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

A Location Based Queries for Securing Content and Assuring Privacy

R.Tejaswi
M.Tech Student
Department of CSE
B V Raju Institute of Technology
Narsapur, India.

Mr.V.Pradeep Kumar
Assistant Professor
Department of CSE
B V Raju Institute of Technology
Narsapur, 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.

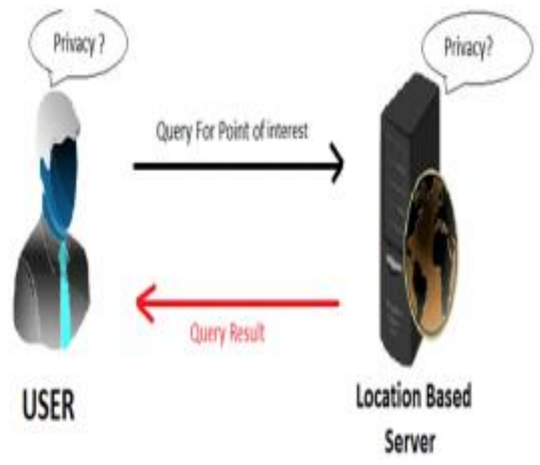


Fig - Location Based Service

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

Preserving techniques and Methods:

There was work proposed in year 1999 that enable a user to access k replicated copies of a database and privately retrieve information stored in the database [6]. This means that each individual server (holding a replicated copy of the database) gets no information on the identity of the item retrieved by the user. This schemes and similar works, proposed very earlier use the replication to gain full real saving with multi-server. In particular, it's presenting a two-server scheme with less communication complexity.

Then as work progress, there was application of the anonymity set technique to location data collected. The anonymity set measurements gives information that pseudonymity technique cannot give users adequate location privacy. However, positive thing made was if one is in the mix zone with 20 other people, it might consider better protected. But when one go in and out of the mix zone the observer will strongly suspect are those lonely pseudonym [3]. This motivated further work on it.

Anonymity had instinctively described as the property of being indistinguishable among a set of individuals. This provides privacy in more efficient way, safeguarding private information of the user. However, guaranteeing anonymous usage of location-based services requires transmission of location information by a user that cannot be easily used to re- identify the subject. The paper "Anonymous usage of location based services through Spatial and temporal cloaking" in year 2003 found middleware architecture and algorithms that can be used by a centralized location broker service. This adaptive algorithm adjusts the resolution of location information along spatial or temporal dimensions to meet specified anonymity constraints, which are based on the entities using location services within a given area [11]. The application of this technique in effective way, it requires location-based services that are used with precise position information by a large user base. It analyzed the technical feasibility of unknown usage of location-based services and properly studied the location data introduces new and potentially more severe privacy risks than in conventional services.

Anonymity and pseudonymity again are not a complete answer to privacy. Moreover, it presents a barrier to authentication and personalization and also vulnerable to data mining, since there is possibility of getting location hence revealing identity often.

Thus, there was the argument that obfuscation is complementary to that times existing privacy protection strategies and demands further investigation. The paper proposed on "A formal model of obfuscation and negotiation" [8]. In this Obfuscation is defined as the means degrading in carefully way the quality of information about an individual's location in order to protect that individual's location privacy. Key assumptions made by architecture are: A client device uses some combination of location-sensing techniques to provide accurate information about the client's location. That client device can be able to communicate with a third-party location based service provider (TPLBSP) via a wireless network. So some information service based on the client's current location is received. The information chosen to reveal about clients' location contains only source of information available to the TPLBSP about that location.

Obfuscation thus became an essential component of an overall approach to location privacy then. It provides a framework for the provision of high quality location-based services based on low quality location information. This model includes algorithms able to achieve a proper balance between privacy and location-based service utility properly.

Along with this, methods such as path confusion or using dummies were implements. Dummy variable thus help in hiding location thus providing users' privacy. Further discussion on devices like computers and other devices are not only used for requesting location. Moving devices like mobile also came in frame working on topic. Mobile devices equipped with positioning capabilities (e.g. GPS) can ask location-dependent queries to Location Based Services (LBS) [10]. To protect privacy, the user location must not be disclosed. Existing solutions before this has utilize a trusted anonymizer between the users and the LBS.

