INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 5, Issue 2 DEC 2015

PIR PROTOCOL USED IN LOCATION BASED QUERIES FOR PROTECTING DATA WITH HIGH SECURITY

[1] K. SUBRAMANYAM, [2] MR. LAKSHMIKANTH

[1]M.Tech Student, Department of CSE.

sai.kavvala@gmail.com

[2] Associate Professor, Department of CSE.

svlakshmikanth@gmail.com

ABSTRACT— ***Location-Based Services (LBS) are a common category of pc program-level services that use location information to manage features. As such, LBS are a vice. This has become a lot of and a lot of necessary with the growth of the data service and contains a number of uses in social networking these days as a recreation service, that is accessible with mobile devices through the mobile network & that uses info on the geographical position of the mobile DE smartphone and medication markets further. LBS embrace parcel following and vehicle following services. LBS will grip mobile commerce once taking the shape of coupons or promotion directed at customers supported their current location. The Location Server (LS), that provides some LBS, resources to compile information concerning varied attention-grabbing POIs. Hence, it's expected that the LS wouldn't reveal any info while not fees. Therefore, The LBS need to make sure that any unauthorized user doesn't access LS's data. Thus, we tend to develop a protocol to realize user and server facet privacy. Victimization oblivious transfer and PIR (Private Info Retrieval) protocols, we tend to succeed secure answer for each parties. we providea new constructions of message authentication schemes supported a cryptological hash operate. Our approaches, NMAC and HMAC, ar evidenced secure as long because the fundamental hash operate has some affordable cryptological strength. Furthermore, we show, in a very quantitative approach, that the schemes retain most the security of the underlying hash operate. additionally, our schemes are efficient and reasonable.***

1. INTRODUCTION

There square measure increasing mobile users worldwide. So location technologies will be presently utilized by wireless carrier operators to produce an honest forecast of the user location. Now a days, variety of users square measure use location primarily based services which may give location-aware data. What is Location primarily based Service (LBS)? Location primarily based service may be a service accessible with mobile phones, pocket PC's, GPS devices. it's like Google maps, map request. Mobile devices with positioning capabilities (e.g. GPS) facilates access to location primarily based services that give data relevant to the user's geospatial context. variety of users uses these services for retrieving Points Of Interest from their current location. LBS can be question primarily based and provides the tip user with helpful information like "Where is that the nearest restaurant?" Basically once user used specific location primarily based service or registered for that, then LBS will give variety of other services like delivery coupons or different promoting information to client United Nations agency is in a very specific geographical region. Now a days, there square measure variety of user takes advantage of location primarily based services and graph is steal increasing.

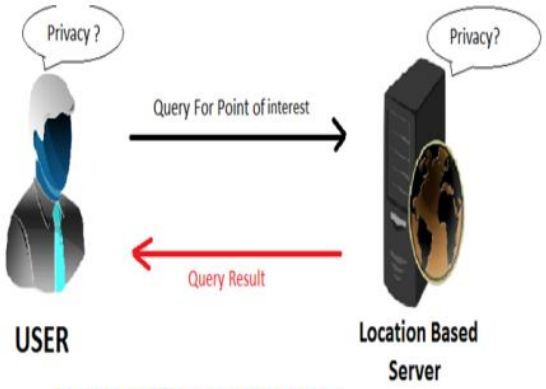


Fig. 1 Location Based Services

But there square measure bound issues whereas victimization LBS that it may collect and use large quantity of data concerning consumer for a large vary of purpose. Location data is sensitive and users don't need to share such data to untrustworthy LBS servers. as a result of variety of malicious adversaries could get additional non-public data of the users. Also, queries hearth by the user having sensitive data about people, together with health condition, life-style habits. So he doesn't need to disclose it. Privacy issues square measure expected to rise as LBSs become additional common. Location privacy suggests that information privacy. therefore here privacy assurance is measure issue. On the opposite, location server has their own database within which, variety of purpose of interest records square measure located (fig.2). therefore server must forestall info access from unauthorized user and additionally user UN agency haven\'t acquire that service.

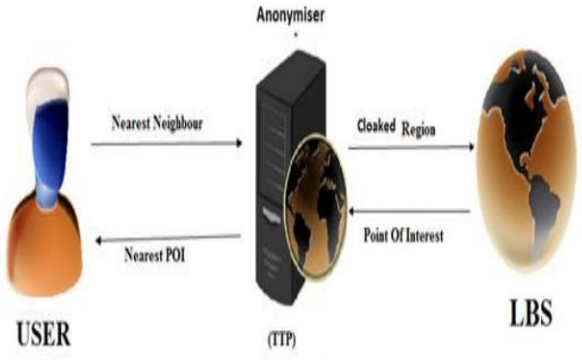


Fig.2 Location Based Service using TTP

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.

