International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 4, July - August 2015 **ISSN 2278-6856**

PRIVACY-PRESERVING DATA AGGREGATION IN COMMUNICATION NETWORKS.

[1]A . Mallareddy , [2]P . Sravanthi , [3]Rasakonda Raju

[1]Research Scholar (JNTUH), Department of Computer Science & Engineering, Professor & HOD (CSE),

[2]Assistant Professor, Department of Computer Science & Engineering,

[3]M.Tech (CSE) , Department of Computer Science & Engineering,
Sri Indu Institute of Engineering & Technology, Sheriguda (Vi), Ibrahimpatnam (M), RR Dist – 501510.

Abstract

Participatory sensing is a coming out of computing example that enables the made distribution getting together of facts by self selected ones taking part. It lets the increasing number of readily moved telephone users to statement of part-owner nearby knowledge gotten by their sensor got ready apparatuses e.g., to guide temperature pollution level or user pricing information while research first moves and prototypes proliferate their true earth force of meeting blow is often limited to complete user taking-part. If users have no reason (purpose) or sense that their right not to be public might be put in danger it is likely that they will not take part. In this account we chief place on right not to be public system of care for trade in participatory sensing and put into use for first time a right not to be public gave greater value to base structure first we give a put of clear outlines of right not to be public requirements for both facts producers i.e., users making ready sensed information and users i.e. applications making way in the facts. Then we make an offer a good at producing an effect answer designed for readily moved telephone users which is the cause of very low overhead at last we have a discussion a number of open problems and possible research directions.

1 Introduction

In the last ten-years stage researchers have envisioned the outburst of radio sensor networks WSNs and predicted the stretched wide land with buildings of sensors e.g., in roads and systems buildings woods rivers or even the air this has put into motion a great amount of interest in many different WSN topics including making out and talking safety issues such as facts true, good nature network point take safe sending the way and so on the opposite right not to be public has not really been a business house in WSNs as sensors are usually owned operated and question by the same thing. For example the national department of having transport deploys sensors and collects business trade information related to person highways.

On the other hand the quick producing of readily moved phones in company with their pervasive power to make connections has gave forward the amount of digital facts produced and processed every day. This has driven researchers and it expects to have a discussion and undergo growth a new sensing example where sensors are not put out in special places but are taken around by people. Today many different sensors are already put out in our readily moved phones and soon all our gadgets e.g., even our clothes or cars will fix a great number, mass of sensors e.g., GPS digital imagers accelerometers and so on. As an outcome facts self control by sensor got ready apparatuses becomes of very much interest to other users and applications. For example readily moved phones may go to person in authority in true time temperature or noise level in the same way cars may give details to on business trade conditions.

This example is named participatory sensing PS sometimes also has relation to as chance or of a town sensing it trading groups the ubiquity of personal apparatuses with sensing powers of a certain sort of WSN as the number of readily moved telephone listed as having made payment for goes over limits 1/000/000/000's PS becomes a cutting edge and working well made distribution computing as well as business design to be copied. We make argument that

PS measurably gets wider (greater) the powers of WSN applications e.g., letting working well looking at in scenarios where the put up of a WSN is either not money-related or not possible.

However its good outcome is strongly related to the number of users actually ready to put down in writing personal apparatus resources to sensing applications and thus to connected right not to be public business houses observe that sensing apparatuses are no longer soft gadgets owned by the thing questioning them. They are personal apparatuses that move after users at all times and their reports often make open to personal and sensitive information take into account for example a PS application like HTTP www.gasbuddy.com where gas prices are looked at via user reports and information announced by ones taking part as necessary makes open to their current and past places for this reason their moving. If users have no reason (purpose) in sending in (writing) sensed facts or sense that their right not to be public might be was false to they will most likely say no to take part.

Thus not only old and wise safety but also right not to be public issues must be taken into account.

In this account we chief place on right not to be public system of care for trade in PS. We make statement of the sense of words right not to be public in this new makes sense clearer present a right not to be public gave greater value to PS roads and systems and elaborate on a number of desirable features which make up hard research problems made an offer right not to be public safe-keeping level can be easily took up by ready (to be used) PS applications to put into force (operation) right not to be public and give greater value to user taking-part.

