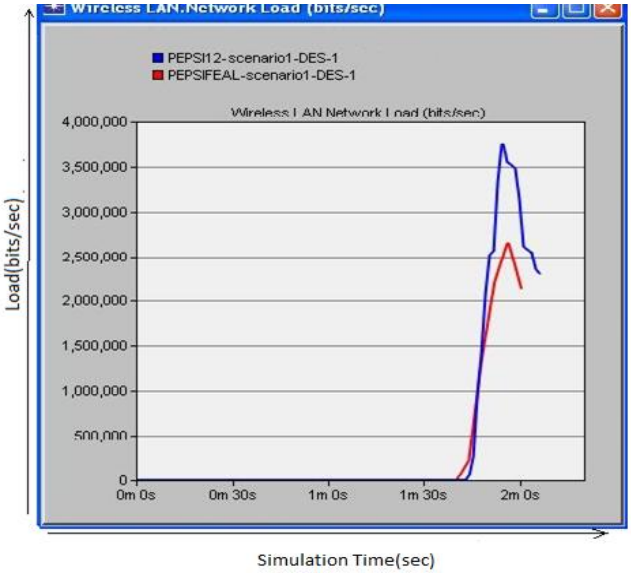

Figure 4: Load

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

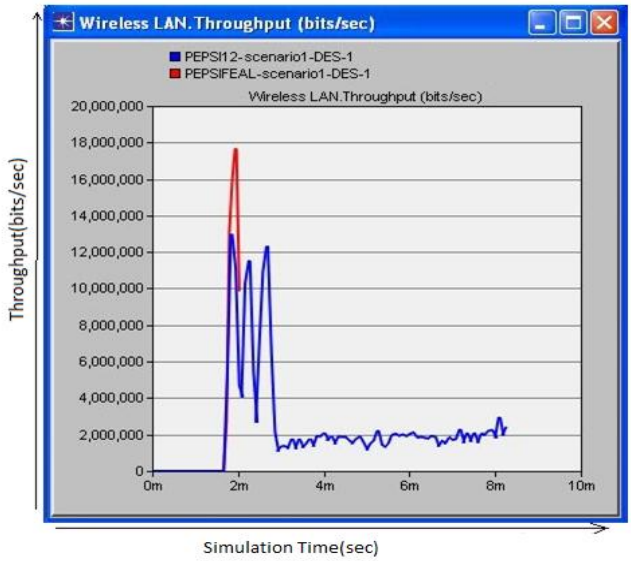

Figure 5: Throughput

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 Iternational 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.

