A Review of Privacy Preserving LBS: Study of Well-Suited Approaches

Neeta B. Bhongade[#1], Guide Prof. S.B.Sarkar [=2]

Student[1], Professor[2],
Dept. of Computer Engineering, SKN-Sinhgad Institute of Technology and Science, Lonavala, Maharashtra, India[1,2]

Abstract **- Usage of wireless data services with Mobile wireless technologies has experienced tremendous growth in the recent past years. By knowing the location of mobile user, Service Provider can offer more enhanced services and applications to the mobile user. These type of applications and services are called as "Location Based Services". Class of location based services is increasing its popularity across all mobile networks like GSM and CDMA.LBS are an entertainment, information and utility services which are accessed through mobile devices such as smart phones, GPS devices, tablets PCs, and operates through mobile network. All the Current researches in Location Based Services(LBS) highlights the privacy requirements and presents the approaches to meet the requirements. This paper presents a brief survey of the approaches that are well suited to keep users location and content of the server private.**

Keywords**- Location based services, location based query, private information retrieval, oblivious transfer, location privacy .**

I. INTRODUCTION

Since last few decades many research focus on the LBS privacy but still there are many challenges in this era. Privacy is the need for the people and for developers it is the most important feature to keep in mind while developing the applications. The techniques and methodology varies according to the application of location based services. This makes it a great challenge to provide location privacy protection for users of location-based services. To keep ones location confidential Location privacy is mandatory for every user. To provide protection against various privacy threats when using Location based services, several studies have proposed different approaches to protect user's privacy while interacting with potentially untrusted service providers, hence coining the term location privacy. This paper presents the study of the various approaches that are well suited for preserving location privacy and also the approaches that takes the location server's privacy into account are studied.

Location-Based Services (LBS) that take the location information of a user, are expected to be accessible and available from anywhere,anytime. A classification of the most popular services includes[3]:

a) *point-of-interest services*: a user infrequently queries an LBS provider to receive a nearby point of interest.

b) *people-locator services*: a watcher asks the LBS provider for the location of a target

c) *notification-based services*: location based alerts or notifications are sent to a user.

A successful privacy-preserving LBS must provide security and accuracy in query results. For building a privacy-preserving LBS, there are two major challenges: security and accuracy (in k -NN search) [2].In general, the kernel of LBS relies on a k -nearest neighbor (k -NN) search mechanism, since users often ask the questions such as "Where is the nearest petrol pump?" or "Is there any coffee shop around me?." Users need to upload their current locations to the remote servers to activate the LBS. LBS are typically based on a point of interest database(POIs) (where a user queries an LBS provider to receive a nearby point of Interest) . By retrieving the Points Of Interest from the database server, the user can get answers to various location based queries, which include but are not limited to discovering the nearest police station ,ATM machine, gas station, hospital.

II. REVIEW OF RELATED WORK

LBS requires users to share their identity and location with potentially untrusted entities offering such services. The tremendous growth of such location servers has made it difficult rather impossible for the users to verify the authenticity of all servers they are interacting with. Sharing such sensitive information with untrusted servers users' privacy violation. Current solutions for the problem of privately querying the POIs databases in location server focus can be broadly classified into three categories[4]:

Location Cloaking replace the exact location of a user with a cloaking region (CR). To ensure result correctness, the CR must enclose the actual user location. Transformation approaches are based on transforming the query to hide user's location. Private Information Retrieval (PIR) uses a cryptographic protocol to achieve privacy of query . This protocol ensures the query privacy.

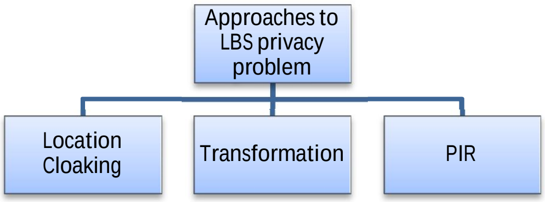

Fig. 1-Approaches to LBS Privacy Problem

A. Evaluation Parameters

Many recent research highlights the importance of privacy preservation in LBSs, and presents solutions that attempt to full fill some or all of the following privacy and security requirements, adopting conventional assumptions in order to reduce or remove the need for trust on system entities (e.g., the LBS provider, the network operator). While many of recent approaches cover aspects of access control and privacy, this paper does not present the thorough review of all the privacy-preservation approaches in LBS services. Current research are evaluated in terms of the parameters[4]: Privacy, Security and Performance

