ISSN 2395-1621

A Review on a Location Based Queries With Privacy-Preserving and Content-Protecting

[#1]Akash Dodke

[1]akashdodke@gmail.com

[#1]Computer Engineering,
Savitiribai Phule Pune University India

ABSTRACT

In today's digital world it is much easier for a person to know his/her location by using GPS enabled devices like mobile phones. Location Based Service provider will provide all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions after entering persons location. Location-based query having two problems: (i) if a user wants to query a database of location data, known as Points Of Interest (POI) and doesn't want to reveal his location just because of privacy concern (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. The location server desires to have some control over its data, since the data is its asset. 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. The system is efficient and practical in many scenarios. Proposed solution can be implemented on a desktop pc's, laptops and mobile phones to assess the efficiency of implemented protocol.

Index Terms: Location based query, private query, private information retrieval, oblivious transfer.

ARTICLE INFO

Article History

Received: 30th June 2016

Received in revised form :

30th June 2016

Accepted: 5th July 2016

Published online :

5th July 2016

I. INTRODUCTION

A Location based service (LBS) is an information, entertainment and utility service generally accessible by mobile devices such as, mobile phones, GPS devices, pocket PCs, and operating through a mobile network. A LBS can offer many services to the users based on the geographical position of their mobile device. The services provided by a LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station.

In recent years there has been a dramatic increase in the number of mobile devices querying location servers for information about POIs. Among many challenging barriers to the wide deployment of such application, privacy assurance is a major issue. For instance, users may feel reluctant to disclose their locations to the LBS, because it may be possible for a location server to learn who is making a certain query by linking these locations with a residential phone book database, since users are likely to perform many queries from home.

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 have 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.

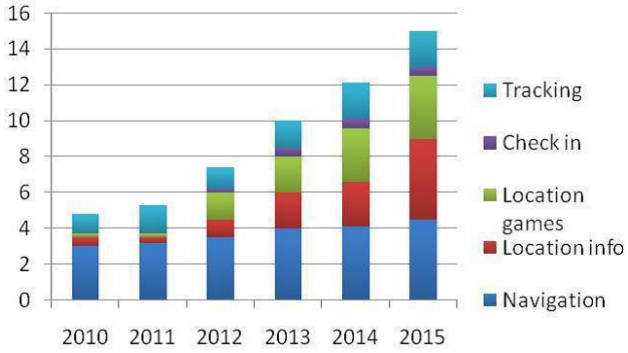

Fig.1- Increasing users of LBS

The rest of the paper is organized as follows: Section II presents the literature survey over the related work. In section III, proposed system is presented. Finally, the section IV concludes the review paper.

II. LITERATURE SURVEY

In this section, we have described earlier work done related to Location based services with Privacy preserving and content Protecting. Various approaches have been developed to preserve te privacy of users and data protection for the server [1].

Beresford [3] proposed the privacy mechanism in location services by constantly changing the name of user or pseudonym within some mixzone.It can be shown that, due to the nature of the data being exchanged between the user (service requirement) and the server (service provider), the frequent changing of the name of user provides little protection for the users privacy.B.Palanisamy [10] had a very recent investigation of the mix-zone approach It was used in road networks. They investigated the required number of users to satisfy the unlinkability property when there are repeated queries over the time interval. This requires careful control of how many users are contained within the mix-zone, which is difficult to get in practice. A complementary technique to the mix-zone approach is based on k anonymity [4].

The concept of k-anonymity was used as a method for preserving privacy when releasing sensitive records. This is done by generalization and suppression algorithms to ensure that a record could not be distinguished from (k 1) other records. These are the solutions for LBS use a trusted anonymiser to provide anonymity for the location data, such that the location data of a user cannot be separated from (k 1) other users. An enhanced trusted anonymiser approach has also been used, which allows the users to set their level of privacy based on the value of k [8], [9]. It states that given the overhead of the anonymiser, a small value of k could be used to increase the efficiency. Conversely, a large value of k could be selected to improve the privacy, if the users felt that their position data could be used maliciously and loses privacy. Choosing a value for k, however, seems unnatural.

There have been efforts to make the process less artificial by using the concept of feeling based privacy [7]. Instead of specifying a k, they propose that the user specifies a cloaking region that they feel and it will protect their privacy, and the system sets the number of cells for the region based on the popularity of the area. The popularity is computed by using historical footprint database that the server collected. Most of the previously discussed issues are solved with the introduction of a private information retrieval (PIR) location scheme [6].