2. RELATED WORK

The main answer for the issue was proposed by Beresford , in which the security of the client is kept up by always showing signs of change the client's name or pen name inside of some blend zone. It can be demonstrated that, because of the nature of the information being traded between the client and the server, the regular changing of the client's name gives little security to the client's protection. A later examination of the blend zone methodology has been connected to street systems . They examined the obliged number of clients to fulfill the unlinkability property when there are rehashed inquiries over an interim. This obliges watchful control of what number of clients are contained inside of the blend zone, which is hard to accomplish by and by. A corresponding strategy to the blend zone approach is in view of k-secrecy . The idea of k-secrecy was presented as a system for protecting security when discharging delicate records.This is accomplished by speculation and concealment calculations to guarantee that a record couldn't be recognized from (k − 1) different records. The answers for LBS utilize a trusted anonymiser to give namelessness to the area information, such that the area information of a client can't be recognized from (k − 1) different clients.

An improved trusted anonymiser methodology has likewise been proposed, which permits the clients to set their level of security in light of the estimation of k. This implies that, given the overhead of the anonymiser, a little estimation of k could be utilized to build the effectiveness. On the other hand, a expansive estimation of k could be decided to enhance the security, on the off chance that the clients felt that their position information could be utilized perniciously. Picking a worth for k, be that as it may, appears to be unnatural.

There have been endeavors to make the procedure less simulated by including the idea of feeling-based security . Rather than indicating a k, they suggest that the client indicates a shrouding area that they feel will secure their security, and the framework sets the quantity of cells for the locale in view of the notoriety of the region. The ubiquity is figured by utilizing verifiable foot shaped impression database that the server gathered.

New security measurements have been recommended that catches the clients' security as for LBSs . The creators start by investigating the deficiencies of straightforward k-namelessness in the setting of area questions. Next, they propose security measurements that empowers the clients to indicate values that better match their question security necessities. From these protection measurements they additionally propose spatial speculation calculations that agree with the client's security necessities. Strategies have additionally been proposed to confound and mutilate the area information, which incorporate way and position disarray. Way disarray was introduced by Hoh and Gruteser. The essential thought is to add instability to the area information of the clients at the focuses the ways of the clients cross, making it difficult to follow clients in light of crude area information that was k-anonymised. Position disarray has additionally been proposed as a way to deal with give security . The thought is for the trusted anonymiser to gather the clients agreeing to a shrouding area (CR), therefore making it harder for the LS to distinguish a person. A typical issue with general CR procedures is that there may exist some semantic data about the geology of an area that gives away the client's area. Case in point, it would not bode well for a client to be on the water without some sort of watercraft.

Additionally, distinctive individuals may discover certain spots delicate. Damiani et al. have exhibited a structure that comprises of a jumbling motor that takes a clients profile, which contains places that the client esteems touchy, and yields jumbled areas in light of conglomerating calculate.

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 .

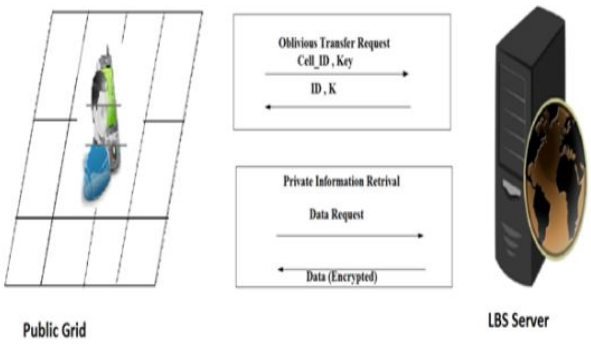


Fig. 3 Privately determine User for LBS Communication

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.

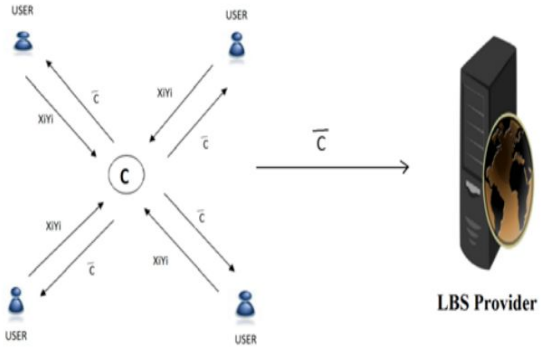


Fig. 4 LBS Services Using Centroid

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.