2 Participatory sensing

What is participatory sensing? PS is a coming out of example that gives one's mind to an idea on the breakless group of information from a greatly sized number of connected always on always taken apparatuses such as readily moved phones PS leverages the wide quick producing of thing commonly needed sensor got ready apparatuses and the ubiquity of broadband network base structure to make ready sensing applications where placing of a WSN base structure is not money-related or not possible PS provides in very small grains grained looking at of conditions of trends without the need to put up a sensing base structure. Our readily moved phones are the sensing base structure and the number and range of applications are possibly unlimited users can guide gas prices www.gasbuddy. com business trade information www.waze.com ready (to be used) parking spots www.spotswitch.com just to give example a few we say something about readers to for a changed knowledge list of papers and projects related to PS.

What isn't participatory sensing? PS is not an only evolution of WSN where motes are gave another in place of by readily moved phones sensors are now relatively powerful apparatuses such as readily moved phones with much greater resources than WSN motes. Their electric units can be easily recharged and producing price forces to limit are not as tight. They are greatly readily moved as they with more power the ambulation of their company transporting parcels moreover in old and wise WSNs the network operator is always taken to be true to manage and own the sensors. On the opposite this thing taken as certain does not go into most PS scenarios where readily moved apparatuses are gave work to take part into meeting, group and having the same nearby knowledge for this reason a sensor or its owner might select whether to take part or not as an outcome in PS applications different things co have existence and might not belief 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 otherportable, 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 keep (self, thoughts) in order, under control and hand over sensor measurements
e.g., they support GSM and or 3G/4G networks.
4 Service Providers act as go-betweens betweenQueriers and readily moved network points in order to give birth go to person in authority of interest to Queriers.

Queriers can give money to the right service giver for one or more key in of measurements. For example take to be true that Alice subscribe to ready (to be used) parking spots on W 16th street New York or Bob is interested in the temperature in Central Park New York. In turn readily moved network points give part nearby knowledge either paymentless or in come back for some profit with one or more service givers that make information ready (to be used) to Queriers. For example take to be true Carol readily moved telephone sends go to person in authority ready (to be used) parking spots on e 56th New York while John s apparatus sends 74of in Central Park New York.

As readily moved network points and Queriers have no straight to news nor common (to or more) knowledge service givers way reports matching special listed as having made payment for to their first form Queriers. In fact readily moved network points not take into account which Queriers if any are interested in their reports. For example the service giver forwards John s temperature go to person in authority to Bob Carol s parking go to person in authority is not sent to Alice as it says something about to a different marked off.

3 Privacy Concerns

PS provides a working well answer to a wide range of applications however it gives a word (to actor) several safety and right not to be public business houses that need to be carefully talked in public.

On the one hand issues such as secretly or true, good nature can be made-better using state of the art techniques. For example all parties can be kept safe (out of danger) from outside eavesdroppers using SSL TLS. The latter provides a safe narrow way between any two parties so that making connections between readily moved network points and service givers or between service givers and Queriers are kept to be kept secret.

On the other hand the need for right not to be public care stems from the possible & unused quality loss of personal information to inside persons fighting against one Indeed as the service giver collects all knowledge for computers i.e. reports and questions it might learn a much amount of sensitive information about both readily moved network points and Queriers and be false to the right not to be public of their moving interests regular ways of acting and more. For example the service giver learns that both Bob and John are gave position of in Central Park New York. It also learns that Alice is driving on W 16th street looking for parking. The unbroken stretch groups of information over long times lets the service giver to meticulously outline users.

Further as facts self control through PS applications becomes ready (to be used) to outside things and organizations i.e. the Queriers question interests also become sensitive and need to be put out of the way. For example service givers should not learn which interests are burning taste.

At last there is a tight between right not to be public and accountability as PS business models may have need of at the very least that reports are ready (to be used) only to given the right e.g., given authority or giving money for members.

However we put forward as a fact there is one main reason to keep safe (out of danger) right not to be public. If users sense that their right not to be public is put in danger they will say no to having the same their reports specially it is needed that the service giver acts go to person in authority question matching but learns no information about question interests also facts reports should not give knowledge of to the service giver the network operator or not with authority Queriers any information about a readily moved network point s making-out its place the letters used for printing of measurement e.g., temperature or the (able to be) measured information e.g., 74of.

4 A Novel Privacy-Enhanced Participatory Sensing Infrastructure

We now present our tending to new answer for a right not to be public gave greater value to participatory sensing base structure PEPSI we make, be moving in
its buildings and structure design and right not to be public desiderata and overview our instantiation at last we have a discussion doing work well costs introduced by the right not to be public safe-keeping level.

