Location Based Queries for Protecting Data with High SecurityUsing PIR Protocol

[1] TULLIMILLI SIVA PRASAD, [2] T. SUBBA REDDY

[1]M. Tech Student, Department of CSE ,Nalanda Institute Of Engineering and Technology, Kantepudi Village, Sattenapalli Mandal. Guntur Dist, Andhra Pradesh, India.

[2] Assistant Professor, Department of CSE ,Nalanda Institute Of Engineering and Technology, Kantepudi Village, Sattenapalli Mandal. Guntur Dist, Andhra Pradesh, India.

ABSTRACT- Privacy based Context-aware systems based on location open up new possibilities to users and data servers in terms of acquiring custom services by gathering context information, especially in systems where the high mobility of users increases their usability. Location-based applications utilize the positioning capabilities of a mobile device to determine the current location of a user, and customize query results to include neighbouring points of interests. However, location knowledge is often perceived as personal information. One of the immediate issues hindering the wide acceptance of location-based applications is the lack of appropriate methodologies that offer fine grain privacy controls to a user without vastly affecting the usability of the service**.**In this paper, novel approach is proposed as a solution to one of the location-based query problems through Privacy preserving based Context Reputation System. The Solution of the System is as Follows, a user wants to query a database of location data, known as Points of Interest (POIs) with respect of protecting their location Information against data leakage. Similarly 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, hence security mechanism named as shared Authority is employed against data sharing also data is reputed based on the reputation mechanism . The solution is efficient and practical in many scenarios. By implementing the solution, it is possible to access the efficiency of the protocol and proposed introducing a security model and analysing the security and reputation of the context of protocol will improve the performance of the system.

1. INTRODUCTION

Location Based Services (LBSs), also known as location dependent information services (LDISs), have been recognized as an important context-aware application in pervasive computing environments. Spatial queries are one of the most important LBSs. According to spatial constraints, spatial queries can be divided into several categories including nearest neighbor (NN) queries and window queries. An NN query is to find the nearest data object with respect to the location at which the query is issued (referred to as the query location of the NN query). For example, a user may launch an NN query like “show the nearest coffee shop with respect to my current location.” On the other hand, a window query is to find all the objects within a specific window frame. An example window query is “show all restaurants in my car navigation window.” In general, a mobile client continuously launches spatial queries until the client obtains a satisfactory answer. For example, a query “show me the rate of the nearest hotel with respect tomy current location” is continuously submitted in a moving car so as to find a desired hotel. The naive method answering continuous spatial queries is to submit a new query whenever the query location changes. The naive method is able to provide correct results, but it poses the following problems: High power consumption. The power consumption of a mobile device is high since the mobile device keeps submitting queries to the LBS server. Heavy server load. A continuous query usually consists of a number of queries to the LBS server, thereby increasing the load on the LBS server. Fortunately, in the real world, the queries of a

continuous query usually exhibit spatial locality. Thus, caching the query result and the corresponding valid region (VR) in the client side cache was proposed to mitigate the above problems. The valid region, also known as the valid scope, of a query is the region where the answer of the query remains valid. Subsequent queries can be avoided as long as the client is in the valid region. In this paper, we focus on the efficient processing of location dependent queries and, in particular, a sub-class of queries called mobile nearest-neighbor (NN) search. A mobile NN search is issued by a mobile client to retrieve stationary service objects nearest to its user.1 It is an important function for LBSs, but the implementation is difficult since the clients are mobile and queries must be answered based on the clients' current locations. If a client keeps moving after it issued a query, the query result would continue to change in accordance with the client's movement. As such, it is difficult to obtain results which are accurate with respect to the position pat which the user receives them. Despite the fact that LBSs open up new research opportunities, most of the on-going research work still concentrates on traditional queries which return answers independent to the locations of the query issuers. In other words, each data object has only one set of attribute values in the server. If a client caches a local copy of the data to improve performance, the cached data become invalid only when the corresponding copy in the server is updated. As for location-dependent queries, a data object usually has multiple sets of attribute values, each of which is valid only when the client is located within a specific region. While mobile data caching and invalidation for locationindependent queries has been actively pursued in the mobile computing research community, very few work had been done on indexing and query processing techniques for location-dependent queries.