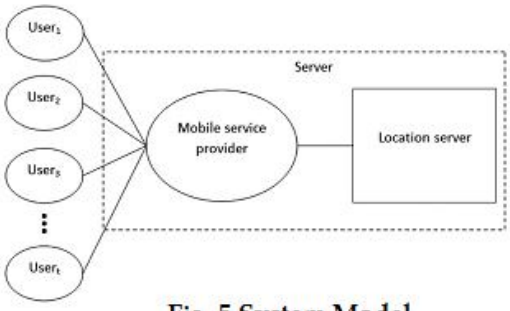


Fig. 5 System Model

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:

Here describe operating of protocol. initial giving a protocol summary to contextualize the projected resolution then describe the solution's protocol in additional detail. the final word goal of projected protocol is to get a collection (block) of dish records from the LS, that ar near the user's position, without compromising the privacy of the user or the info stored at the server. One bring home the bacon this by applying a two stage Approach shown in Fig. 2. the primary stage is predicated on a twodimensional oblivious transfer and also the second stage is based on a communicationally economical PIR. The oblivious transfer based mostly protocol is employed by the user to obtain the cell ID, wherever the user is found, and the corresponding cruciform key. The information of the cell ID and the cruciform secret's then utilized in the PIR based mostly protocol to obtain and rewrite the placement information.

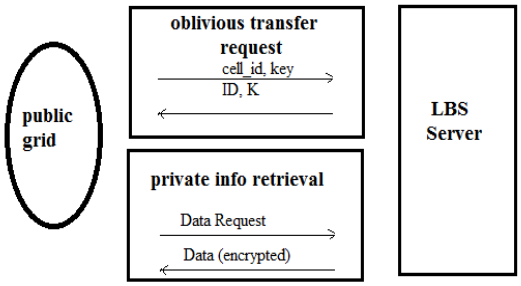


Figure 6: Privately determine user for LBS communication

The user measures his/her location insidea public generated grid P by mistreatment his/her GPS coordinates and forms an oblivious transfer query. The minimum dimensions of the public grid ar outlined by the server and ar created obtainable to all users of the system. This public grid superimposes over the in camera partitioned off grid generated by the location servers as dish records, such for

every cell energy,j in the servers as partition there's a minimum of one Pi,j cell from the public grid because PIR doesn't need that a user is constrained to get only 1 bit/block, the placement server needs to implement some protection for its records. This is achieved by encrypting every record within the dish data with a key employing a cruciform key formula, anywhere the key for encryption is that the same key used for secret writing. This secret's augmented with the cell data information retrieved by the oblivious transfer question. Hence, notwithstanding the user uses PIR to obtain more than one record, the info are going to be hollow ensuing in improved security for the server's data.

4. EXPERIMENTAL RESULTS

Performance Analysis:

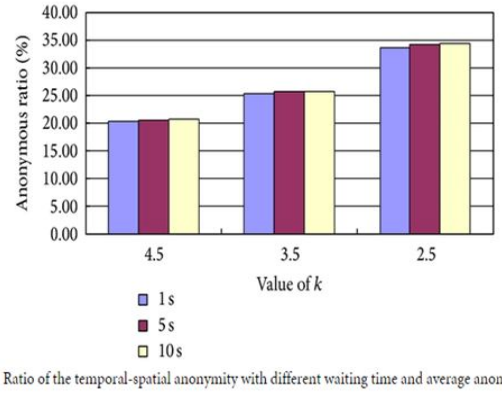
When we are performing operations on our application we have taken the values like below table

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

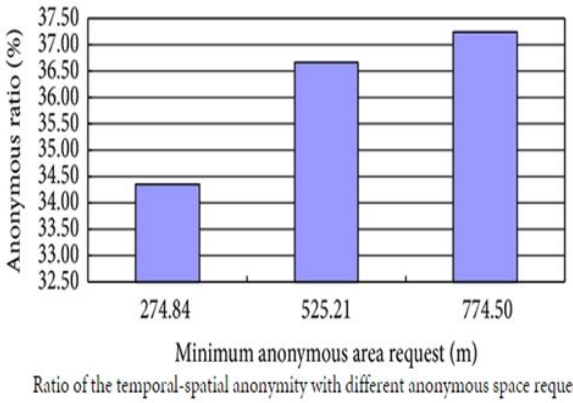
As per the table values the resultant graphs will be like below

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.