ISSN 2395-1621

Survey on Securing Privacy and Protecting Content of Location Based Queries

[#1]Ashwini B.Lothe,[#2] R. S .Apare

[1]ashulothe@gmail.com

[#12]Department of Information Technology
[#12]Kashibai Navale College of Engineering Pune, India

ABSTRACT

The Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is assumed that LS would reveal any information without fees. Therefore the LBS have to ensure that LS's data is not captured by any unauthorized user. During the process of transmission the users should not be allowed to find any meaningful data of their interest for which they have not paid. It is thus essential that solutions be devised that address the security of the users issuing queries, but also prevent users from accessing content to which they do not have authorization. The server likes to have some control over its data.Several problems exist in location based query problem. Among those, two are discussed here. First the user may require a database of a location data and does not want to show their identity to location server , and second is location server does not does not like to distribute its data for all users without paying the fee. Among many challenging barriers to the broad deployment location based query problems, privacy assurance is a major issue. For instance, users may not wish to disclose their locations to the LBS, because it may be possible for a location server to determine who is accomplishing a query by associating these locations with a residential phone book database since users are likely to perform many queries from domestic locations.

Keywords— **Location Server, LBS, PIR**

ARTICLE INFO

Article History

Received :9 th January 2016

Received in revised form :

12th January 2016

Accepted : 13th January , 2016

Published online :

18th January 2016

I. INTRODUCTION

Location-Based Services (LBS) are a generic class of computer program-level services that need location information to manage features. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is available with mobile devices through the mobile network and which uses information on the geological position of the mobile device. This become more and more important with the expansion of the Smartphone and tablet markets as well. Location technologies can be currently used by wireless carrier operators to provide a good estimate of the user position. Significantly more precise positioning is obtained by global positioning system technology which is already integrated in some mobile phones, and it is likely to become a common feature of mass product phones. Considering that mobile phones are rapidly evolving into multipurpose devices that can access a wide range of services, there is a general concern about how positioning information is stored, managed and released to possibly untrusted service providers. There are several privacy issues involved in accessing location-based services, i.e., services that, based on the user current position, can provide location-aware information. LBS include services to identify a location of a person or object, such as discovering the nearest ATM or the ware house of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. Location privacy is a specific type of information secrecy that is characterized as the ability to prevent other parties from learning one's current or past location. The Location Server, which offers some LBS, spends its resources to compile information about

various positions. Hence, it is expected that the LS would not reveal 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 permitted to find any information for which they have not paid. It was thus crucial that solutions be devised that address the security of the users issuing queries, but also prevent users from accessing content to which they do not have authorization.

II. RELATED WORK

When location systems track users automatically on an ongoing basis, they generate an enormous amount of potentially sensitive information. Privacy of location information is about controlling access to this information. It is not necessary to stop all access, because some applications can use this information to provide useful services. In [1], a privacy-protecting framework based on frequently changing pseudonyms is used, so users avoid being identified by the locations they visit. This framework is further developed by introducing the concept of mix zones and showing how to map the problem of location privacy into that of anonymous communication, this gives us access to an increasing body of theoretical tools from the information-hiding community. In this context, two metrics are developed for measuring location privacy, one based on anonymity sets and the other based on entropy. As the temporal and spatial resolution of the location data generated by this approach is high, location privacy is minimum, even with a relatively large mix zone. Mix-zones are identified as an alternative and complementary approach to spatial cloaking based approach to location privacy protection. Mix-zones break the continuity of location exposure by ensuring that users' movements cannot be traced while they reside in a mix-zone. [2] Illustrate a set of counter measures to make road network mix-zones attack resilient. The vulnerabilities of road network mix-zones are distributed into two classes: one due to the road network characteristics and user mobility, and the other due to the temporal, spatial and semantic association of location queries. For instance, the timing information of users' entry and exit into a mix-zone gives knowledge to launch a timing attack. The non-uniformity in the transitions taken at the road intersection may lead to transition attack. They investigated the required number of users to satisfy the unlink ability property when there are repeated queries over an interval. This needs careful control of how many users are included within the mix-zone, which is challenging to achieve in practice. Solution to privacy protection problem provided in [3][4] includes a formal protection model named k-anonymity and a set of accompanying policies for deployment. A release provides k-anonymity protection if the information for each person contained in the release cannot be distinguished from at least k-1 individuals whose information also appears in the release. It also examines re-identification attacks that can be realized on releases that adhere to k-anonymity unless accompanying policies are respected. The k-anonymity protection model is important because it forms the basis on which the real-world systems known as Data fly, µ-Argus and k-Similar provide guarantees of privacy protection. Composite residuosity Class Problem and its applications to public-key cryptography is investigated in [5][12]. Trapdoor mechanism is proposed and from this mechanism, three encryption schemes such as a trapdoor permutation and two homomorphism probabilistic encryption schemes are introduced. This cryptosystems, based on usual modular arithmetic, are provably secure under appropriate assumptions in the standard model. But it does not provide any proof of security against chosen cipher text attacks. In [5], a framework is proposed to support private location dependent queries, based on the theoretical work on Private Information Retrieval (PIR). It does not require a trusted third party, since privacy is achieved via cryptographic techniques. Compared with other methods, this approach achieves stronger privacy for snapshots of user locations; moreover, it is the first to provide provable privacy guarantees against correlation attacks. This framework is used to implement approximate and exact algorithms for nearest-neighbor search. It optimizes query execution by employing data mining techniques, which identify redundant computations. Contrary to common belief, the experimental results suggest that PIR approaches incur reasonable overhead and are applicable in practice. This method requires the extension of this framework to different types of queries, such as spatial joins. Hashem and Kulik presented a scheme [6] whereby a group of trusted users construct an ad-hoc network and the task of querying the LS is delegated to a single user. This idea is different from the previous works by the fact that there is no single point of failure. If a user that is querying the LS suddenly goes offline, then another candidate can be easily found. However, generating a trusted adhoc network in a real world scenario is not always possible. Speed. Another potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. To overcome these problems, Advanced Encryption Scheme (AES) is proposed here for the encryption of data. Associate symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR [13], to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage. This protocol thus provides protection for both the user and the server. The user is shielded 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 compensated for. In [7], each coordinate of the location is enciphered in the oblivious transfer by ElGamal Encryption scheme. Here, the main disadvantage of ElGamal encryption scheme is the need for randomness, slower speed.

