 ISSN: 2321-8169
3548 – 3551

A Survey on Privacy Preserving and Content Protecting Location Based Queries

Swapnil Ramesh Jadhav
ME Research Scholar
JSPM's Imperial College of Engineering
Pune, Maharashtra
dreamsswapnil36@gmail.com

Prof. Rajesh Nandkumar Phursule
Asst. Professor
JSPM's Imperial College of Engineering
Pune, Maharashtra
rphursule@gmail.com

***Abstract*—** In today's modern world, it is very easy for a person to know his/her location with the help of devices having GPS facility. When user's location is provided to LBS, it is possible to user to know all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions. The massive use of mobile devices pave the way for the creation of wireless networks that can be used to exchange information based on locations. When the exchange of location information is done amongst entrusted parties, the privacy of the user could be in harmful. Existing protocol doesn't work on many different mobile devices and another issue is that, Location Server (LS) should provide misleading data to user. So we are working on enhancement of this protocol.

Keywords- Location Privacy, Private Information Retrieval, Centroid.

*****

I. INTRODUCTION

There are increasing mobile phone users worldwide. So location technologies can be currently used by wireless carrier operators to provide a good forecast of the user location. Now a days, number of users are use location based services which can provide location-aware information.

What is Location Based Service (LBS)?

Location based service is a service accessible with mobile phones, pocket PC's, GPS devices. It is like Google maps, map request. Mobile devices with positioning capabilities (e.g. GPS) facilates access to location based services that provide information relevant to the user's geo-spatial context. Number of users uses these services for retrieving Points Of Interest from their current location. LBS can be query based and provides the end user with useful information such as "Where is the nearest restaurant?"

Basically when user used specific location based service or registered for that, then LBS can provide number of other services like delivery coupons or other marketing information to customer who is in a specific geographical area. Now a days, there are number of user takes advantage of location based services and graph is steal increasing. (fig.1).

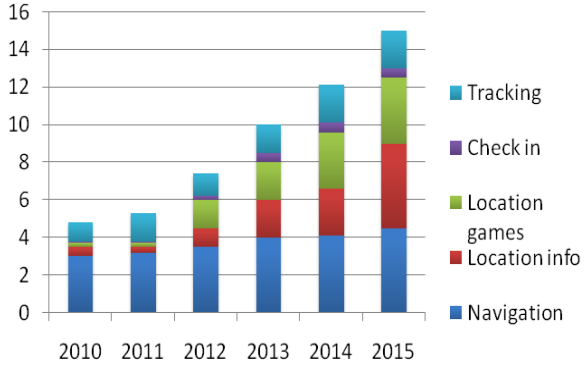

Fig.1- Increasing users of LBS

But there are certain problems while using LBS that it may collect and use vast amount of information about consumer for a wide range of purpose. Location information is sensitive and users don't want to share such information to untrustworthy LBS servers. Because number of malicious adversaries may obtain more private knowledge of the users. Also, queries fire by the user having sensitive information about individuals, including health condition, lifestyle habits. So he doesn't want to disclose it. Privacy concerns are expected to rise as LBSs become more common. Location privacy means data privacy. So here privacy assurance is measure issue. On the other, location server has their own database in which, number of point of interest records are located (fig.2). So server has to prevent database access from unauthorized user and also user who have not pay for that service.

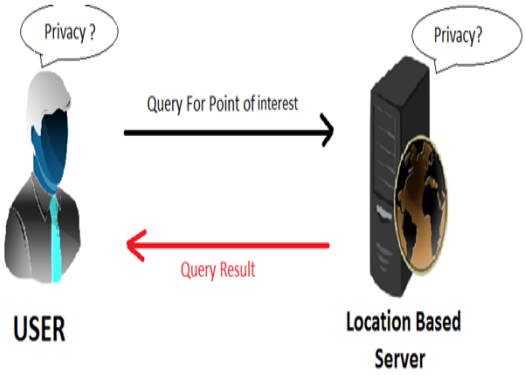

Fig 2- Location Based Service

Number of Existing system used protocols for privacy of Location based services. But we have to secure three things i) location privacy ii) query privacy iii) database privacy.

II. PROBLEM STATEMENT

Existing system involve two protocols namely oblivious transfer and private information retrieval [8]. But these protocol doesn't work on different mobile devices and additional problem will arise that location server LS should supply misleading data to client is also interesting.

Compared to previous work, we have to achieve reasonable communication and CPU cost. It's better to use A-TTP free protocol for location privacy in location based services.