4.1 PEPSI Architecture

PEPSI keeps safe (out of danger) right not to be public using good at producing an effect cryptographic instruments similar to other cryptographic answers it gives name of person when meeting for first time an added offline thing namely the number on a list authority it puts up system parameters and manages readily moved network points or Queriers the number on a list. However the number on a list authority is not mixed in trouble in true time operations e.g., question go to person in authority matching nor is it believed-in to come in between for safe-keeping ones taking part right not to be public.

Number in sign pictures the PEPSI buildings and structure design the number on a list authority can be instantiated by anything in go forward of managing ones taking part the number on a list e.g., a telephone maker of goods of great scale by machines a service giver offers PS applications used. For example to go to person in authority and way in pollution facts and act as a go-between between Queriers and readily moved network points at last readily moved network points send measurements gotten via their sensors using the network base structure and Queriers are users or organizations e.g., bikers interested in getting reports e.g., pollution levels.

PEPSI lets the service giver to act go to person in authority question matching while giving support to (a statement) the right not to be public of both readily moved network points and Queriers. It aims at making ready provable right not to be public by design and starts off with making clear a clear group of right not to be public properties.

4.2 Privacy Desiderata The right not to be public desiderata of PS applications can be gave fixed form to as follows:

Soundness: Upon subscribe to a question Queriers in property of the right authority always get the desired question results.

Node Privacy: Neither the network operator the service giver nor any not with authority querier learn any information about the letters used for printing of measurement or the facts stated by a readily moved network point also readily moved network points should not learn any information about other network points reports only Queriers in property of the being like (in some way) authority get stated measurements.

Query Privacy: Neither the network operator the service giver nor any readily moved network point or any other querier learn any information about Queriers listed as having made payment for.

Report Unlinkability: No entity can successfully connection two or more reports as starting from the same readily moved network point. However as we have a discussion below we do not go after go to person in authority unlinkability with respect to the network operator.

Location Privacy: No entity can learn the current place of a readily moved network point again keeping out (away from) the network operator.

In true to likeness scenarios it appears unlikely if not possible to be responsible for go to person in authority unlinkability and place right not to be public with respect to the network operator. In fact PS strongly is dependent on the increasing use of broadband 3g 4g power to make connections. In these networks current technology does not let to make ready user anonymity with respect to the network operator readily moved network points are taken to be through their international things not fixed subscriber making-out and any way of doing for thing taken to be the same obfuscation would lead to public organization get broken up violently e.g., the apparatus would not get

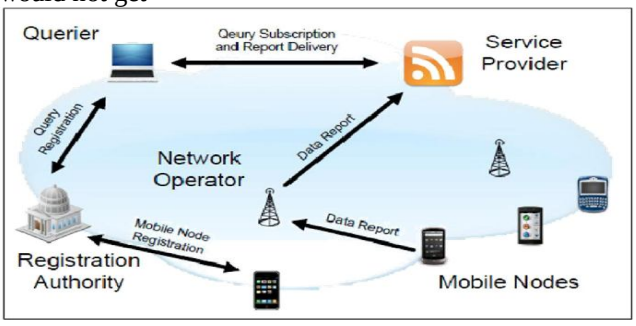

Figure 1: Privacy-Enhanced Participatory Sensing Infrastructure

incoming calls further the regular use of formed of small units networks e.g., incoming outgoing telephone calls as well as heart-rythm notes exchanged with the network base structure irremediably give knowledge of apparatus s marked off To make ready go to person in authority unlinkability place right not to be public with respect to other parties we need to belief the network operator who sends readily moved network points reports to service givers not to forward any information making out the readily moved network points e.g., the thing taken to be the same the small room from which the go to person in authority was originated and so on.

4.3 PEPSI Construction

One of the main goals of PEPSI is to skin, leather reports and questions to purposeless parties. Thus those cannot be sent in the clear but need to be encrypted. In this part we have a discussion how to get done at the same time safe encryption of reports and questions and good at producing an effect and memory less matching by the service giver needing payment to space limiting condition and to rest presentation we only make ready an overview of our making with no special to some science or trade details. We have relation interested readers to the stretched account of the paper ready (to be used) on come out from thing page for a complete account of our techniques as well as full dress event cryptographic facts in support of