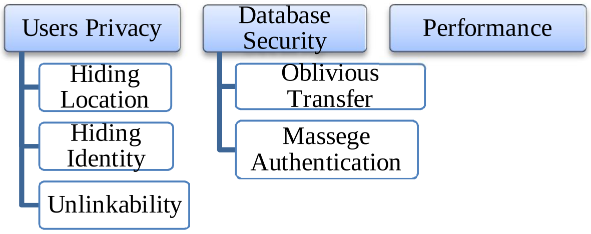

Fig. 2 - Evaluation parameters for LBS

1) User's Privacy Requirements

In order to meet user's privacy requirements LBS services should satisfy some or all of the basic requirements stated here,

Hiding Location: The protocol should not allow the LBS provider to access user's location information . This gives the LBS user a sense of private information retrieval.

Hiding Identity: The LBS provider should not be able to find user's identity, based on the location information received during the user access. That is in general, no unauthorized entity should be able to know the real identity of the user.

Unlink ability: The LBS provider must not be able to link two or more successive users positions. That is in general, no unauthorized entity should be able to link different sessions of the user.

2) Database Security Requirements

In order to protect the POIs Database, LBS services are expected to have following properties,

Oblivious Transfer: User should not be able to obtain more than he is subscribed for or more than the requested information from the LBS provider.

Message Authentication: Messages exchanged between system entities should be authenticated and integrity protected. LBS provider require user authentication in order to prevent service misuse, while users may also require to identify the LBS provider, to protect themselves from spoofing attacks.

B. Review of Location Cloaking approaches

Many of the location cloaking approaches use a trusted location anonymiser .Such type of anonymiser protects user's identity and location from service provider i.e. untrusted location server. Such type of architecture is 3-tier architecture as shown in figure below.K-anonymity approaches[5,6] relies on the concept of hiding the user's location among K-1 neighbors[7-10]. Concept used the idea of sending a locations' box instead of only one i.e. instead of sending user's actual location it hides the user among other in this way decreasing the probability to identify the real location of user to less than 1/K. In most of on K-anonymity techniques [5-10] a middleware (the anonymizer) is used. This anonymizer is a third party responsible for creating a Cloaking Region (CR), which contains the true user's location, as well as K-1 other neighbors. To explain this technique, consider a typical scenario where a user trying to localize the nearest bank. The user sends his requests (including credentials) to the middleware(anonymizer) through a wireless net-work. Then, the anonymizer, which knows the real locations of all current users, perform authentication first so as to authenticate the requester and then chooses a set of K-1 neighbors to create a CR which is then sent to location server instead of the user's position. Since the server is answering the whole CR, this approach reduces the risk of violating user's privacy because it makes it difficult to locate the position actual user who started the process.

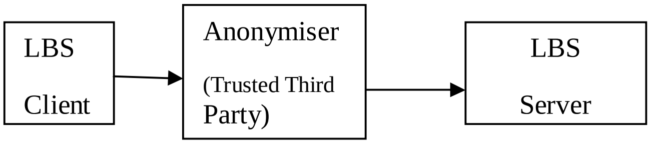

Fig.3-Location Cloaking using anonymizer between user and location server

Drawbacks: Drawbacks of this approach are- Firstly, the anonymizer(third party) have access to the users' data still and thus the user's privacy problem is yet not solved completely. We still can't deny the possibility that the anonymizer can be misused if a malicious hacker gains access to it. Secondly, permanent communication and remote monitoring of the users is required to let the anonymizer update the current location of all the subscribed users repeatedly, which obliviously the violation of the users' privacy. Finally, to perform well these approaches need relatively big number of neighbors at the time of receiving the requests. Therefore, middleware approach could not be considered as a perfect solution to secure location-dependent queries and hence we can say that any secure solution need direct communication between user and the Location Based Server without any intermediately.

C. Review of Transformations Based approaches

This class of approaches is transformation-based approaches [2,16] and do not employ location cloaking and Anonymizers to achieve anonymity. In this class a query is transformed to protect the query content thereby hiding the user's locations.