III. LITERATURE SURVEY

On the basis of above survey we compare some mechanisms used for the privacy and Content protection in location base queries.

Title	Author	Conference/Journal	Mechanism	Limitation
1] Privacy-Preserving and Content-Protecting Location Based Queries	Russell Paulet, Md. GolamKaosar, Xun Yi, and Elisa Bertino,	IEEE-2014	Use ElGamal enable private information search scheme for encryption. Hide user privacy and send data to authorized users.	1)It is need randomness 2)slower speed 3)Message expansion by a factor of two takes place during encryption
2"MobiMix"-Protecting location privacy with mix-zones over road networks	B. Palanisamy and L. Liu	IEEE-2011	To protect location privacy of mobile users on mobile network it breaks continuous availability of information. Illustrate a set of counter measures to make road network mix-zones attack resilient.	1)This needs careful control of how many users are held within the mix-zone, which is difficult to achieve in practice.
3] A privacy preserving approach to policy –based content Dissemination	Ning Shang , Mohammed Nabeel, Fedrica Paci, Elisa Bertino	IEEE-2011	Content are enciphered document and delivered to whom those have key Document broadcasting based on access control policy	1)Scalability and optimization issue 2)Need to implement fast linear algebra operation
4] Private Queries in Location Based Services: Anonymizers are not Necessary	Gabriel Ghinita, Panos Kalnis,AliKhoshgozaran, Cyrus Shahabi	IEEE-2009	Existing solutions utilize a trusted anonymizer between the users and the LBS.	users must trust the third party Anonymizer, which is a single point of attack. Privacy is guaranteed only for a single snapshot of user locations.
5)Oblivious Transfer Based on Wireless channel characteristics	Zhuo hao,shang,mao	IEEE-2012	Traditional cryptographic tool based on normally computational assumption which may term invalid to user .	Oblivious transform protocol and its applications are secure in semi-honest manner

Table 1: Comparison methods of privacy preserving and content protecting queries

IV. CONCLUSION

In this paper we have discuss , a novel protocol for location based queries that has major performance improvements with respect to the existing approaches is suggested. The protocol is installed according to two stages, in first user privately determine his/her location within public 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 proposed. The 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 ID and associate symmetric key

REFERENCES

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

[2] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in *Proc. ICDE*, Hannover,
Germany, 2011, pp. 494–505.

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

[4] M. Gruteser and D. Grunwald, "Anonymous usage of locationbased services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. MobiSys*, 2003, pp. 31–42

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

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

[12] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. EUROCRYPT, vol. 1592, Prague, Czech Republic, 1999, pp. 223–238.

[13] 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. 121–132.

[14] Ning shang Mohamed Nabeel, Federica paci, Elisa Bertino ," A privacy preserving Approach to policy – Based Content Dissemination" in IEEE Purdue university ,west Lafayette, Indiana, USA-2010

