Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.314 – 321

RESEARCH ARTICLE

Improving Privacy Protection for Location Based Services

[1]V. Kartheek Kumar Reddy, [2]Dr. A.P. Siva Kumar **M.Tech,Ph.D**

[1]PG Scholar, Department of Computer Science & Engineering (Artificial Intelligence), JNTUA College of Engineering (Autonomous), Anantapuramu, AP, India

[2]Assistant Professor, Department of Computer Science & Engineering, JNTUA College of Engineering (Autonomous), Anantapuramu, AP, India

[1] kartheek.reddy1234@gmail.com

[2] SivaKumar.ap@gmail.com

Abstract: The present's modern world, it is very facile for a person to grasp his/her location with the avail of contrivances having GPS facility. When user's location is provided to LBS, it is possible to grasp all the user information depending on the locality such as locality of friends or nearby restaurant, or more about something like traffic conditions. Extensive utilization of mobile contrivances surface the way for the formation of wireless networks that can be confirmed to exchange data implied on localities. If the locale information is exchanged among trusted parties, then the privacy of the user would be in destructive way. Subsisting protocol doesn't work on many different mobile contrivances and another issue is that, Location Server (LS) should provide illuding data to user. So we are working on enhancement of this protocol.

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

I. INTRODUCTION

A location predicated accommodation (LBS) is a data, regalement and service accommodation generally attainable by mobile contrivances just as, GPS contrivances, pocket PCs, mobile phones and percolates over a mobile network. Location based servers provides many accommodations to the customers predicated on the geological area of their mobile contrivance. The accommodations afforded by a LBS are usually predicated on a database of point of interest. By getting back the Points Of Interest (POIs) from the server's database, customer gets the solutions to sundry locale predicated questionnaires, that adds but it is not constrained for exploring the most proximate gas station, police station, ATM machine or hospital. During the past years, there was a drastic raise in the statistics of mobile contrivances questioning the locality servers for the clues about POIs. In the middle of several challenging barricades to the broad deployment of that sort of application like assurance of providing the privacy is a big issue. Actually, the customers hesitate to show their locality to the LBS, why because there is a possibility for the locality server to trace the person querying by associating the locale with residential phonebook database, because customers usually perform querying from house. 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 homomorphic cryptosystems, an efficacious secure - NN search protocol, Private Circular Query Protocol (PCQP), is proposed to deal with the aforecited 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 convert points of interest in two dimensional arena into single dimensional arena, and the locality based services questionnaire is concluded in the one dimensional transformed arena with the secret circular shift scheme. Time engrossing arena conversion attempt is paid only in the starting point for constructing an locality based services. The corollary two dimensional to single dimensional arena conversion can be perpetually reused.

II. RELATED WORK

In this section, related work is outlined. It includes the model of LBS.

A. Existing System:

The Locality Server (LS), that is providing some locality based services, usually consumes its asserts to collect the intelligence about sundry intriguing POI's. So, locality server has decided not to expose any intelligence by not taking any fair. So that the locality based services has to ascertain that locality server's intelligence is not accessible by the invalid user. While the transmission process the customers are not sanctioned to explore any intelligence for that they didn't pay. Many frameworks have been framed for providing secrecy to the queries issued by the customers and moreover for preventing the customers from accessing those who do not have sanction.

B. Proposed System

Proposed System organized according to two stages. Stage one, the utilizer confidentially finds his/her locality in a public grill utilizing uninformed transmission. This transformed data comprises of both the ID and associated symmetric key for the block of data in the private grill. Second stage, the utilizer executes a communicational efficient PIR, to get the felicitous chunk in the confidential grill. That chunk is decrypted utilizing the symmetric key gained in the antecedent stage. Proposed system principle thereby provides auspice for the utilizer and server. Utilizer is bulwarked, since the server is in a position of not finding his/her locality. Same way, the server's data is forefended since a malignant utilizer is the only one who can decrypt the chunk of data gained by PIR using the encryption key gained in the antecedent phase. In other terms, utilizers have the capability of gaining the intelligence for only which the fair has paid.

a) 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 forefend 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 impuissance's. 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.

b) 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.

