INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

# DEVELOPMENT IN LOCATION BASED PRIVACY PRESERVING FRAMEWORK FOR PARTICIPATORY SENSING

**C. Chandrasekhar Reddy[1], Mr. K. Suresh Babu[2]**

*[1]M Tech- Computer networks information security, cchandumtech@gmail.com*
*[2] Assistant professor in cse, kare_suresh@yahoo.co.in*
*School of information technology, JNTU Hyderabad, India*

## ABSTRACT:

In now a day we have many mobiles with various sensors like Bluetooth, Acidometers, GPS system and Wi-Fi sensors. All these are used very widely in this world. Some organisations are depends on this system. It is much important to ensure privacy for the information which flows through this system. With privacy preserving all individuals and many communities are getting benefits. In the system, we may have the collection of the information like location details and trajectory information. All these are sensitive data. To ensure privacy for this information we have many existing systems in this world. All these systems are mainly concentrates on location base privacy preserving methods. But its not much better to use that method. And some existing systems are focused on trajectory privacy. Initially we made a survey about information threats in privacy preserving networks. This results that information will be lost in the trajectory path only. And finally our team decided to develop a framework for preserving privacy in the trajectory path also. This leads to our proposed system. We analysed this with different background knowledge and made some notes. We calculated the effectiveness of this developed system on the basis of information entropy. Finally we made good comparison among the existing systems with the new developed system. This tells that our system is much efficient in privacy preserving among the trajectory path with lower cost and high speeds.

**Keywords**: Trajectory, information entropy, privacy preserving, framework.

## 1. INTRODUCTION

We have much development in the sensor networks like wireless LANS, Wireless Fidelity, Zigbee protocols, Bluetooth integration, GPS system, 3G and WiMax. These networks are going to involved in mobile communication technology. So our mobile devices are developed with the latest equipment of these participatory sensors. These can participate in sensing network to share some information like sharing of knowledge along the network. These devices having storing and processing capabilities. The participatory sensing is also known as urban sensing. When compared with existing systems like WLAN networks, this

sensing network results good in the field of cost and efficiency and speed. This privacy preserving system is involved in intelligent transportation system and some health care systems to serve the users greatly. In this network all the participators can share sensitive information like trajectory information. Its necessary to preserve privacy in the network.

In the existing world, the privacy preserving is totally depends on the huge information about geographical areas like details about longitude and latitude. This information is very much useful for users to identify the location on the earth. The participator generally uploads the information by tagging with location details into the network by joining this privacy preserving application.

The general ways in which the participators information threatens by hacker are by tracing the information on the trajectory line itself. There are some loopholes in the trajectory while travelling the information. So trajectory path is the sensitive area to be focused. The participators gets attacks by unknown persons when they got to know the current location details of user, and taking his/her photographs and do some unwanted actions like shooting the private scenes and saving the personal chats into their systems.
When the participators know that the information uploaded by them is not safe and it is threaten by others, then they will not show any interest to join in the network. They may have bad opinion on the privacy preserving network. This leads the system gets failure in the real world. Hence the primary task in the system is to provide some privacy along the trajectory while travelling the uploaded information to the server. This will be handled by our location based privacy preserving framework for participatory sensing.

In many of the existing privacy preserving systems, the information which is uploaded by the participators will get revealed to the hackers along the trajectory. Analysts made a survey on this based on the published trajectories in the system. I will give most suitable example, If any one wants to build a hospital in the city, He simply observe the trajectories which have hospital information and can take a decision where to build the hospital to get good profits. He can build the hospital where no hospital is exist. And the transportation system can plan by observing the vehicle trajectories.

In the feasible studies our analysts known that the spatial temporal information is rich and it is very sensitive information for participator. Normally the data will be uploaded will be catch by using the links between the reports. We have a link for next report. Using this place where the data is collected will be known to others. To prevent this we need to cut the links among the reports as it is compulsory. For this i developed the location based privacy preserving framework which is good system for privacy. We know that participators information may not be always sensitive based on the locations. And it will be sensitive only on sensitive trajectory segments. In this proposed system i used a mix zone which helps in preventing to trace the trajectory. Generally these mix zones are placed at road intersections where there is not possible for the participator to upload or share the information to the system. And at the road intersections, the data may not be sensitive and it may be sensitive at some other locations. Hence we introduced the theoretical mix zones. Using this system is much efficient in speed and there will be no data loss for participators.