The approach has several drawbacks:
(i) All users must trust the third party anonymizer, which is a single point of attack.
(ii) A large number of cooperating, trustworthy users is needed.
(iii) Privacy is guaranteed only for a single snapshot of user locations; users are not protected against correlation attacks.

So again overcome above problem, new propose of novel framework to support private location dependent queries, based on the theoretical work on Private Information Retrieval (PIR) [9]. This framework does not require a trusted third party; instead it made use cryptographic techniques for privacy. Compared to existing work, this approach achieves stronger privacy for snapshots of user locations; moreover, provide provable privacy guarantees against correlation attacks. In this work implement involved approximate and exact algorithms for nearest-neighbor search. Also optimize query execution performed in by employing data mining techniques. The experimental results suggest that PIR approaches incur reasonable overhead and are applicable in practice. This work was first to provide a practical PIR implementation with optimizations that achieve communication and CPU cost as well as to protect against correlation attacks compared to previous work. In the future, plans to investigate the extension of this framework to different types of queries.

Also other contributions in privacy preserving by defining location-based quasi-identifiers and by introducing the notion of Historical k-anonymity [4], some of the research work provide a formal framework to evaluate the risk of revealing personal sensitive location information. It proposes a technique to preserve a specified level of anonymity, and identify several evolving research directions on this topic.

Existing privacy-enhancing techniques protect user identities. Nevertheless, the query contents may disclose the physical location of the user. Hence, new presentation of a framework for preventing location-based identity inference of users who issue spatial queries to location-based services. It proposes transformations based on the well-established K-anonymity concept to compute exact answers for range and nearest-neighbor search, without revealing the query source. The methods optimize the entire process of anonymizing the requests and processing the transformed spatial queries.

There were again implementations of two other approaches in working on it. The first one, referred as Naive [2], assumes the location updates made a service user are independent to each other. For each location update, Naive just finds a cloaking box and reports it as the service user's location in her service request. The second approach is referred to as Plain. This scheme determines the cloaking set for the service users by finding the footprints closest to users' start position. After fixing the cloaking set, algorithm is applied to compute the cloaking boxes for the user to know during entire service session.

In middle there is theory that present a single-database private information retrieval (PIR) scheme with communication complexity O(k+d), where $k \geq \log n$ is a security parameter that depends on the database size n and d is the bit-length of the retrieved database block [2]. This communication complexity is better one than earlier single-database PIR schemes. The scheme also provided improved performance for practical parameter settings whether whatever is size of block.

Previously work focused on finding good trade-offs between privacy and performance of user protection techniques. The approaches to protect based on hiding locations inside cloaking regions (CRs) and encrypting location data via PIR protocols. Further, contribution of this work has the approach that proposed (i) a cryptographic protocol which allows private evaluation. They use this protocol as a building block in determining the nearest POI to a given user location. It could adapt to other types of spatial queries easily. (ii) Development of a hybrid approach that efficiently supports PIR processing with respect to a user-generated cloaked region Q. The proposed method controls CRs as well as disclosed POI information. Furthermore, it proved more efficient than its PIR-only [12].

The paper then proposed a hybrid technique for private location-based queries which provides protection for both the users and the service provider. It was then first work to consider the protection of the POI database. Even further working carried on with protocol.

An alternative and complementary approach to spatial cloaking based location privacy protection is to break the continuity of location exposure by introducing techniques, such as mix-zones. The aim of the mix zone model was to prevent tracking of long-term user movements, but still permit the operation of many short-term location-aware applications. Mix- zones anonymize user identity by restricting the positions where users can be located [3]. Presenting on this a model MobiMix is framework for building mix-zones on road networks. It is used for protecting the location privacy of mobile clients.