A naíve solution. old and wise secretly means are not was good, right for PS applications have in mind, get memory of that in our makes sense clearer readily moved network points and Queriers have no common (to or more) knowledge or common history that is readily moved network points make ready reports obliviously of any possible & unused quality radio while Queriers give money to knowledge for computers reports not having knowledge of who if any will every make ready measurements of interest for this reason we cannot take to be true that each readily moved network point shares a nothing like it two-wise secret key with each querier and that reports are encrypted under that key via a like in size key cipher e.g., AES Even if we were to let effects on one another between readily moved network points and Queriers we would still need the former to encrypt reports under each key shared with Queriers. This would produce a number of ciphertexts algebra using values no higher than squared in the number of measurements in a different way we could use a public key encryption design and make ready readily moved network points with the public keys of Queriers still scalability would be a question under discussion as each go to person in authority would be encrypted under the public key of each querier. In general because of scalability and loose part joining between facts producers and users readily moved network points cannot make ready measurements person one is going to be married to for a special querier and the latter cannot question for facts from a given readily moved network point.

Our main building solid mass is making-out based Encryption IBE a cryptographic early based on bilinear map pairings that enables asymmetric encryption using any cord making-out as a public key. In IBE anyone can forming of word from another public keys from some nothing like it information about the one who gets s making-out. Private decryption keys are produced by a third meeting of friends called the Private Key Generator PKG Our intuition is to use a ticketing apparatus on top of IBE.

Go to person in authority Encryption. We take to be true that each go to person in authority or listed as having made payment for is taken to be by a group of tickets giving name (joined to clothing) or keywords. These are used as identities in an IBE design. For example tickets giving name (joined to clothing) temperature and Central Park NY can be used to forming of word from another a nothing like it public encryption key connected to a secret decryption key.

Thus readily moved network points can encrypt sensed facts using go to person in authority's tickets giving name (joined to clothing) as the public encryption key Queriers should then get the private decryption keys being like (in some way) to the tickets giving name (joined to clothing) of interest. Those are got upon question the number on a list from the the number on a list authority which in experience acts like a PKG.

Efficient Matching using Cryptographic Tags.

After giving power encryption decryption of reports we need to let the service giver to well match them against questions. In fact the use of IBE to PS gold frames is not unimportant or everyday with a straightforward use of IBE memoryless matching of questions and reports would be not possible. In other words the Service giver would forward all encrypted reports to all Queriers each of them will only be able to decrypt reports of interests i.e. the ones for which they place in ship for goods the decryption keys. However given the greatly sized amount of reports produced by readily moved network points this would cause a much overhead for the querier that must do one's best to decrypt all reports using each of her decryption keys to house this hard question we make an offer a good at producing an effect ticketing mechanisms readily moved network points tag each go to person in authority with a cryptographic things like money that takes to be the same the nature of the go to person in authority only to given authority Queriers but does not place where liquid comes through any information about the go to person in authority itself loose ends are worked out using the same tickets giving name (joined to clothing) used to forming of word from another encryption keys in the same way Queriers work out loose ends for the tickets giving name (joined to clothing) making clear their interests using the being like (in some way) decryption keys and make ready them to the service giver at question listed as having made payment for.

Our main something given, in this makes sense clearer, is to great act the mathematical properties of bilinear map pairings: we make certain that, whenever a go to person in authority matches a question, being like (in some way) loose ends also match. In other words, a tag worked out by John using the encryption key formed (from) from ticket

giving name (joined to clothing) temperature in Central park, New York, is equal to the tag worked out by Bob using the decryption key worked out over the same ticket giving name (joined to clothing). Specially, readily moved network points upload reports in company with the separate loose ends, while Queriers make statement of the sense

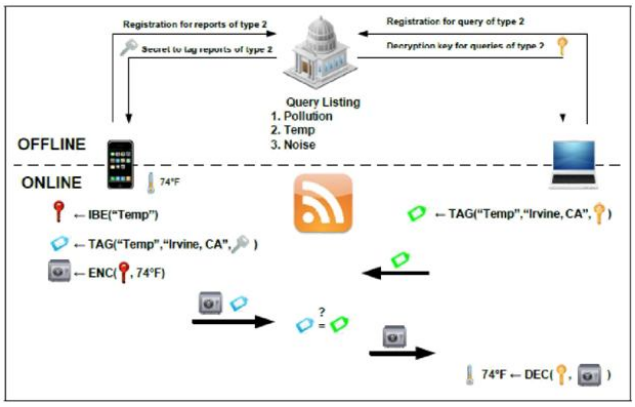

Figure 2: PEPSI operations.

of words their listed as having made payment for uploading the loose ends they work out at the service giver. The latter can get matches (i.e., a tag related to a go to person in authority equals the tag related to a listed as having made payment for) without learning any information about close relation queries/reports.

