International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-2, February 2015

Security Handling In Participatory Sensing

Tincy Chinnu Varghese

***Abstract*— Participatory Sensing is an evolutionary model now-a-days for acquiring some basic information (temperature, population, traffic control) with the help of sensors. Here as we said we are receiving this some basic in formations with the help of certain sensors which we can use in equipments that we use today that is always-on and portable For eg, Mobile Phones .By updating the devices with sensors we can do the Participatory Sensing very easily. In this PS method we can share data which are collected using our sensor equipped devices to a group. As we are facing the security problems all over networking section here also we need a secured way for PS. In this article we are introducing the security infrastructure feature for a secured PS Environment.**

***Index Terms*— Participatory Sensing (PS), Privacy, Participant, Querier, Service Provider (SP), Registration Authority (RA)**

I. INTRODUCTION

Last decade itself we all know the usage of mobile phones are at the maximum limit.We all are used to mobile phones.In the early times it was a device only for making calls and messaging.But now we can have a lot of applications in it for our use.As we know we need a device which is alwayson and portable for performing the sensing process.Such a device is our mobile phones.The usage of mobile phones have increased upto 5milions.As the need for participatory sensing is a useful one and we should make it into reality by embedding them to our mobile phones that are commonly used electronic devices.As these mobile phones are always-on and easily portable the sensors can be embedded into it. With the help of cameras,voice recorder in the mobilephones we can easily sense the information.We can also add sensors to them according to our needs.The idea of participatory sensing helps us to gather some useful information which wiil be helpful for us one or the other way.The informations which we can access can also be sent to others.

As we take the network connectivity into consideration while updating details the user's indentification may be disclosed to the group.Here we should provide a secure way for updating our information on to the pool by not letting the pool to know whether who have sent this data.To maintain this privacy we have introduced this new concept of Enabling privacy in participatory sensing,which will give us a way to update our information more securely.For this we need our mobile phones to be embedded with some sensors which will sense the datas about the traffic,temperature,parking. details,consumer details etc.Here we are saying about an infrastructure which would help us to perform this secure sensing and to update the sensed datas.

Here the datas that are collected using the sensor equipped objects are updates by several users.But there is a problem about the trust on these datas ,whether this is true and could be taken into consideration and used for our needs.In order to maintain the privacy for the user and consumer we are using the encryption algorithm here so that the information that are updated by the user and the consumers who are using it will be true and not attacked

Manuscript received February 23, 2015.

Tincy Chinnu Varghese, Computer Science and Engineering, MG University

II. PARTICIPATORY SENSING

Participatory Sensing is a new concept that looks into the endless gathering of information using some sensor embedded equipments such as mobile phones that are portable and used in large scale now a days .As we know we need an network infrastructure in order to do this sensing the idea of wireless networks is not economically practical. To avoid this we cal take into consideration the mobile networks itself to sense datas and gather them and simultaneously update them through our mobiles. Thus we can sense different types of datas such as parking availability in a particular city, traffic in urban areas, gas prices, temperature,weather forecasting etc.

Here the users are in contact with an application server or service provider.In the Registration Authority first time the user should register themselves.By updating some required details as an basic information for our account .Next time we can directly start the updating of information into the pool. By registering we can make sure that the users coming into contact are not fake people. The consumers are also needed to register for the first time .By practicing this it is possible to maintain a secure manner to share our sensed information to others .Fig :1 shows a basic structure of our concept.

III. PARTICIPATORY SENSING COMPONENTS

A participatory sensing strucuture include the following parties:

1 .**Mobile Nodes** are the combination of mobile phones and the senosrs embedded in it.They provide the sensed information to be reported to the application server.

2.**Network Connectivity** are responsible for the gathering datas that are happening around us and to upload it to the respective pool foe further usage.

3.**Consumer:** One who sends some query to a service provider and waits for a matching reply.

4.**Service Provider:** Works as a mediator between the consumer and the mobile nodes.It receives reports from users and queries from customers.Finally gives the report for the required query to the end users.