One of the methods is new metrics to measure users' query privacy considering user profiles. It computes regions expressed in terms of metrics using design spatial generalisation algorithm. The extend k-anonymity that it propose new metrics to correctly measure users' query privacy in the context of LBSs [5], which enable users to specify their query privacy requirements in different ways. The main idea of k-anonymity is to guarantee that a database entry's identifier is indistinguishable from other k−1 entries. Further by knowing concept deeper, k-anonymity reveals its drawbacks in preserving. Based on the analysis, they conclude that cloaking (e.g., k-anonymity) is effective for protecting query privacy but not location privacy focus on protecting query privacy using cloaking with the assumption that the opponent learns users' real-time locations. The illustration with the features of different metrics gives a better protection than k-anonymity to users. We consider a powerful attacker who can obtain user profiles and has access to users' real-time positions in the context of LBSs.

The concept of answering location-related information for encrypted positions became better and promises to improve security needs. Indeed, such a mechanism can strongly attract the attention of researchers as it supports the preservation of the users' privacy. Further working developed a novel fully secure location-based mechanism based on a homomorphic encryption scheme. It described the circuits that allow a LBS server to process encrypted inputs to retrieve targeted records that match the user's request.

This work model presents and describes protocol. It analyses the security performance and efficiency of the protocol with working using two platforms: a desktop and a mobile. The ultimate goal here was to obtain records from the LS and maintain privacy at users' and server. It is by applying an approach of oblivious transfer. It uses public grid to obtain record. The analysis is concern with the security of the client and the server both.

In recent year, paper proposed a novel protocol for location based queries that have major performance improvements with respect to the approach by Ghinita at el. This protocol is organized according to two stages. In the first stage, the user privately gets its 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. And then in 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. This protocol thus provides protection in both ways. The user is protected because the server is unable to determine the 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. The working implementation demonstrates the efficiency and practicality of the new approach.

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.

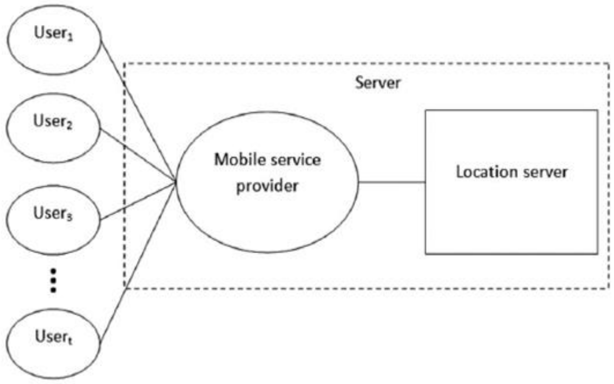
Our protocol thus provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired 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:



Modules

1. User
2. Oblivious Transfer Phase
3. Private Information Retrieval Phase
4. Location Server

User

The ultimate goal of our protocol is to obtain a set (block) of POI records from the LS, which are close to the user's position, without compromising the privacy of the user or the data stored at the server. We achieve this by applying a two stage approach shown in fig. The first stage is based on a two-dimensional oblivious transfer and the second stage is based on a communicationally efficient PIR.

The oblivious transfer based protocol is used by the user to obtain the cell ID, where the user is located, and the corresponding symmetric key. The knowledge of the cell ID and the symmetric key is then used in the PIR based protocol to obtain and decrypt the location data. The user determines his/her location within a publicly generated grid P by using his/her GPS coordinates and forms an oblivious transfer query. The minimum dimensions of the public grid are defined by the server and are made available to all users of the system.

Oblivious Transfer Phase

The purpose of this protocol is for the user to obtain one and only one record from the cell in the public grid P, We achieve this by constructing a 2-dimensional oblivious transfer, based on the ElGamal oblivious transfer, using adaptive oblivious transfer proposed by Naoret al. We remark that this key structure of this form is an enhancement from, as the client doesn't have access to the individual components of the key.

Private Information Retrieval Phase

With the knowledge about which cells are contained in the private grid, and the knowledge of the key that encrypts the data in the cell, the user can initiate a private information retrieval protocol with the location server to acquire the encrypted POI data. Assuming the server has initialized the integer e, the user ui and LS can engage in the following private information retrieval protocol using the IDQi,j , obtained from the execution of the previous protocol, as input. The IDQi,j allows the user to choose the associated prime number power πi, which in turn allows the user to query the server.

Location Server

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.

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