A study of query evaluation in a transformed space[16] uses space filling curves as one-way transformations to encode the user's location and POI into an encrypted space and to evaluate a query in this transformed space . Space transformation efforts are time-consuming but that are paid only in the initialization phase for building an LBS. The distance properties of the original space are maintained by the transformed space thereby enabling efficient evaluation of location queries. One-way transformation can be viewed as a space encryption scheme. Space-filling curves is a class of curves which traverse through all cells in a 2-D space and do not cross themselves. Hilbert curve is one important member of this class. Hilbert curve has the capability of partially retaining the neighbouring adjacency of the original data. Lots of works have shown that Hilbert curves can achieve the best clustering property. Using connected space-filling curves and hormomorphic cryptosystems , a secure k-NN search protocol, Private Circular Query Protocol (PCQP) is presented[2]. It deals with the security and accuracy challenges. The Moore's version of Hilbert curve (i.e. Moore curve) is used to map POIs from 2-D space into 1-D space. Then secrete circular shift is performed to resolve query in 1-D transformed space.

Drawbacks: Like cloaking approaches, these approaches suffers from several privacy leaks and costly computation or communication overhead if exact results and strict privacy are required.

D. Review of PIR Based approaches

Approach based on the Private Information Retrieval (PIR) scheme [13,14] as well as Grid Cells (GCs) access the POIs database privately.PIR protocol can retrieve a database data without revealing the query content or the identity of the user to the location server. Approach using Grid Cells request a reduced LBS set representing the area of interest to the user. In this approach firstly user(e.g. Alice) ask for the appropriate cells to the server and then anonymously retrieve the data of his/her interest. Some of the issues associated with the above mentioned approaches are solved with this PIR scheme. A mathematical model to minimize the risk of privacy violations in PIR's queries[15] presented a system which enhances LBS exchange protocol and makes communication more secure, regardless of using a TTP server as middleware between the users and the LBS server.

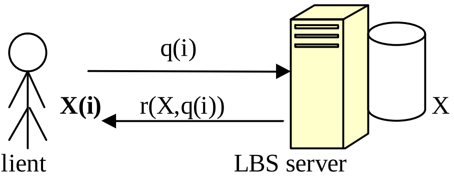

Fig. 5- PIR Based Approach Framework

As an enhancement over the previous approaches using PIR, a two stage approach is presented[1] which uses the Oblivious Transfer protocol in first step and PIR protocol in second step. Thus both the user and the server is protected.. Since server is unable to determine user's location the user is protected .Similarly, the server's contents are protected because a malicious user can decrypt only the block of data obtained by PIR with the encryption key.

Drawbacks: It relies on unguaranteed expectations such as extensive data processing at the user's side and also incurs more computation and communication overhead. In most cases, the user is submitting the request through a mobile phone that has very limited processing capabilities.

III. EVALUATION AND SUMMARY OF RELATED WORK

Cloaking approach hides a user inside a cloaking region (CR), typically of rectangular shape. For correctness, the CR must enclose the actual user location and also must satisfy certain constraints dictated by a privacy theory, which clears the privacy requirements of the user. Query processing is done with respect to a rectangular region, regardless of the method used to generate the CR,as opposed to an exact user location. LS returns the result as a super-set of the actual query result. All previous work using above techniques evaluates these location privacy techniques based on two measure user's privacy and performance.

However, third and equally important dimension to evaluate private location queries techniques is database security(i.e. the amount of protection provided to the database). It is must to control tightly the amount of POI disclosure. This methods operate under a strong constraints(set of assumptions), but relatively are more efficient in terms of computational and communication overhead.

In Transformation-based approaches algorithms(KNN) presented are approximate although it is shown that the amount of approximation is quite satisfactory. The PIR approaches guarantees privacy, for both one-time, as well as continuous (i.e., repetitive) queries.

Approach ⇩	**Evaluation parameters** ⇨	**Hiding Identity**	**Hiding Location**	**Unlink ability**	**Oblivious transfer**	**Examples from Literatures surveyed**
Location cloaking		X	√	X	X	M. Gruteser and D. Grunwald,2003 C. Y. Chow, M. F. Mokbel and X. Liu,2006 B. Gedik and L. Liu,2005
Transformation		X	√	√	X	Khoshgozaran A. and Shahabi,2007 Ting Lien, Yu-Hsun Lin,2013
PIR Protocol		X	√	√	√	Ghinita, Kalnis,Khoshgozaran,Shahabi,2008 D. Rebollo-Monedero and J. Forne,2010

Fig. 6- LBS privacy approaches and their properties

Furthermore, PIR does not require trusted third party component(TTP). Cryptographic elements in PIR requires powerful computational resources (e.g., parallel machines), communication channels and high-bandwidth.