The work done by the team is given below:

- We developed the framework called location base privacy preserving framework for participatory sensing to serve the participator better.
- We introduced theoretical mix zones model to ensure that the participators information is threat free.
- Here we use graph theory for maintaining mix zones model.
- In the system we satisfies three metrics they are 1: privacy level metrics
  2: privacy loss metrics
  3: information loss metrics.
- And we analyse the attacks model to prevent attacks on information with different

background knowledge.

- And finally we compare our new system with old existing system and made a report which tells that this system is well in cheap cost and high performance in less time.

## 2. EXISTING SYSTEM

There exists many systems for privacy preserving area. But many of the systems are focused on the location based privacy preserving methods. We are not sufficient with the location privacy as we still have threats of information in existing systems. The old systems are not capable of maintain privacy along the trajectories. Trajectories are main important because participators can upload the data in the system. That information has to travel in a path called trajectories. These are too sensitive to reveal the information like location details. So it cause to reveal temporal information and others can analyze the trajectories in existing systems.

In many of the existing systems there is a threat of location details which is known as theft of spatial temporal information. It is mainly because of linking between reports. In uploading process we tag some location based details along with the information. This location details are very sensitive. So its necessary to unlink between the output reports. This unlink process is not exist in old systems.

### 2.1 Disadvantages in existing system:

i. In the existed system, if the adversary has prior information about the system architecture, how it works and all these things, Then its effortless and useless to use the system.
ii. And the adversary may knows the first entry and the first exit of participators information, this also may cause to threat to information.
iii. These are mainly focus on preserving the locations where participators exist. But not preserving the trajectories. This also a drawback of existing system.
iv. Time consuming to operate the old systems. But no efficiency in using it. Installation cost also too much.

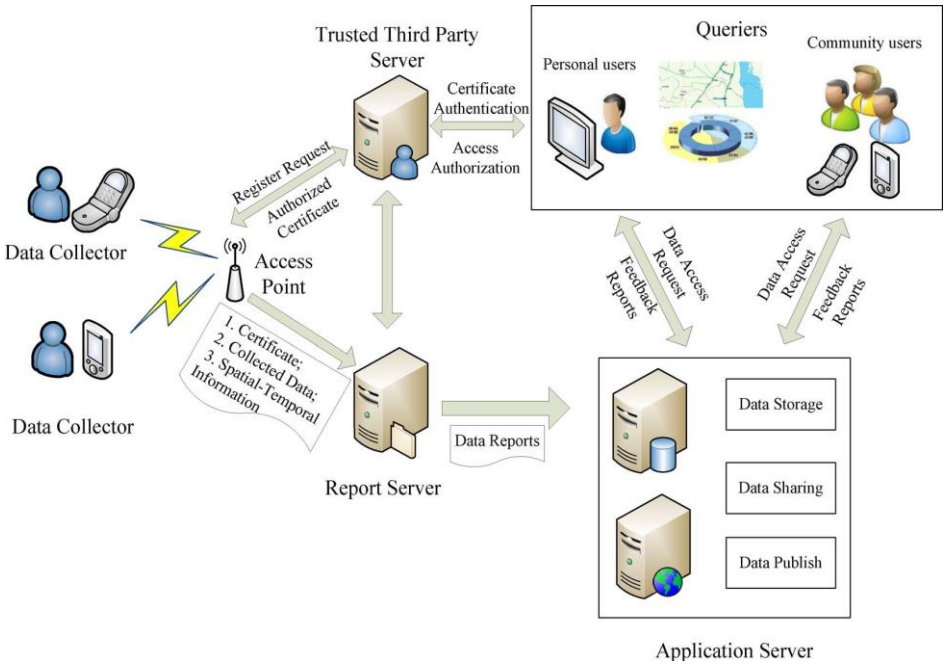
## 3. PROPOSED SYSTEM:

I proposed a system called location based privacy preserving framework for participatory sensing. It's the extension of existing trpf system. Where the old systems concentrates on location privacy, my system will concentrates on trajectory privacy effectively. The information travelling on the trajectories will not be safe. So we proposed this system and it will concentrate only on sensitive areas. This privacy preserving framework will takes only sensitive trajectory segments. There are some new technologies introduced in this system. That is mix zones model. In trajectory the participators may be traced by others. To prevent unnecessary tracing we use this mix zones model. These mix zones works at the road intersections, so these called road mix zones. At the intersection the information may not be sensitive. And the participators are not able to upload or share their information to the server. To serve the participator better with preserving good privacy we use theoretical mix zones model which is not present in any of the existing systems.