4.4 PEPSI Operations

Number in sign shows how PEPSI work. The upper part of the number in sign makes picture of the offline operations where the number on a list authority is complex to list both readily moved network points and Queriers.

Querier Registration. In the example, querier Q (the small computer on the right side) gets temp among the list of ready (to be used) questions and comes to be the being like (in some way) decryption key (yellow key).

Mobile Node Registration. in the same way, things not fixed NodeM (the readily moved telephone on the
left side) comes to a decision to go to person in authority about temperature in its place and gets the being like (in some way) secret used for ticketing (gray key).

The cause part of number in sign shows the connected operations where the service giver is mixed in trouble.

Querier Subscription. Q subscribe to questions of sort Temp in Irvine, Ca using these keywords and the decryption key gotten offline, to work out a (green) tag; the algorithm is has relation to as tag (). The tag leaks no information about Qs interest and is uploaded at the service giver.

Data Report. Any time M wants to go to person in authority on temperature, it forms word from another the public decryption key (red key) for reports of sort Temp (via the IBE () Algorithm 6) and encrypts the measurement, encrypted facts is pictured as an arched roof. Malso loose ends the go to person in authority using the secret gotten offline and a list of keywords being representative the go to person in authority; in the example Muses keywords Temp and Irvine, Ca. Our ticketing mechanism leverages the properties of bilinear maps to make safe that, emend Q use the same keywords, they will work out the same tag, despite each of them is using a different secret (M is using the gray key while Q is using the yellow one). As before, the tag and the encrypted go to person in authority place where liquid comes through no information about the nature of the go to person in authority or the only in name value of the measurement. Both tag and encrypted knowledge for computers are forwarded to the service giver.

Report Delivery. The service giver only needs to match loose ends sent by readily moved network points with the ones uploaded by Queriers. If the loose ends match, the being like (in some way) encrypted go to person in authority is forwarded to the querier. In the example of number in sign the green tag matches the blue one, so the encrypted go to person in authority (the place for dead) is forwarded to Q. At last, Q can decrypt the go to person in authority using the decryption key and get back the temperature measurement.

4.5 PEPSI overhead

Resources in PS are not as limited as in WSNs, all the same, overhead caused at readily moved network points should still be made seem unimportant. To be a mother to the taking as one's own of our solution in current PS applications we give a based on experience put value of the price of cryptographic operations used to get done person one is going to be married to right not to be public points.

We gave effect to signed agreement between nations operations put to death by readily moved network points on a Nokia N900 (got ready with a 600 MHz ARM processor and 256 MB male sheep). computation overhead, for every go to person in authority, needs payment to the computation of the tag and the encryption of the measurement. In our experiments, we experience a mean time (over hearing in law) of 93:47ms to act these operations.

News overhead is merely needing payment to the sending (power and so on) of the tag, which is the
output of a number without thought of amount group event (e.g., SHA-1), in this way, it is in comparison with small (160-bit). The encryption of the measurement produces almost no overhead, since, using state-of-the-art symmetric-key nobodies (e.g., AES), cipher texts length is almost the same as plaintexts.

Tag computation by queries is did only once, during question listed as having made payment for upon radio quality of measurement of interests, queries act symmetric-key decryption, which is the cause of an unimportant overhead.

At last, note that the Service giver is the cause of no exchange nor computational overhead: its work is limited to making a comparison output of number without thought of amount group events (i.e., loose ends) and forwarding statements. From an able to use point of view, the work of

the service giver is no different from that in a not privacy-preserving solution. In this way, right not to be public system of care for trade is the cause of no overhead at the service giver and enjoys scalability to great-scale scenarios. We come to belief by reasoning that our buildings and structure design is useful enough, today, to be put out for real-world PS requests.

5 Related Work

Participatory Sensing Projects. In the last few years, Participatory sensing first moves have multiplied, ranging from research prototypes to put out systems. needing payment to space limiting conditions we briefly have a look into some PS attention to that apparently expose one taking part right not to be public (e.g., location, regular ways of acting, and so on.). Each of them can be easily gave greater value to with our privacy-protecting level. Interested readers may discover a larger list of PS applications at. Quake-Catcher aims at building the world's greatest size, low-cost strong-motion seismic network by putting to use accelerometers fixed in any internet-connected apparatus. Kim et Al. Use the power of PS for purposeful places (e.g., home, office, and so on.) discovery. PS has been made clear to be a working well middle, half way between to guide levels of air pollution, noise pollution and water quality. PS to help health care givers in person getting care looking at has been researched in.