2. RELATED WORK

M. Bellare and S. Micali. They are proposed an client and fair proto col for secure two-party computation in the Optimistic model, in which a partially trusted 3rd party T is available, but not in volved in normal executions of protocol. T is required only if there exist disruption in communication or if one Of the two parties denies or misbehaves. This protocol ensures that even if one party terminates the protocol at any of the time, the computation is still fair for the second party Communication is over an asynchronous network. All protocols we are using are based on client proofs of knowledge and involve no general zero-knowledge to ols as intermediate steps we describe e±cien tveriØ- able oblivious transfer.

A. Beresford and F. Stajano they are proposed an As location-aware applications begin to track our movements in the name of convenience, how can we protect our rivacy? This article introduces the mix zone-a new construction inspired by anonymous communication techniques-together with metrics for assessing anonymity of an user which is based on pseudonyms which are frequently changing.

C. Bettini, X. Wang, and S. Jajodia They proposed an manuscript & we present a solution to one of the location predicated query quandaries. This quandary is defined as follows: (i) a utilizer wants to query a database of location data, kenned as Points Of Interest (POIs) and does not optate to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not optate to simply distribute its data to all the users. Here the location server wishes to have some control over its data, since the data is its asset. We recommend a major enhancement upon anterior solutions by introducing a two stage approach, where the first step is predicated on Oblivious Transfer and the second step is predicated on Private Information Retrieval (PIR), so as to achieve a secured solution for both the parties. The solution which we present is quite efficient and more practical in many of the scenarios. We then implement our solution onto a desktop machine and a mobile contrivance to assess the efficiency of our protocol. We additionally introduce a security model and analyze the security in the context of our protocol. Finally, we highlight a security impotency of our an tecedent work and present a solution to surmount it.

X. Chen and J. Pang They proposed an Vehicular networks are envisioned to play an important role in the building of

intelligent transportation systems. However, the dangers of the wireless transmission of potentially exploitable information such as detailed locations are often overlooked or only inadequately addressed in field operational tests or efforts of standardization. The main reasons for this is that the concept of privacy is difficult to quantify. While vehicular network algorithms are usually evaluated by means of simulation, it is a non-trivial task to assess the performance of a privacy protection mechanism. In this paper we discuss the principles, all the challenges, and also the necessary steps in terms of privacy assessment in vehicular N/Ws. We also identify all useful and the practical metrics that allow the comparison and evaluation of privacy protection algo's. We hereby present a very systematic literature review that sheds light on the current state of the art and give recommendations for future research directions in the field.

B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan the proposed a survey the notion of Single-Database Private Information Retrieval (PIR). The first Single-Database PIR was constructed in 1997 by Kushile vitz and Ostrovsky and since then Single-Database PIR has emerged as an important primitives of cryptography. For ex., Single-Dbase PIR turned out to be intimately connected to collisionresistant hash functions, the oblivious transfer and also public-key encryptions with some additional properties. Here in this survey, we state an overview of many of the constructions for Single-Database PIR (including an abstract construction based upon homomorphic encryption) and describe some of the connections of PIR to other primitives.

T. ElGamal proposed A new signature scheme, together with the implementation of the Diffie-Hellman public key distribution scheme that achieves a public key cryptosystems. The secureness of the both systems relies on the difficulty of computing discrete logarithms over finite fields.

