A Survey Paper on Privacy Preserving and Content Protecting Location Based Queries Using Two Phase Protocol

Subhash Pingale[1], Dinesh Jadhav[2]
M.E(Computer), Assistant Professor, Department of Computer Science Engineering, SKN Singhgad College of Engineering, Korti, Pandharpur, Solapur University, Solapur[1]
M.E (Computer), Department of Computer Science Engineering, SKN Singhgad College of Engineering, Korti, Pandharpur, Solapur University, Solapur
dinesh.jadhav0208@gmail.com[2]

Abstract: Location Based Service LBS is the service accessed on mobiles or devices with GPS. In order to use these services there are certain issues to the data being shared and the information of the user who is using this service may be exposed publicly, even though the user doesnot want to share his information in public domain.

A lot of research has been done over this, to protect the users data to be accessed by unauthorised users and those who are not the intended users of that information.

We propose a solution to one of the location-based query problems. A user wants to query a database of location data, known as Points of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; And the owner of the location data, that is, the location server, does not want to simply distribute its data to all users.

Keywords*: Location Based Queries, User Privacy, Private Information Retrieval, Content Protection*

*****

I. INTRODUCTION

Location based service is a service accessible with mobile phones, pocket PC's, GPS devices. There are many services which allows user to use or access the location data like Google maps, map request. GPS enabled devices such as Mobile devices provides access to location based services that provide information relevant to the user's geospatial context. Number of users asks for finding the preferred location or Points Of Interest from their current location such as finding the nearest movie theatre.

Any user who wants to use the location based services, he/she has to register for it and then only Location Based Services are made available to them. Now days, there are number of user takes advantage of location based services.

While using those services certain problems arise such as the certain information about the user may be collected and usedfor a different purposes. Location information is sensitive and it must not to be shared 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 common. So here privacy assurance for the users datais measure issue. Also the location server has their own database in which, number of point of interest records also some information such as geo-spatial data are stored. So to avoid the unauthorized access to the LBS servers must be avoided and users who do not pay for those should not be allowed to use that data.

II. RELATED WORK

Many researchers have done some research to overcome the issues of the LBS services. There is still no assurance about the privacy of user's data and query.

i)Path Confusion: Here the algorithm is used in order to protect the users data from each other and continuously collect location sample from a large group of users. If two users move in parallel, the path perturbation algorithm perturbs the
This algorithm technique is unable to protect time-series location information.

ii) Dummy Locations: This technique provided the idea of dummy locations to protect a user's location privacy. These technique propose to generate dummy location specific geo-spatial data in order to confuse the different unauthorised accesses. In this user fires a query with his own original location and some k-1 dummy locations, this information is sent to the server using the mobile devices Here privacy is not protected using the dummy locations, because to get the response to the user's query, real location of the user is required.

TABLE 1: Related Work

Sr. no	Paper name	Author name	Description	Disadvantage
1	Location privacy in pervasive computing	A. Beresford, F. Stajano	The privacy of the user is maintained by constantly changing the user's name or pseudonym. The frequent changing of the user's name provides little protection for the user's privacy	This requires careful control of how many users are contained within the mix-zone, which is difficult to achieve in practice.
2	A hybrid technique for private location-based queries with database protection	G. Ghinita, P. Kalnis, M. Kantarcioglu, E. Bertino	Two stage protocol, first phase of the protocol to privately detect user's location in cell and second stage, PIR is used to retrieve the data contained within the appropriate cell.	This gives only privacy to the database of the location servers.
3	LocaWard: A Security and Privacy Aware Location-Based Rewarding System	Ming Li, Sergio Salinas, Pan Li	A new location-based rewarding system, called LocaWard, where mobile users can collect location-based tokens from token distributors, and then redeem their gathered tokens at token collectors for beneficial rewards	Do not provide security to general LBS
4	Privacy-Preserving and Content-Protecting Location Based Queries	Russell Paulet, Md. Golam Kaosar, Xun Yi, Elisa Bertino	It gives a major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties	This model will face the many answer problems.

. **iii) Private Information Retrieval:**Here idea is to add privacy to the users location query. Privacy is achieved using cryptographic algorithms. Server has the information about the point of interests POI. While answering to query, server first send regions to user. The user finds the region belong to him and then finds the PIR in 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.

III. SYSTEM ARCHITECTURE

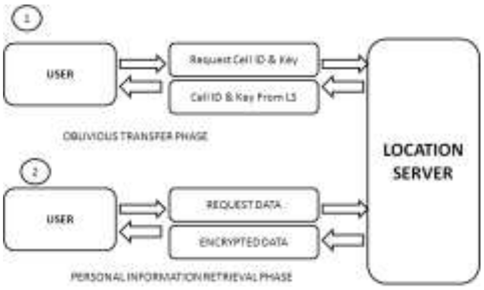

Fig.System Model

IV. CONCLUSION

This model gives solution for location based query that define protocol that enables a user to privately determine and acquire location data without sharing the user's own data to Location Servers. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage.

V. REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.

[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.

[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[6] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib. /supported/IEEEtran/

[8] FLEXChip Signal Processor (MC68175/D), Motorola, 1996.