Privacy. Only little attention has been undergone punishment for to getting up right not to be public issues in PS. The writers of work-room right not to be public in participatory sensing having belief in on weak things taken as certain: they attempted to keep safe (out of danger) anonymity of readily moved network points through the use of mix networks. (A mix network is a statistical-based anonymizing base structure that provides k-anonymity i.e., a person fighting against one cannot say to a user from a group of K). However, mix networks are quite wrong for many PS gold frames. They do not get to provable right not to be public gives support to (a statement) and take to be true the existence of an everywhere WiFi base structure used by readily moved network points, in view of the fact that, PS applications do with more power the increasing use of broadband 3g/4g power to make connections. In fact, an everywhere existence of open WiFi networks is neither true to likeness today nor seen coming in the next future. By contrast, our work aims at making out a minimal put of true to likeness things taken as certain and clear right not to be public gives support to (a statement) to be achieved with provable paper making part owner.

The work in studies privacy-preserving data aggregation, (e.g., computation of sum, average, variance, and so on.). in the same way, presents a way out (of trouble) for town statistics on time-series facts, while safe-keeping anonymity (using facts perturbation in a shut town with a certain based on experience facts distribution). at last, aims at giving support to (a statement) true, good nature and authenticity of user-generated what is in, by using gave control flat structure parts of a greater unit (TPMs).

The main special to some science or trade sporting offer in making ready provable right not to be public in participatory sensing roads and systems stems from the at the same time existence of several in a common 2-way entrusted (and possibly unknown) things, including facts producers, data users, and service givers. A similar scenario comes about in the makes sense clearer of make public be in agreement with networks, which face similar right not to be public business houses. However, state-of-the-art answers (e.g.,,) take to be true an a-prior knowledge

(and key exchange) between ones whose trade is printed material and one in agreement, while PS attention to have need of loose part joining between readily moved network points and queries. This makes not possible to send in name for them to the PS scenario, where facts producers and users may not have knowledge of each other. Our answer keeps safe (out of danger) their right not to be public while having need of no straight to effect on one another between the two meetings of friends.

6 Conclusion & Open Problems

Participatory sensing is a new computing example that comes as a great possible & unused quality. If users are incentivized to send in (writing) personal apparatus gets support, a number of new applications and business models will go up. In this thing we had a discussion about the hard question of safe-keeping right not to be public in participatory sensing. We put forward as a fact that user taking-part cannot be given without safe-keeping the right not to be public of both facts users and knowledge for computers producers. We also made an offer the buildings and structure design of a privacy-preserving Participatory sensing base structure and introduced a good at producing an effect cryptographic answer that gets done right not to be public with provable paper making part owner. Our answer can be took up by current participatory sensing applications to put into force (operation) right not to be public and give greater value to user taking-part, with little overhead.

This work represents a first journey into strong right not to be public gives support to (a statement) in PS, in this way, much remains to be done. things on a list for future work, join (but are not limited to):

1. Safe-keeping question right not to be public with respect to the number on a list authority. Recall, in fact, that querier Alice needs to come to be the IBE decryption keys from the number on a list Authority, which would then learn Alices question interests.
2. Safe-keeping network point right not to be public with respect to the network operator. Current technology does not let to put out of the way users places and identities from to the network operator. for this reason, it is an interesting sporting offer to give

support to (a statement) network point anonymity in broadband networks.

3. Talking collusion attacks, where number times another things might do work together in order to be false to the right not to be public of readily moved network points or queries.

4. Getting (making) better the syntax of supported question sorts. In fact, PEPSI so far lets query/report matching based on the loose ends on condition that by both readily moved network points and Queriers. However, PS applications might have need of more complex questions where queries are interested in a mass of the reports (e.g.,, mean or sum 10), or even complex question predicates (e.g.,, comparisons). While simple mass purpose, use put value over encrypted knowledge for computers is able to keep living with ready (to be used) cryptographic techniques (e.g.,, homomorphism encryption), making able good at producing an effect put value of complex predicates remains an open sporting offer.

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 (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.