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

Location based query on location Server for Privacy Efficiency

R.Ravali Raj
M.Tech Student,
Department of Computer Science Engineering,
MVSR Engineering College,
Nadergul, Saroornagar Mandal,
Rr Dist Hyderabad-501510.

N.Priyanka
Assistant Professor,
Department of Computer Science Engineering,
MVSR Engineering College,
Nadergul, Saroornagar Mandal,
Rr Dist Hyderabad-501510.

Abstract:

In this paper 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 (POI), 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 users. The location server desires to have some control over its data, since the data is its asset. Anterior solutions have utilized a trusted anon miser to address privacy, but introduced the impracticality of trusting a third party. More recent solutions have utilized homomorphic encryption to abstract this impuissance. Briefly, the utilizer submits his/her encrypted coordinates to the server and the server would determine the utilizer's location homomorphically, and then the utilizer would acquire the corresponding record utilizing Private Information Retrieval techniques. We propose a major enhancement upon this result by introducing a kindred two stage approach, where the homomorphic comparison step is superseded with Oblivious Transfer to achieve a more secure solution for both parties. The solution we present is efficient and practical in many scenarios. We additionally include the results of a working prototype to illustrate the efficiency of our protocol.

Keywords:
Location based query, location Server, Privacy, Efficiency.

1.Introduction:

A location predicated accommodation (LBS) is an information, regalement and utility accommodation generally accessible by mobile contrivances such as, mobile phones, GPS contrivances, pocket PCs, and operates through a mobile network.

LBS can offer many accommodations to the users predicated on the geographical position of their mobile contrivance. The accommodations provided by LBS are typically predicated on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the utilizer can get answers to sundry location predicated queries, which include but are not constrained to - discovering the most proximate ATM machine, gas station, hospital, or police station. In recent years there has been a dramatic increase in the number of mobile contrivances querying location servers for information about POIs. Among many challenging barriers to the wide deployment of such application, privacy assurance is a major issue. For instance, users may feel reluctant to disclose their locations to the LBS, because it may be possible for a location server to learn who is making a certain query by linking these locations with a residential phone book database, since users are liable to perform many queries from home.

The Location Server (LS), which offers some LBS and spends its resources to compile information about sundry intriguing POIs. So, it is expected that the LS would not disclose any information without fees. Therefore the LBS has to ascertain. In the most representative research work [1], the precision of -NN search is proximate to 100% when however, it will drop when increases. Therefore, on the substructure of connected space-filling curves and hormomorphic cryptosystems, an efficacious secure - NN search protocol, Private Circular Query Protocol (PCQP), is proposed to deal with the afforested two challenges. In PCQP, the Moore's version of Hilbert curve [2], [3] (or Moore curve in short) is culled as the mapping implement to transform POIs in 2-D space into 1-D space, and the LBS query is resolved in the 1-D transformed space with the proposed secret circular shift scheme. The time-consuming space transformation effort is paid only in the initialization phase for building an LBS.

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

The resultant 2-D to 1-D space transformation can be perpetually reused. Section II Shows the Cognate work for this paper, Section III presents and describes our proposed protocol. Section IV analyses the security of the protocol. Section V summarises the key contributions of this paper and future directions.

2.Related Work:
Existing System:

The Location Server (LS), which offers some LBS, spends its resources to compile information about sundry intriguing POIs. Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBS has to ascertain that LS's data is not accessed by any unauthorized utilizer. During the process of transmission the users should not be sanctioned 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 additionally avert users from accessing content to which they do not have sanction.

Existing System Disadvantages:

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

a)Proposed System:

our protocol is organized according to two stages. In the first stage, the utilizer privately determines his/her location within a public grid, utilizing 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 utilizer executes a communicational efficient PIR, to retrieve the felicitous block in the private grid. This block is decrypted utilizing the symmetric key obtained in the antecedent stage. Our protocol thus provides auspice for both the utilizer and the server. The utilizer is bulwarked because the server is unable to determine his/her location. Similarly, the server's data is forefended since a malignant utilizer can only decrypt the block of data obtained by PIR with the encryption key acquired in the antecedent 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 an antecedent 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.

b)The Location Privacy Protocols on Application Layer
K-Anonymity:

K-anonymity [12][13] is a popular solution for providing location privacy[10] to users. The concept emanates from achieving privacy in data mining, such that when relational data including private data of many users 26 will be relinquished, K-anonymity auspice mechanism is applied on the data to forfend privacy of users.Since one of the aims of this project is to investigate subsisting protocols on location privacy, the investigation commenced from K-anonymity. It has both strengths and impuissances. For example, when a utilizer is located in a crowd, K-anonymity can provide expeditious and simple solution. Since there are an abundance of people around the utilizer, it is very facile to compose a cloaked region that users can obnubilate underneath it. If the utilizer is present in that area arbitrarily, he/she can rely on K-anonymity. However, its impotency is the k value and working in a discrete and independent manner. Utilization of k value emanates from a data mining perspective and it is not congruous for preserving location privacy [10] most of the time. For example, an adversary might have cognizance about a user's home and work locations.