The basic idea is to employ PIR to enable the user to query the location database without compromising the privacy of the query. Generally speaking, PIR schemes allow a user to retrieve data (bit or block) from a database without disclosing the index of the data to be retrieved to the database server [3]. Ghinita et al. used a variant of PIR which is based on Point of Interest (POI).This idea was extended to provide database protection [2], [5]. This protocol consists of two stages. In the first stage, the user and server use holomorphic encryption to allow the user to privately determine whether his/her location is contained within a cell, without disclosing his/her coordinates to the server. In the second stage, PIR is used to retrieve the data contained within the appropriate cell. The holomorphic encryption scheme used to privately compare two integers is the Paillier encryption scheme [4].The Paillier encryption scheme is known to be additively holomorphic and multiplicatively by- a-constant holomorphic. This states that we can add or scale numbers even when all numbers are encrypted. Both features are used to determine the sign (most significant bit) of (a b), and hence the user is able to determine the cell in which he/she is located, without disclosing his/her location.

PROBLEM COMPLEXITY:

The problem described in the paper has a primary purpose to preserve the privacy of the user and protecting the contents from the server. To implement these procedures an algorithmic approach is stated for the implementation of the proposal, along with some few propositions to assure security in system while execution of tasks is in action. The entire sets of propositions have a finite set of calculation steps and methodology for which solution is reachable and feasible. Hence, the problem can be tagged as NP-Complete.

III. PROPOSED SYSTEM

Proposed system having 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.

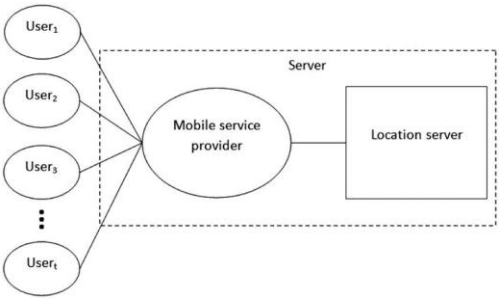

Fig 2: Proposed System Architecture

This Protocol 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. This paper is an enhancement of a previous work.

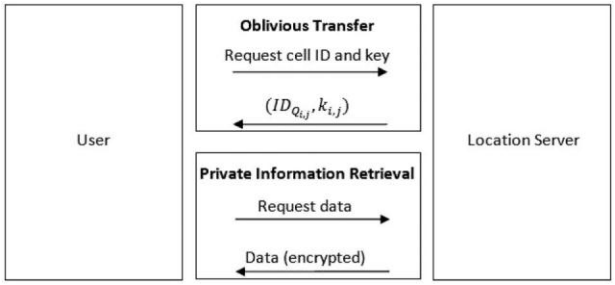

Fig.3 Overview of Protocol

IV. CONCLUSION

We have studied different methods to preserve privacy and protect the contents of server. We propose an efficient approach to secure location based service access for users and server prospective. 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.

ACKNOWLEDGEMENT

I am glad to express our sentiments of gratitude to all who rendered their valuable guidance to us. I would like to express our appreciation and thanks to the Principal of our college. I am also thankful to the Head of Department and my guide Prof. P. M. Mane. I am thank to the anonymous reviewers for their valuable comments

REFRENCES

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

[2] 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,

[3] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, Private information retrieval, J. ACM, vol. 45, no. 6, pp. 965981, 1998.

[4] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in Proc. EUROCRYPT, vol. 1592, Prague, Czech Republic, 1999, pp. 223238.

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, Private queries in location based services: Anonymizers are not necessary, in Proc. ACM SIGMOD, Vancouver, BC, Canada, 2008, pp. 121132. G.

[6] 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. 128, 2010.

[7] L. Marconi, R. Pietro, B. Crispo, and M. Conti, Time warp: How time affects privacy in LBSs, in Proc. ICICS, Barcelona, Spain, 2010, pp. 325339.

[8] S. Mascetti and C. Bettini, A comparison of spatial generalization algorithms for lbs privacy preservation, in Proc. Int. Mobile Data Manage. Mannheim, Germany, 2007, pp. 258262.

[9] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, The new casper: Query processing for location services without compromising privacy, in Proc. VLDB, Seoul, Korea, 2006, pp. 763774.

[10] B. Palanisamy and L. Liu, MobiMix: Protecting location privacy with mix-zones over road networks, in Proc. ICDE, Hannover, Germany, 2011, pp. 494505.

[11] C. Gentry and Z. Ramzan, 'Single-database private information retrieval with constant communication rate', in Proc. ICALP, Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, 2005, pp. 803815, LNCS 3580

[12] C. Bettini, X. Wang, and S. Jajodia, 'Protecting privacy against location-based personal identification', in Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M. Petkovic, Eds., Trondheim, Norway, 2005, pp. 185199, LNCS 3674

[13] A. Beresford and F. Stajano, Location privacy in pervasive com-putting, IEEE Pervasive Computer, vol. 2, no. 1, pp. 4655, Jan.Mar. 2003

[14] (2011, Jul. 7) Openssl [Online]. Available: http://www.openssl.org/

[15] M. Bellare and S. Micali, Non-interactive oblivious transfer and applications, in Proc. CRYPTO, 1990, pp. 547557