B. Gedik and L. Liu they are proposed a solution to one of the location predicated query quandaries. This quandary is defined as follows: (i) a utilizer wants to query a database of location data, kenned as Points Of Interest (POIs) and does not optate to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not optate to simply distribute its data to all the users. Here the location server wishes to have some control over its data, since the data is its asset. We recommend a major enhancement upon anterior solutions by introducing a two stage approach, where the first step is predicated on Oblivious Transfer and the second step is predicated on Private Information Retrieval, so as to achieve a very secure solution for both the parties. The solution which we present is too efficient and practical in most of the scenarios. We then implement our solution to/on a desktop machine and a mobile contrivance to assess the efficiency of our protocol. We additionally introduce a security model and analyze the security in the context of our protocol. Finally, we highlight a security impotency of our an tecedent work and present a solution to surmount it.

C. Gentry and Z. Ramzan the are proposed an 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 of users. When we get done with exchange of location information 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. Mobile devices with global positioning capabilities allow users to retrieve points of interest (POI) in their proximity area. To protect the user privacy, its important not to disclose exact user coordinates to un-trusted entities that provide location-based services. Currently, there are two main approaches to protect the location privacy of users: (i) hiding locations inside cloaking regions

3. FRAMEWORK

Existing work contains two protocols particularly oblivious transfer part and personal data retrieval .First user publically determines his location victimization GPS coordinates then he determines non-public location in an exceedingly public grid victimization oblivious transfer .After obtaining cell id and related interchangeable key from

server, user fires question victimization PIR .

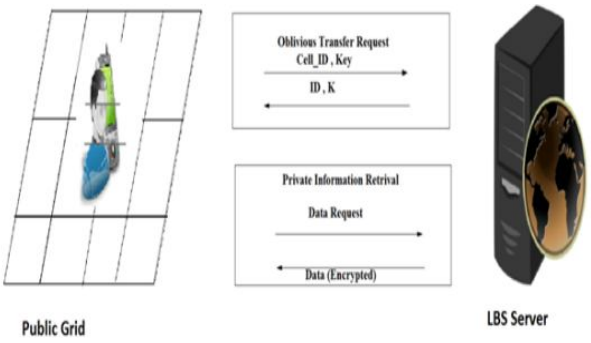


Fig. 3 Privately determine User for LBS Communication

protocol and find correct block from information that he needs. Here there's assurance of privacy each for user and server. By learning on top of analysis works by scholar we have a tendency to are going to enhance this method. as a result of on every occasion user desires to determine his location and per that he fires question to the server. thus there ar spare steps to done to amass block of knowledge from information server. So we have a tendency to ar progressing to propose system with range of users in same public grid or region can acquire information mistreatment a single purpose. In existing system, user question to server for his NN, then server challenge dish concerning to its location. Here we 've taken under consideration an idea of centroid i.e. during a explicit region, there ar range of unknown users use location based mostly services. thus for each user, he needs to verify his location and send it to server. So we decided that we are able to create single purpose within the region for communication with server .So there\'s no have to be compelled to each user to determine its region all the time.

The idea of centre of mass is totally different than previous existing systems. Here we have a tendency to assume that, all the users in a public grid renowned to every alternative i.e. they're trusty with each other. Then one in all the teams from the general public grid will make a centre of mass purpose for communication with server as a result of they have a trust on one another. thus one in all the trusty user in the cluster gain locations of alternative user and create a centre of mass point.

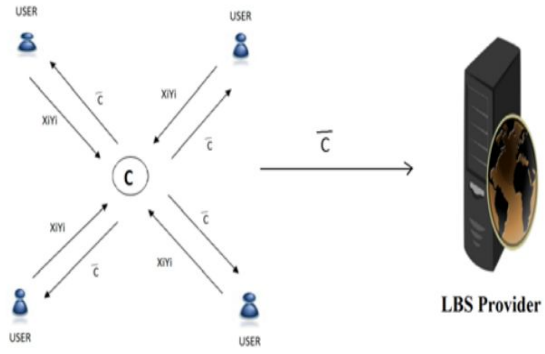


Fig. 4 LBS Services Using Centroid

After computing the centre of mass, user sends it to any or all his companion and LBS supplier. thus actual position of the user and his companions remains hidden. By obtaining centre of mass all the users fires the question regarding thereto centre purpose. Here we have a tendency to cannot search nearest neighbors question .But user will access information from server from their real location and LBS server wouldn't recognize actual position of user and it'll send information to centre of mass. One advantage therein is we are able to take restricted range of users from a public grid. All the users ar trusty and known to every alternative. thus privacy is will increase. conjointly we have a tendency to are going to enhance this by masking the locations of user and their companions whereas creating a centre of mass.