5.**Registration Authoirty**:This is responsible for the registration of both the users and the consumers.Avalis user or consumer can take part in this Participatory Sensing Process.

Here th eabove mentioned components are responsible for the smooth processing of our Participatory Sensing.The mobile

phones which we use as the main source is first registered with the Registration Authority.The network operators are responsible for sending the sensed datas to the Service Provider.The consumers also should be registered with the Registration Authority.The query which needs report are sent to the Service Provider from the consumers and the respective reports are sent from Service Provider to the Consumers.

IV. PRIVACY NEEDS

The need for privacy is very important in this concept.Here the sensed datas are sent to the Service Provider from different users.The users who are sending the specific informations should feel that the datas they are sending are secure and their identity is not disclosed.For this security purpose the details regarding the user name is encrypted and send to the consumers.By providing this technique users feel that their identity is safe and go forward with the information updation.As a part of our security the communication bteween the service providers and Mobile nodes and consumers and Service Providers are kept confidential. The privacy checking starts from the point when the informations are sent to the Service Provider by the user.When a user sent an information to the Service Provider it accepts it and generates a key for that particular data and the same is stored in the database of the Service Provider.When a query is sent to the Service Provider from a consumer it is also receiving a key for that particular query and the same is stoerd in the database.Here the next steps takes place ie; the Service Provider is now searching for their matching keys for the query sent by the consumer.If a matching key is obtained it will retireve the particular information thus providing the consumer a report for their query. Other privacy handling is by registering the users or mobile nodes to a Registration Authority and also the consumers with the Registration Authority.By doing this registration only valid users can update information and valid consumers can access the information.This make the feel that the informations that we are receiving are true and can be trusted.

V. PROPOSED WORK

We are now looking into our privacy enhancing structure in our partipatory sensing.The process done in this structure is given by a diagram which gives us a clear idea of our concept.

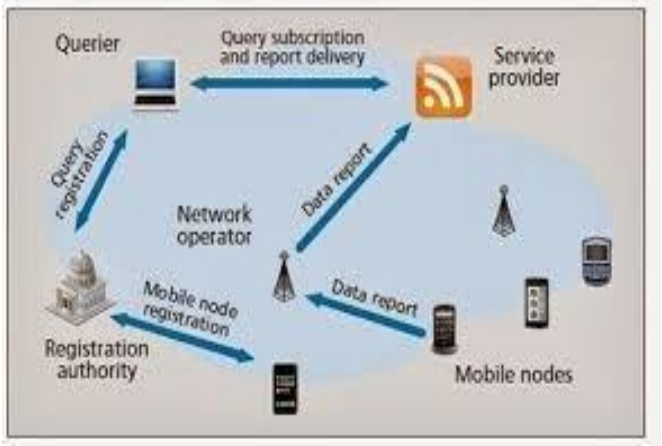


Fig:2 **PEPSI** Architecture

The main aim of this architecture to provide as secure way of privacy for sensing data and sharing it to others.The mobile nodes are first registered with the Registration Authority and also the quqeriers or consumers are registered with Registration Authority.Then the Service Provider who acts as a intermediator between the mobile nodes and querier helps to update information and to get the information from there.

Here the privacy is ensured for both the users and the customers by registering them with Registration Authority and using the Encryption Algorithm Techniques.

VI. OPERATIONS IN PEPSI

1.Registeration of Querier: Here the Querier Q picks "Temp" among the list provided from the Registration Authority and register te querier with the Registration Authority. In return the querier receives a decryption key.

2.**Registration of Mobile Nodes:** Here Mobile Node decides to report about temperature and obtains the corresponding secret for tagging it.

3. Querier Subscription. Query subscribes to queries of type "Temp" in "Texas, USA" using these keywords and the decryption key, to compute a tag. The information about Q's interest and is uploaded at the Service Provider.

4.Report Data: Data report deals with the reporting of certain informations say temp of a particular area.Already there will be certain keys for each information which are being loaded into the Service Provider.For eg:If we want to load the temperature we first register it with the RegistrationAuthority.From there we receive a key to upolad it to the Service Provider along with the information.The information is encrypted and send along with some keywords defining the information along with the key obtained from the RA into the database.