c)Metrics for the Location Privacy:
Uncertainty-Based Metric:

Dubiousness-predicated metric considers only the entropy of events of a utilizer. It is a very general solution. It is not opportune for estimating the probabilistic nature of the adversary. It is very hard to model the adversary; because the adversary's cognizance and probability assignment are unknown. Besides, the adversary can cull erroneous events as favorite. Thus, the precision of the adversary is another variable in the system. Skeptically-predicated metric cannot capture this kind of detail. It is additionally not felicitous for calculating tracking errors that is identification of traces of users.

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

Clustering Error Based Metric:

In clustering error predicated metric, adversary gets observed events and partitions them into multiple subsets for each utilizer. The error in partitioning betokens the location privacy[10] of the system. Here, the observed events are transformation of the genuine events. For instance, a mechanism, such as anonymization or obfuscation, etc., is applied on authentic events in order to forfend location information of the utilizer from disclosure to public. In this metric, there are two quandaries that are calculation of set of all possible partitions and congruousness for tracing.

Traceability-Based Metric:

Traceability-predicated metric aims to estimate certainty of an adversary in tracking a utilizer. It is mentioned that a utilizer will be traceable until a point in time or location. This point is called a perplexity point; as the adversary's dubiousness is above a threshold. [15] It is withal mentioned that querying the LBS periodically, in time space, exposes sensitive locations for users. They suggest that querying the LBS can be done predicated on areas, which denotes that 28 the users do not send queries or the LBS does not expect queries at some locations, which are private areas to utilize the accommodation. Those places are out of the range of the accommodation.

Distortion-Based Metric:

The set of criteria, which is utilized to evaluate subsisting location privacy[10] metrics, is composed of adversary's probability of error and tracking error, users' authentic traces and private location-time couples, quantification of traceability of users, genericity of the metric and the granularity of the resulting location privacy value. Each criterion reveals more insight about the quandary and subsisting metrics. For example, adversary can make mistakes; but dubiousness predicated metrics or K-anonymity metric is not able to count in adversary's error in probability assignment or tracking users. Furthermore, considering authentic traces of users at all times is withal consequential, because it avails to assess how prosperous the adversary is in tracking a utilizer.

d)System Architecture:

The system model consists of three types of entities (see Fig. 1):
1. Users
2. Mobile service provider
3.Location server.

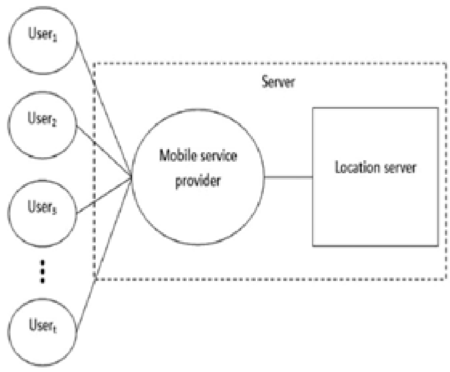

Fig 1:System Architecture Model.

3.Implementation

3.1 Users:

The users in our model utilize some location-predicated accommodation provided by the location server LS. For example, what is he most proximate ATM or restaurant? The purport of the mobile accommodation provider SP is to establish and maintain the communication between the location server and the utilizer. The location server LS owns a set of POI records ri for 1≤ri ≤ρ. Each record describes a POI, giving GPS coordinates to its location (xgps,ygps), and a description or name about what is at the location.

3.2 Mobile Service Provider:

We plausibly surmise that the mobile accommodation provider SP is a passive entity and is not sanctioned to collude with the LS. We make this posit because the SP can determine the whereabouts of a mobile contrivance, which, if sanctioned to collude with the LS, thoroughly subverts any method for privacy. There is simply no technological method for obviating this assailment. As a consequence of this posit, the utilizer is able to either use GPS (Ecumenical Situating System) or the mobile accommodation provider to acquire his/her coordinates.

3.3 Location Server:

We are postulating that the mobile accommodation provider SP is trusted to maintain the connection, we consider only two possible adversaries. Each and every one for individual communication direction.

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

We consider the case in which the utilizer is the adversary and endeavors to obtain more than he/she is sanctioned. Next we consider the case in which the location servers LS is the adversary, and endeavors to uniquely associate a utilizer with a grid coordinate.

4.Experimental Results:

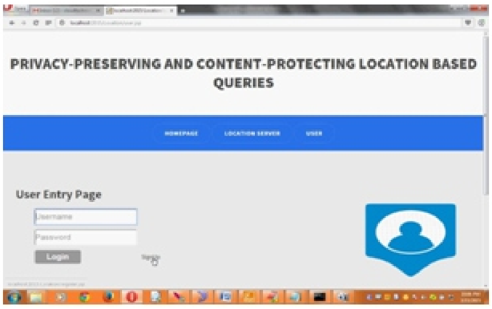

Fig 2: user login page.

