ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Content Protecting Privacy Preserving Location Based Queries

K Karthik Bhargav
M.Tech Student
Department of CSE,
St.Peter's Engineering College,
Hyderabad, TS, INDIA

Dr. N. Chandra Sekhar Reddy
Professor and HoD
Department of CSE,
St.Peter's Engineering College,
Hyderabad, TS, INDIA

K.Rajani
Assistant Professor
Department of CSE,
St.Peter's Engineering College,
Hyderabad, TS, INDIA

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***

INTRODUCTION

Location based queries are provided by location based service (LBS). These are generally based on a point of interest (POIs). By retrieving the Points Of Interest from the database server, user probably get answers to various location based queries, which are for example discovering the nearest hospital, ATM machine or police station, restaurant.

In years there has been increase in the number of devices querying location servers for information about POIs. Queries are thus use for obtain required information from database [1].

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 geospatial 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?"

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

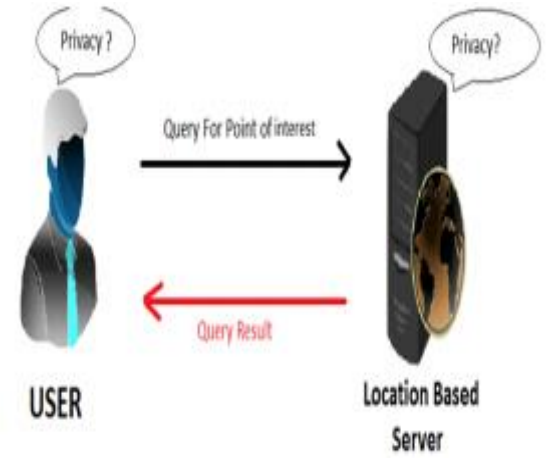


Fig - Location Based Service

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

EXISTING SYSTEM:

The Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBS has to ensure that LS's data is not accessed by any unauthorized user. During the process of transmission the users should not be allowed to discover any information for which they have not paid. It is thus crucial that solutions be devised that address the privacy of the users issuing queries, but also prevent users from accessing content to which they do not have authorization.

DISADVANTAGES OF EXISTING SYSTEM:

- Among many challenging barriers to the wide deployment of such application, privacy assurance is a major issue
- The user can get answers to various location based queries,

PROPOSED SYSTEM:

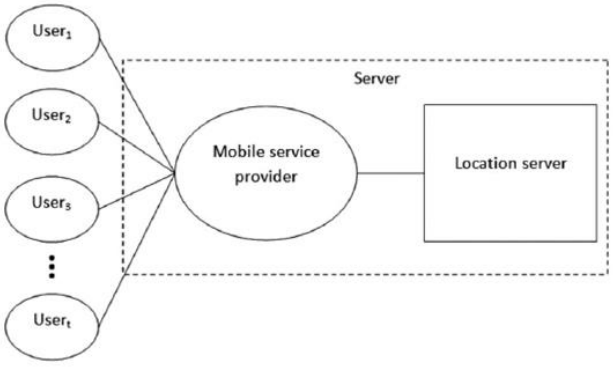
In this paper, we propose a novel protocol for location based queries that has major performance improvements with respect to the approach by Ghinita at el. And. Like such protocol, our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR, to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.

Our protocol thus provides protection for both the user and the server. 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. In other words, users cannot gain any more data than what they have paid for. We remark that this paper is an enhancement of a previous work.

ADVANTAGES OF PROPOSED SYSTEM:

- Redesigned the key structure.
- Added a formal security model.
- Implemented the solution on both a mobile device and desktop machine.

SYSTEM ARCHITECTURE:



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Conclusion

In today's world, privacy has proved to be major concern. Sensitive information is preserve by people and there is always worry about not allowing it to be share in process of querying. This paper thus put forth survey on existing literature and techniques used in field of privacy for protection of data and other content. Working with privacy preserving, various different techniques used are studied in paper along with their pros and cons. All methods implemented new approach of working in order to satisfy objective is reviewed. The proper maintenance of privacy and the detection of the query that violate privacy is the aim to look upon in process of transfer and retrieval of data between user and server. Working on PIR and related work proved adaptive method among them. Based on this future work could be done in efficient way and faster in much more real time. This could be contribution to the system further.

REFERENCES

[1] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino," Privacy-Preserving and Content-Protecting Location Based Queries", IEEE Transactions on knowledge and data engineering, VOL. 26, NO. 5, MAY 2014.

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

[3] 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.

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

[5] 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.

[6] 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.

[7] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino,"Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010.

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

[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