While using these protocols we can fire only one query at a time. We have to enhance this protocol for executing number of queries at a time and can execute different types of spatial joins queries. Also we will enhance public grid in which group of users can determine his location at a time.

III. RELATED WORK

A lot of research has been done on privacy preserving. But no one gave absolute guarantee of user's data and query.

i)Path Confusion

With the help of path perturbation algorithm [1] that continuously collect location sample from a large group of users. When two users met at one location, this algorithm can cross paths in area. So adversary would confuse the paths of different users.

If two users move in parallel, the path perturbation algorithm perturbs the parallel segment into crossing segment.

But this algorithm technique is unable to protect time-series location information.

ii) Dummy Locations

This method mainly employs the idea of dummy locations [7] [9] to protect a user's location privacy. These methods propose to generate dummy trajectories in order to confuse the adversaries. In that when user can query to server with their mobile location and parameters, it can be converted into another query having user's real location and k-1 dummy locations and their parameters.

But observe that, privacy is not protected by replacing the real user identity with fake one [11] because in order to process location dependent queries, the LBS needs the exact location of querying user.

iii) K-anonymity

K-anonymity [3] is a wide-spread general privacy concept not restricted to location privacy. It provides the guarantee that in a set of k objects (mobile users), the target object is indistinguishable from the other k – 1 objects.

With this technology it adds one concept ANONYMISER [10] which is trusted third party (fig 3). A user sends its location, query and K to the anonymiser, which is a trusted third party in centralized systems or a peer in decentralized systems. The anonymiser removes the ID of the user. TTP regenerate cloak for user location by making K-anonymise spatial region in which number of k-1 users are involved. Then anonymiser sends the K-ASR and query to the LBS sever, which calculates the candidate results respect to the cloaked region and sends them back to the anonymizer. Then the anonymiser which knows the locations of all the users calculates the actual results and sends them back to the user.

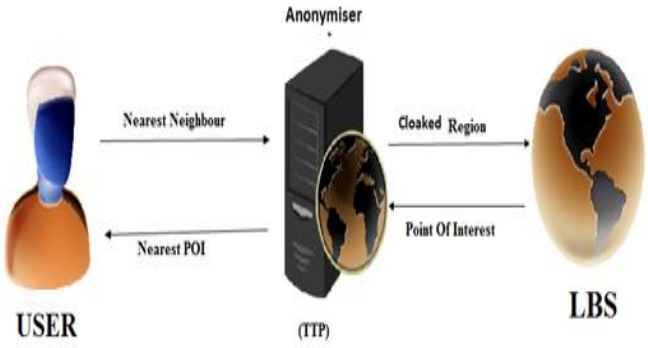

Fig 3- Location Based Service using TTP

There is a enhancement of this system that is rather sending all cloaked region to server, an anonymiser only sends a center of K-anonymizing spatial region (K-ASR).

But still there are drawbacks in K-anonymity-

(i) If attacker directly gains the access of anonymiser, the privacy of all users is compromised.

(ii) At least minimum user should subscribe, otherwise CR cannot be constructed.

(iii) User updating is another for making clocking regions.

(iv) If user fire query out of the clocked region, he can be easily identified because he will be included in all CRs.

iv)Private Information Retrieval

The basic idea is to employ PIR [12] to enable the user to query the location database without compromising the privacy of user .Existing system requires clocked region and a TTP, but it doesn't need of anonymiser[2] and privacy is achieve through cryptographic techniques. Here server forms the region regarding to POI and while answering to query, server first send regions to user. The user finds the region that contains him and utilizes PIR to request all points within that region. So, the server does not know which region was retrieved.

But this technique is expensive and high CPU cost. Also user can go through high preliminary test, so extra time required to execute query is greater.

IV. PROPOSED WORK

Existing work contains two protocols namely oblivious transfer phase and private information retrieval [8].First user publicly determines his location using GPS coordinates and then he determines private location in a public grid using oblivious transfer (fig 4).After getting cell id and related symmetric key from server, user fires query using PIR

 ISSN: 2321-8169
3548 – 3551

protocol and get proper block from database which he wants. Here there is assurance of privacy both for user and server.

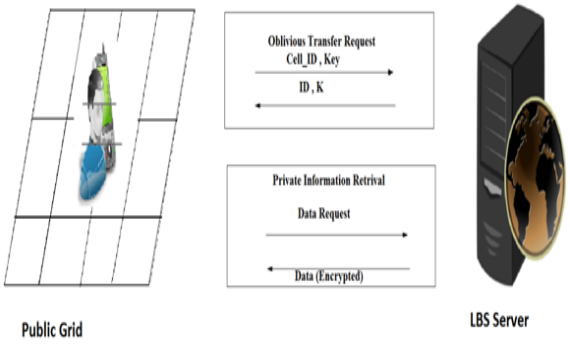

Fig.4- Privately determine User for LBS communication

By studying above research works by scholar we are going to enhance this system. Because every time user needs to determine his location and according to that he fires query to the server. So there are unnecessary steps to done to acquire block of data from database server.