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 forefend 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.

c) System Architecture

The system model consists of three types of entities (see Fig. 1)

1. Users

2. Mobile service provider

3. Location server

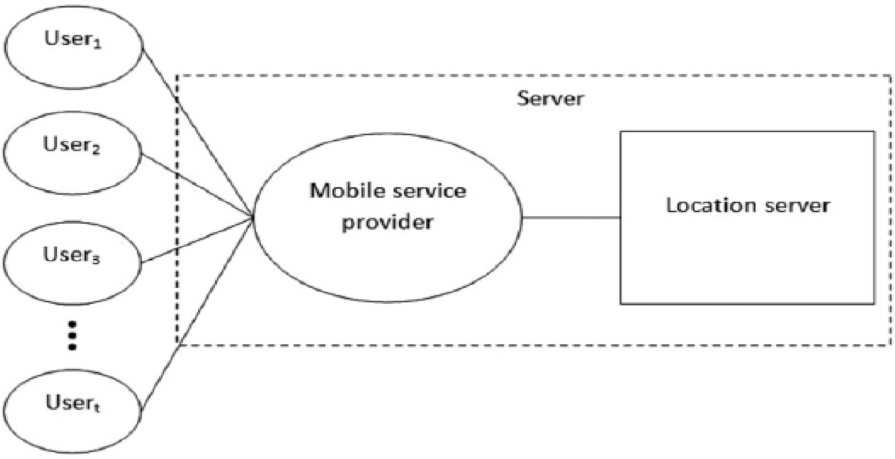


Fig 1: System Architecture Model.

III. 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 r_i for $1 \leq r_i \leq \rho$. Each record describes a POI, giving GPS coordinates to its location (x_{gps}, y_{gps}), 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. 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 server LS is the adversary, and endeavors to uniquely associate a utilizer with a grid coordinate.

IV. EXPERIMENTAL RESULTS

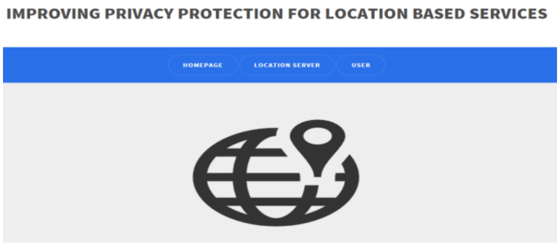
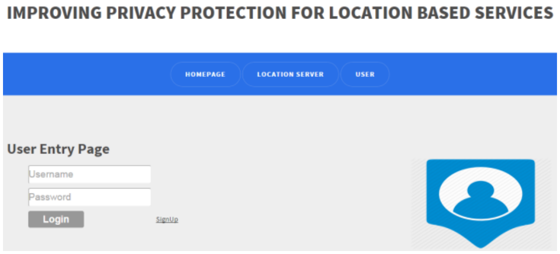


Fig 1: Project Home Page



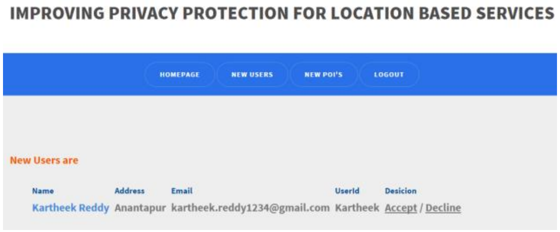
User Entry Page

Username

Password

Login SignUp

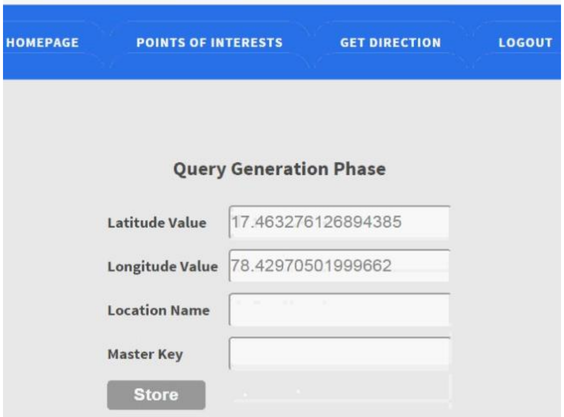
Fig 2: User Login Page



New Users are

Name	Address	Email	UserId	Desicion
Kartheek Reddy	Anantapur	kartheek.reddy1234@gmail.com	Kartheek	Accept / Decline

Fig 3: Location Server users Accepting Page.