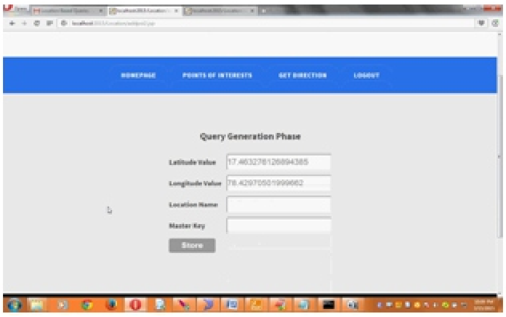

Fig 3: user location based Query Page.

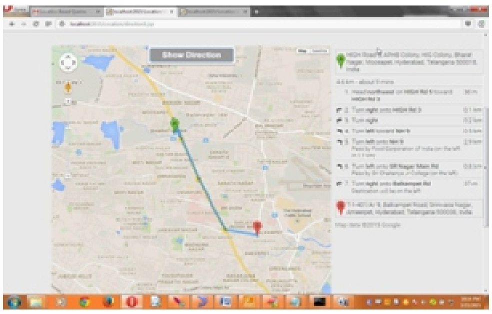

Fig 4: Location result page based on Query.

5.Conclusion:

In this paper we have presented a location predicated query solution that utilized for a utilizer to privately determine his/her location utilizing oblivious transfer [4] on a public grid a private information retrieval interaction that retrieves the record with high communication efficiency.

According to our analysis of cognate work on the location privacy, we decided to implement the location privacy [10] evaluation model of Distortion-Predicated Metric [15], which we used to assess our implementation of K-anonymity solution. The modifications that we have done on K-anonymity implementation of [10] were elimination of personalization and adaptation to the evaluation model of Distortion-Predicated Metric. We have eliminated personalization from K-anonymity; because we aimed to observe results of K-anonymity protocol when it covers k-many users at a time, hence we made it work in all cases. We analyzed the performance of our protocol and discerned it to be both computationally and communicationally more efficient than the other subsisting solutions.

6.References:

[1] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L.Tan,"Private queries in location based services: anonymizers are not necessary," in Proc. 2008 ACM SIGMOD Int. Conf. Management of Data, New York, NY, USA, 2008, pp. 121–132, ser. SIGMOD'08, ACM.

[2] E. H. Moore, "On certain crinkly curves," Trans. Amer. Math. Soc., vol. 1, pp. 72–90, Jan. 1900.

[3] H. Sagan, Space-Filling Curves. New York, NY, USA: Springer- Verlag, 1994.

[4] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," Proc. CRYPTO'99, 1999, vol. 1666, pp. 791 - 791.

[5] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," Proc. CRYPTO'89. 1990, pp. 547 - 557.

[6] M. Mokbel, "Towards privacy-aware location-based database servers," in Proc. 22nd Int. Conf. Data Engineering Workshops, 2006, pp. 93–102.

[7] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location- based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[8] A.-A. Hossain, A. Hossain, H.-K.Yoo, and J.-W. Chang, "H-star: Hilbert-order based star network expansion cloaking algorithm in road networks," in Proc. IEEE

14th Int. Conf. Computational Science and Engineering (CSE), Aug. 2011, pp. 81–88.

[9] T. ElGamal, “A public key cryptosystem and a signature schemebased on discrete logarithms,” IEEE Trans. Inform. Theory, vol. 31,no. 4, pp. 469–472, Jul. 1985.

[10] B. Gedik and L. Liu, “Location privacy in mobile systems: A personalizedanonymization model,” in Proc. ICDCS, Columbus, OH,USA, 2005, pp. 620–629.

[11] C. Gentry and Z. Ramzan, “Single-database private information retrieval with constant communication rate,” in Proc. ICALP,L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung,Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.

[12] Marco Gruteser and Dirk Grunwald. Anonymous usage of locationbased services through spatial and temporal cloaking. In Proceedings of the 1st international conference on Mobile systems, applications and services, MobiSys ’03, pages 31–42, New York, NY, USA, 2003. ACM.

[13] Ling Liu BugraGedik. A customizable k-anonymity model for protecting location privacy. Technical Report GIT-CERCS-04-15, Georgia Institute of Technology, April 2004.

[14] Chi-Yin Chow, Mohamed F. Mokbel, and Xuan Liu. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems, GIS ’06, pages 171–178, New York, NY, USA, 2006. ACM.

[15] Reza Shokri, JulienFreudiger, MurtuzaJadliwala, and Jean-Pierre Hubaux.A distortion-based metric for location privacy. In Proceedings of the 8th ACM workshop on Privacy in the electronic society, WPES ’09, pages 21 30, New York, NY, USA, 2009. ACM.