IV. CONCLUSION

This paper presents a survey report of different well-suited privacy approaches in location based services. Three distinct classes of approaches for protecting users' location information in LBS are studied. First class is of approaches based on location cloaking /anonymity technique .It offers flexible schemes supporting privacy-aware location servers responding to various queries. But it suffers from privacy leaks problem. The second class of approaches are based on transformation. It transforms the queries to blind the server from reading the user's location while evaluating user query.The third and last class is of PIR approaches which addresses all the privacy concerns of previous approaches but incur expensive computations .

REFERENCES

[1] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, Fellow, IEEE," *Privacy-Preserving and Content-Protecting Location Based Queries*",IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 5, May 2014

[2] Ting Lien, Yu-Hsun Lin, Student Member, IEEE, Jyh-Ren Shieh, and Ja-Ling Wu, Fellow, IEEE,"*Novel Privacy Preserving Location-Based Service Protocol With Secret Circular Shift For k-nn Search",* IEEE Transactions On Information Forensics And Security, Vol. 8, No. 6, June 2013

[3] Emmanouil Magkos ,"*Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey",*IJITSA

[4] Gabriel Ghinita, Panos Kalnis, Murat Kantarcioglu, and Elisa Bertino1," A Hybrid Technique for Private Location-Based Queries with Database Protection",2009.

[5] M. Gruteser and D. Grunwald, "*Anonymous Usage of Lo- cation-Based Services through Spatial and Temporal Cloak-ing,"* Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, San Francisco, 5-8 May 2003, pp. 31-42.

[6] C. Y. Chow, M. F. Mokbel and X. Liu, "*A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location- Based Services,"* Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic In-formation Systems, Arlington, 10-11 November 2006, pp. 171-178.

[7] B. Gedik and L. Liu, "*Location Privacy in Mobile Sys-tems a Personalized Anonymization Model,"* Proceedings of the 25th International Conference on Distributed Com- puting System of the IEEE ICDCS, Columbus, 10 June 2005, pp. 620-629.

[8] M. F. Mokbel, C. Y. Chow and W. G. Aref, "*The New Cas-per: Query Processing for Location Services without Compromising Privacy,"* Proceedings of the VLDB 2006, Seoul, 12-15 September 2006, pp. 763-774.

[9] D. Reid, "*An Algorithm for Tracking Multiple Targets,"* IEEE Transactions on Automatic Control, Vol. 24, No. 6, 1979, pp. 843-854.

[10] B. Gedik and L. Liu, "*A Customizable k-Anonymity Mo- del for Protecting Location Privacy*," Technical Report, Georgia Institute of Technology, Atlanta, 2004.

[11] H. Kido, Y. Yanagisawa and T. Satoh, "*An Anonymous Communication Technique Using Dummies for Location- Based Services,*" Proceedings of the International Conference on Pervasive Services of the IEEE ICPS 05, San-torini, 11-14 July 2005, pp. 88-97.

[12] T. You, W. Peng and W. Lee, "*Protect Moving Trajectories with Dummies,"* Proceedings of the International Conference on Mobile Data Management, Mannheim, 1 May 2007, pp. 278-282.

[13] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi and K.-L. Tan, *"Private Queries in Location-Based Services: Anonymizers Are Not Necessary*," Proceedings of the SIGMOD 08, Vancouver, 9-12 June 2008, pp. 121-132.

[14] C. Gentry and Z. Ramzan, "*Single-Database Private Information Retrieval with Constant Communication Rate,"* Proceedings of the 32nd International Colloquium on Automata, Languages and Programming, Lisboa, 11-15 July 2005, pp. 803-815.

[15] D. Rebollo-Monedero and J. Forne, "*Optimized Query Forgery for Private Information Retrieval,*" IEEE Trans-actions on Information Theory, Vol. 56, No. 9, 2010, pp. 4631-4642.

[16] Khoshgozaran A. and Shahabi, C. (2007) '*Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy*', SSTD, pp.239–257.

[17] Ali Khoshgozaran and Cyrus Shahabi," *A taxonomy of approaches to preserve location*
privacy in location-based services", Int. J. Computational Science and Engineering, Vol. 5, No. 2, 2010