### 3.1 Advantages with proposed system:

I. It is much feasible to calculate the trajectory privacy level. Here we can achieve maximum of the privacy in this approach. We can see this in the reports.
II. Its cheaper to install in the current environment.
III. In this proposed system, Nothing information will get lost.
IV. And its very speed in the aspects of time factor.

## 4. ARCHITECTURE:




## 5. ALGORITHM:

### 5.1 Input:

i. Set of managers ( M ) 1<i<n
ii. Set of departments ( Di )
iii. Set of customers ( Ci )
iv. Request made by $i^{th}$ user for $j^{th}$ dept ( R ij ).

### 4.2 Output:

i. Response from manager. (0 / 1) .

**Step 1:**

- If R ij ==0
  - Get D j from request by admin. (dept)
  - Get U i from request by admin. (user)
  - List of managers in dept Dj = Mi(Dj)
  - Excepted service location made by user for dept = (Lui)Rij
  - List of managers for Dj from Lui where (Mi)Dj @ (Mi)Dj ==== (Mi)Dj Lui
  - Get status of (Mi)(Dj)Lui… if free allocate Rij for (Mi)(Dj)Lui

**Step 2: (By Manager)**

- View request from admin Rij

**Step 3: (By Manager)**

- Upload response to dataset.

**Step 4: (By Manager)**

- Set RS to 1.

**Step 5: (By User)**

- User can receive reply of the request R(Rij) from the system.

This algorithm is mainly consists of 3 objects. They are Admin, Manager and User. Admin will maintain whole system as he having his own password to enter into the system. Manager will signup first to get an account, Then he will get a password to enter into system. User is the participator he will also signup to get the password for entry to system.

This algorithm having 5 steps. In first step the user will request the system for some resource. The steps 2,3 and 4 will be taken by the manager. In step2 the manager can view request came from admin. In step3 he can upload the response to the dataset. In the step4 he will set the value of RS to 1. As the request is resolved.

Here user can make only one step. That is step 5. In this step the user can receive a reply for his request in step 1. It is either 0 or 1. If its 1, The request is accepted by the system. Otherwise the system rejects the request from user.

All these steps are maintained by admin. If no manager is allocated to user, Then the admin have capabilities to assign a manager for users request. And admin can check the status of each and every request.