A. System Model:

The framework model comprises of three sorts of substances (see Fig. 1): the arrangement of users1 who wish to get to area information U, a versatile administration supplier SP, and an area server LS. From the perspective of a client, the SP and LS will create a server, which will serve both capacities. The client does not should be concerned with the specifics of the correspondence.

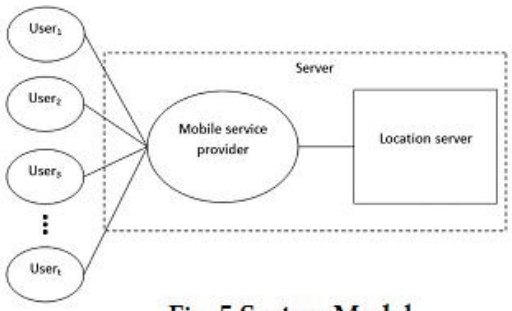


Fig. 5 System Model

The clients in our model utilize some area based

administration given by the area server LS. Case in point, what is the closest ATM or eatery? The motivation behind the versatile administration supplier SP is to build up and keep up the correspondence between the area server and the client. The area server LS claims an arrangement of POI records ri for $1 \leq ri \leq \rho$.

B. Protocol Description:

Protocol Summary: 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 . 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 query2. The minimum dimensions of the public grid are defined by the server and are made available to all users of the system. This public grid superimposes over the privately partitioned grid generated by the location server's POI records, such that for each cell Qi,j in the server's partition there is at least one Pi,j cell from the public grid.

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.

Client's Security: Fundamentally, the information that is most valuable to the user is his/her location. This location is mapped to a cell Pi,j. In both phases of our protocol, the oblivious transfer based protocol and the private information retrieval based protocol, the server must not be able to distinguish two queries of the client from each other.

Server's Security: Intuitively, the server's security requires that the client can retrieve one record only in each query to the server, and the server must not disclose other records to the client in the response. Our protocol achieves the server's security in the oblivious transfer phase, which is built on the Naor-Pinkas oblivious transfer protocol.

4. EXPERIMENTAL RESULTS

Performance Analysis:

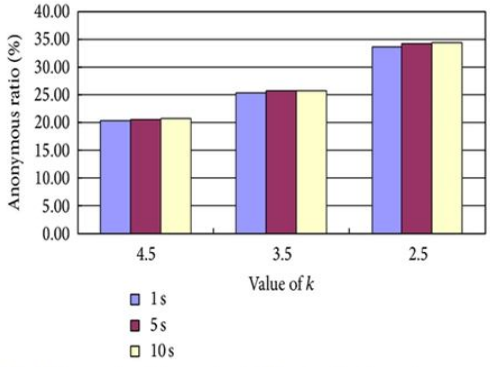
When we are performing operations on our application we have taken the values like below table

TABLE 1

Average service delay request (second)	Average location precision (mile)	Request amount	Average spatial request (k_s)	Average temporal request (k_t)	Minimum radius R_{min} in average anonymous area (mile)	Maximum radius R_{max} in average anonymous area (mile)
1	50.03	466034	4.49	4.50	274.94	637.11
1	50.04	503432	3.50	3.50	275.43	637.43
1	50.08	453293	2.50	2.50	275.10	636.67
5	50.06	457712	4.50	4.50	275.08	637.25
5	49.98	446796	3.50	3.50	275.19	636.99
5	50.01	442778	2.50	2.50	275.12	637.86
10	50.08	456924	4.50	4.50	274.79	637.74
10	49.93	697428	3.50	3.49	275.01	637.54
10	49.98	681940	2.50	2.49	274.84	637.43
10	50.00	493648	2.50	2.50	525.21	1263.51
10	49.97	455932	2.49	2.50	774.50	1387.06
20	49.97	448366	2.50	2.51	275.27	637.64
30	50.03	472418	2.50	2.50	275.37	637.87