5.Delivery Report:The Service Provider needs to match the keys uploaded by the Mobile nodes with the one uploaded by the querier.If both the key matches then the informations are sent to the consumer.Here the consumer can decrypt the information using the dercryption key obtained from RA and can acess the data for further use.

VII. PEPSI CONSTRUCTION:

We know that the main goal of our concept is to provide privacy to our intereactions.Here we are discussing about a method that help as to maintain security and privacy in our interactions.As theusers who are updating the information to the Service Provider should feel that their identity is not disclosed and only the datas that they are sending are known to the world.On the other hand consumers should also feel that the informations that they are accessing are true and can be trusted.For both this security and privacy we need the concept of a secure algoritm ie;AES alogorithm.This algorithm gives a full support for our needs and therefore considered as our cryptographic tool.

Using this algorithm our interactions are secured.Let us see about the various encryption steps taking plac here.Several steps are:

1.User Registration:

The users who have registered with the RA can be seen here.(Tab 1)

2.Consumer Registration:

The one who are accessing this informations should also be registered wth RA.(Tab 2)

3. All Report Details:
The reports uploaded by the user into the Service Provider can be seen here.(Tab 3)

4.All Query Details:
All the submitted queries to the Service Provider can be seen here.(Tab 4)

5.Privacy for User Details:
Here we can see that the name of the user is in encrypted form which shows the privacy of user identity.(Tab 5)

6.Request for matching key:
When a consumer submits a query the Service Provider should give a matching key.After receiving that key he can access any report.(Tab 6)

7.Matching key Generation:
Here the matching key is generated for the particular query.(Tab 7)

8.Message for registering the non-registered query:
The users are asked to register the query if any not registered with the Service Provider.(Tab 8)

9.After receiving Matching Key:
The query gets a matching key for decrption from the Service Provider.(Tab 9)

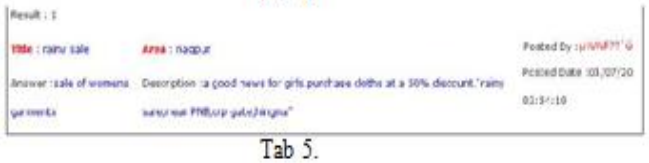
10.Accessing Request:
Consumer accessing the required query.

Tab 1.

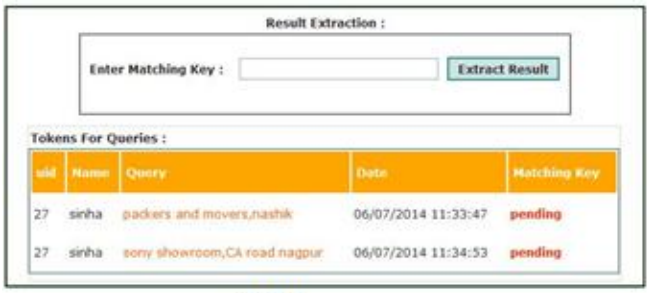
Tab 2.

Tab 3

Tab 4.



Tab 5.

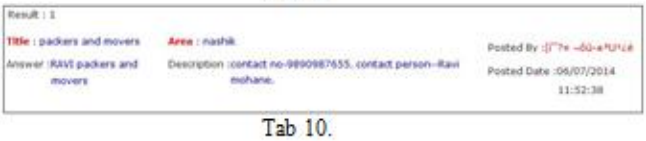


Tab 6.

Tab 7.

Tab 8.

Tab 9.



Tab 10.

VIII. CONCLUSION

Participatory Sensing is a concept with great potential. If users are interested to contribute personal device resources, many applications and business models will arise. In this article we discussed about need for protecting privacy in Participatory Sensing. We claim that user's participation cannot be a asked without protecting the privacy of both users and consumers. We also discussed about the architecture of a privacy-preserving .Participatory Sensing infrastructure and introduced an efficient cryptographic tool that gives privacy with trusted security. Our solution can be adopted by current Participatory Sensing applications to enforce privacy and

enhance user participation, in the future.

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.

[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. 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