## 6. The application:

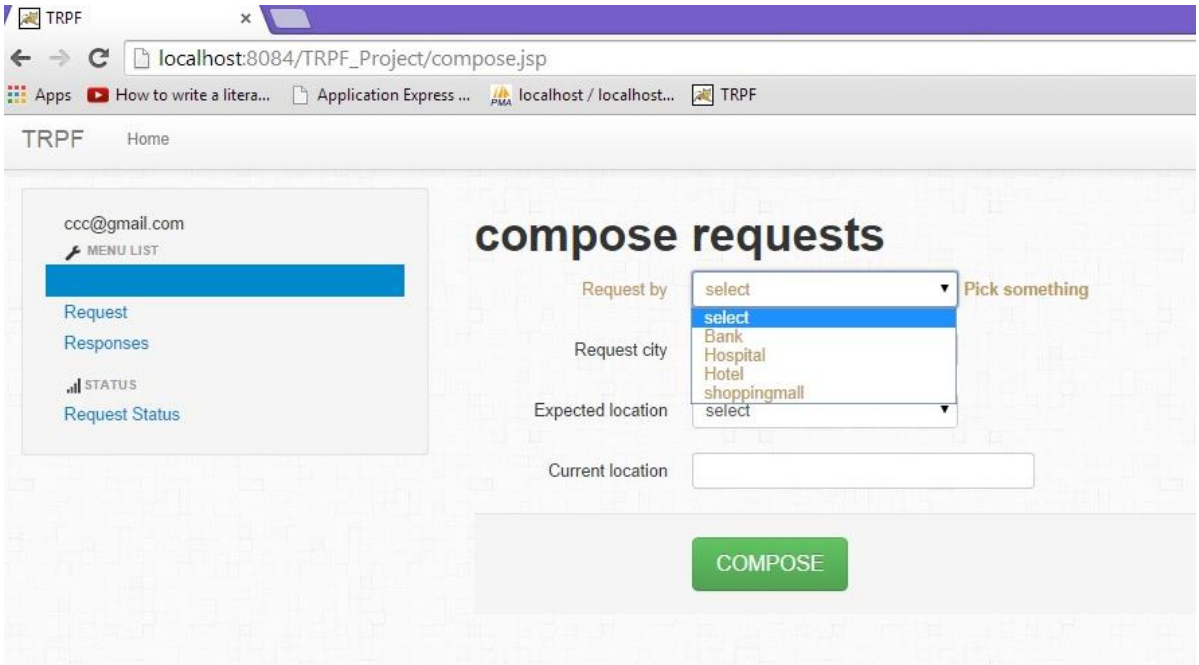



**Fig: User generating request**

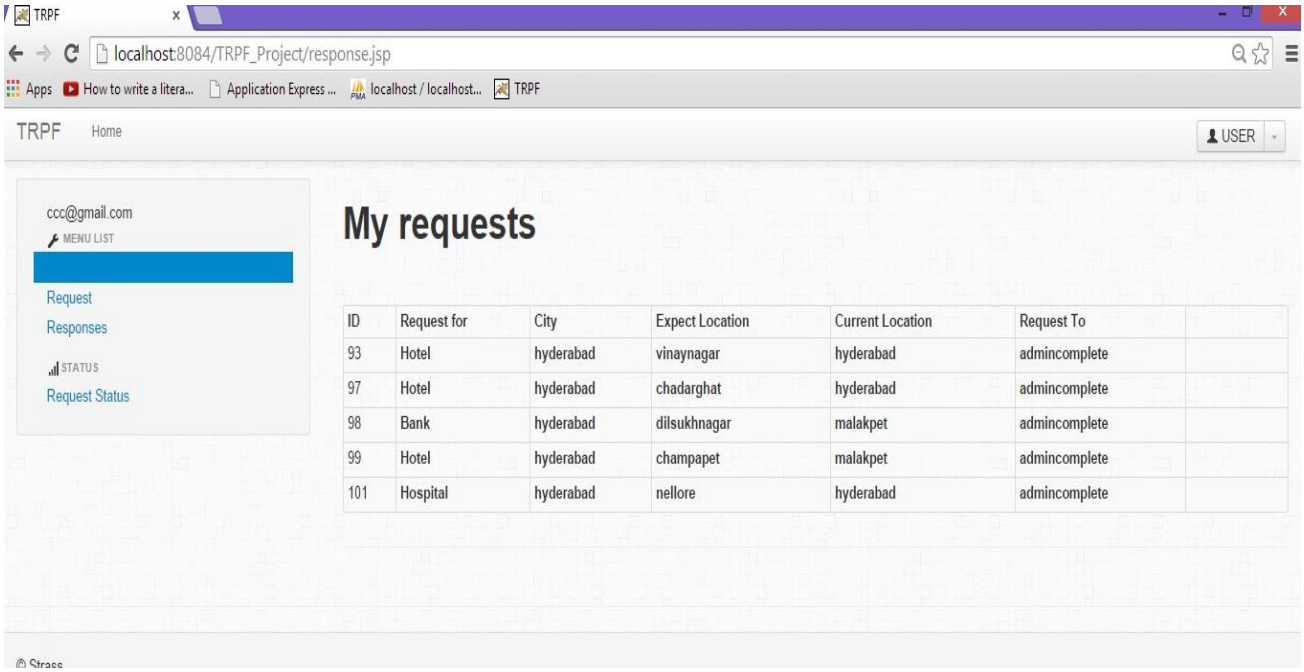



**Fig : User checking request status**

## 4. Conclusion

The openness in the existing system causes threat in trajectory information and the participators are reluctant to share the personal information in the system. This causes many problems to the users. Hence in this location based privacy preserving framework we installed theoretical mix zones for ensuring the privacy for participator. The users are very happy to share their information within the network. Here we developed the mechanism which will works in preserving the trajectories.

And the reports were collected, is estimated that our proposed system is much better than the old systems in terms of preserving information and as well as time consumption. It takes lesser costs for installing this system in our environment.

## REFERENCES:

[1] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Commun. Mag., vol. 48, no. 9, pp. 140–150, Sep. 2010.

[2] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "Anonysense: Opportunistic and privacy-preserving context collection," Pervasive Comput., vol. 5013, pp. 280–297, 2008.

[3] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. ACM 1st Int. Conf. Mobile Systems, Applications and Services, 2003.

[4] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 1–18, Jan. 2008.

**A Brief Author Biography**

***C Chandrasekhar reddy*** **–** Received B.Tech degree in the stream of computer science from JNTU Anantapur. And presently working toward M.Tech degree in the stream of Computer science information security from School of information technology, JNTUH, Hyderabad.

***Mr. K Suresh babu*** **–** Completed M.Tech from Hyderabad Central University (HCU) , Hyderabad. Presently pursuing Ph.D. from JNTU Hyderabad in the field of network security in MANETs. Currently Assistant Professor of CSE in School of information technology, JNTUH, Hyderabad.