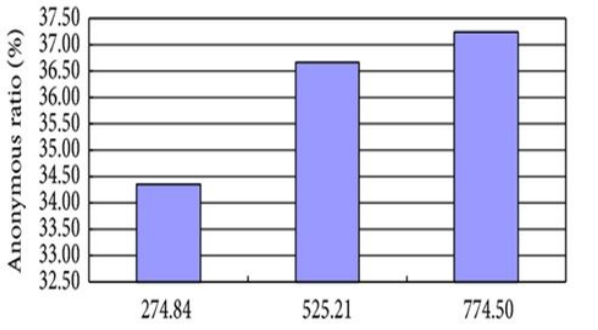
As per the table values the resultant graphs will be like below

i) ratio of the temporal-spatial anonymity with different waiting time and average anonymous request.



Ratio of the temporal-spatial anonymity with different waiting time and average anonymous request.

ii) ratio of the temporal-spatial anonymity with different anonymous space requests.



Ratio of the temporal-spatial anonymity with different anonymous space requests

5. CONCLUSION

In this paper we given a location based mostly question solution that employs two protocols that allows a user to privately verify and acquire location information. the primary step is for a user to in private verify his/her location victimization oblivious transfer on a public grid. The second step involves a private data retrieval interaction that retrieves the record with high communication potency. Authors analyzed the performance of protocol and located it to be each computationally and communicationally additional economical than the solution by Ghinita et al., that is that the most up-to-date solution. Authors enforced a software system epitome employing a desktop machine and a mobile device. The software system prototype demonstrates that protocol is inside sensible limits. Future work can involve testing the protocol on several different mobile devices. The mobile result that authors provide could also be totally different than alternative mobile devices and software environments. additionally there's ought to cut back the overhead of the property check utilized in the non-public data retrieval based mostly protocol.

REFERENCES

[1] (2011, Jul. 7) Openssl [Online]. Available: http://www.openssl.org/.

[2] M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” in Proc. CRYPTO, 1990, pp. 547–557.

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

[4] 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. 185–199, LNCS 3674.

[5] X. Chen and J. Pang, “Measuring query privacy in location-based services,” in Proc. 2nd ACM CODASPY, San Antonio, TX, USA,2012, pp. 49–60.

[6] Mokbel, M.F., C.Y. Chow and W.G. Aref, “The New Casper: A Privacy-aware Location-based Database Server”, in IEEE 23rd International Conference on Data Engineering, ICDE 2007, IEEE, 2007.

[7] Ghinita, G., P. Kalnis and S. Skiadopoulos, "PRIVE: Anonymous Location-based Queries in Distributed Mobile Systems", in Proceedings of the 16th international conference on World Wide Web, ACM, 2007.

[8] Chow, C.Y., M.F. Mokbel and X. Liu, “Spatial Cloaking for Anonymous Location-Based Services in Mobile Peer-to-Peer Environments”, GeoInformatica, vol. 15, No. 2, pp. 351-380, 2011.

[9] Bamba, B., et al. “Supporting Anonymous Location Queries in Mobile Environments with Privacy grid”, in Proceedings of the 17th International Conference on World Wide Web, ACM, 2008.

[10]Gao Rui, Wang Wenjun, et al. "Privacy Preserving Traffic Speed Estimation via Mobile Probe", International Journal of Digital Content Technology and its Applications, vol. 6, no.1, pp.446-453, 2012.