So we are going to propose system with number of users in same public grid or region will acquire database using a single point. In existing system, user query to server for his NN, then server send back POI regarding to its location.

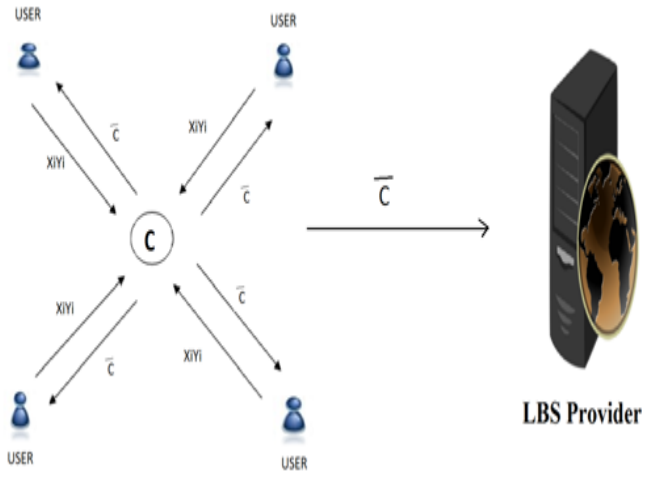

Fig.5- LBS Services Using Centroid.

Here we have taken into account a concept of centroid i.e. in a particular region, there are number of unknown users use location based services. So for every user, he has to determine his location and send it to server. So we decided that we can make single point in the region for communication with server .So there is no need to every user to determine its region all the time.

The concept of **CENTROID** is different than previous existing systems. Here we assume that, all the users in a public grid known to each other i.e. they are trusted with each other. Then one of the groups from the public grid can make a centroid point for communication with server because they have a trust on each other. So one of the trusted user in the group gain locations of other user and make a centroid point.(fig 5).After computing the centroid, user sends it to all his companion and LBS provider. So actual position of the user and his companions remains hidden.

By getting centroid all the users fires the query regarding to that centre point. Here we cannot search nearest neighbors query .But user can access data from server from their real location and LBS server wouldn't know actual position of user and it will send data to centroid.

One advantage in that is we can take limited number of users from a public grid. All the users are trusted and known to each other. So privacy is increases. Also we are going to enhance this by masking the locations of user and their companions while making a centroid.

V. CONCLUSION

In this paper we have done survey on privacy preserving and content protecting location based queries. We have studied all the references by scholars to develop a protocol both for user and server for their privacy assurance.

In these days there is necessary to provide high-end privacy to user and server in location based services.

Our proposed work shows that we are giving privacy to number of users at a time. Also we will enhance this protocol because sometimes server gives misleading data to user. So we have to avoid it because user pay for service and getting wrong information is not fair.

REFERENCES

[1] B. Hoh and M. Gruteser, "Protecting location privacythrough path confusion," in Proc. 1st Int. Conf. SecureComm, 2005,pp. 194–205.

[2] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan,"Private queries in location based services: Anonymizers are not necessary," inProc. ACM SIGMOD, Vancouver, BC, Canada, 2008, pp. 121–132.

[3] B. Gedik and L. Liu, "Location privacy in mobile systems: A per-sonalized anonymization model," inProc. ICDCS, Columbus, OH, USA, 2005, pp. 620–629.

[4] C. Gentry and Z. Ramzan, "Single-database private informa-tion retrieval with constant communication rate," inProc. ICALP,L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung,Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.

[5] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database pro-tection," in Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.

[6] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino,"Approximate and exact hybrid algorithms for private nearest-neighbor queries with database

ISSN: 2321-8169
3548 – 3551

protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010.

[7] Deepika Nair, Bhuvaneswari Raju "Privacy Preserving in Participatory Sensing" in IJSR,Volume 3 Issue 5, May 2014

[8] R.Paulet, M.GolamKaosar, X.Yi,andE.Bertino,"Privacy-preserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53

[9] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," inProc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468.

[10] L. Sweeney, "k-Anonymity: A model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002

[11] A. Beresford and F. Stajano, "Location privacy in pervasive com-puting,"IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar.2003.

[12] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998