Query Generation Phase

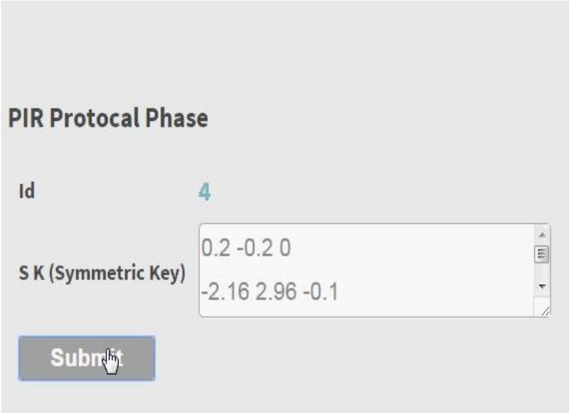
Latitude Value 17.463276126894385

Longitude Value 78.42970501999662

Location Name

Master Key

Fig 4: User Query Generation Page.

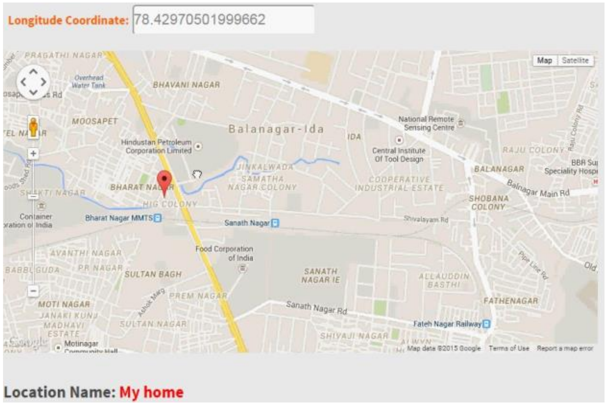


PIR Protocal Phase

Id 4

S K (Symmetric Key) 0.2 -0.2 0
-2.16 2.96 -0.1

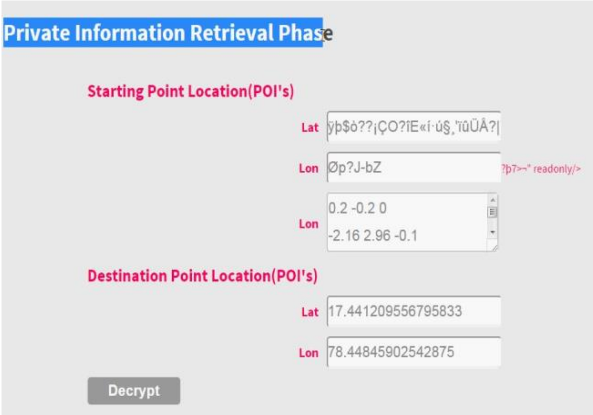
Fig 5: User PIR Protocol Generation Page.



Longitude Coordinate: 78.42970501999662

Location Name: My home

Fig 6: User Get Location Page.



Private Information Retrieval Phase

Starting Point Location(POI's)

Lat ÿþ$ò??¡ÇO?ÎE«í·ú§,'îûÜÅ?|

Lon Øp?J-bZ ?þ7>¬" readonly/>

Lon 0.2 -0.2 0
-2.16 2.96 -0.1

Destination Point Location(POI's)

Lat 17.441209556795833

Lon 78.44845902542875

Fig 7: User Private Information retrieval Page.

V. 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 confidential intelligence recuperation cooperation that recuperates the record with immense transmission capability. 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 [20] 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 communication ally more efficient than the other subsisting solutions.

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 scheme based 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 Bugra Gedik. 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, Julien Freudiger, Murtuza Jadliwala, 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.

AUTHORS

V.KartheekKumarReddy, studying Masters in Computer Science and Engineering in Artificial Intelligence specialization in JNTU Anantapuramu. Completed my Bachelors in Intell Engineering College under Computer Science and Engineering stream, Anantapuramu.

Dr. A.P.SivaKumar is currently working as Assistant Professor in Computer Science at JNTUniversity, Anantapuramu, A.P, India. He received the bachelor's degree in 2002 and master's degree in 2004,boath from JNTU Hyderabad,. He has around 10 Years of experience as a Lecturer/Research and Development with strong analytical background in the education sector. His research interests are Cross Lingual Information retrieval and Natural Language Processing.