International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 271-278
http://dx.doi.org/10.14257/ijsia.2015.9.4.25

# Authentication Model for Location based Queries

Roshan S. Deshmukh[1] and Dr. D. G. Harkut[2]

[1]*M.E II Year Department of Computer Science and Engineering*
*Prof Ram Meghe College of Engineering and Management*
*Badnera-Amravati, India*
[2]*Associate Professor, Department of Computer Science and Engineering*
*Prof Ram Meghe College of Engineering and Management*
*Badnera-Amravati, India*
*roshan.deshmukh@gmail.com, dg.harkut@gmail.com*

***Abstract***

*The popularity of location-based services leads to serious concerns on user privacy. 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 Location Based Services (LBS), it is possible for user to know all location dependent information like location of friends or Nearest Restaurant, weather or traffic conditions. The massive use of mobile devices paves the way for the creation of wireless networks that can be used to exchange information. When the exchange of 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. This gives rise to new challenges and reconsideration of the existing privacy metrics.*

***Keywords:*** *Location Based Services, Location Server*

## 1. Introduction

There are increasing mobile phone users worldwide. So location technologies can be currently used by wireless carrier operators to provide a good forecast of the user location. Now a day, numbers of users are using location based services which can provide location-aware information. What is 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 geo-spatial context. Number of users uses these services for retrieving Points of Interest from their current location. LBS is question primarily based and provides the top user with helpful data like "Where is that the nearest Hotel?" essentially once user used specific location based service or registered for that, then LBS will offer variety of different services like delivery coupons or different selling data to client United Nations agency is during a specific geographic region. Now a day, there are number of user takes advantage of location based services and graph is steal increasing.

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.

ISSN: 1738-9976 IJSIA

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.1). So server has to prevent database access from unauthorized user and also user who have not pay for that 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.

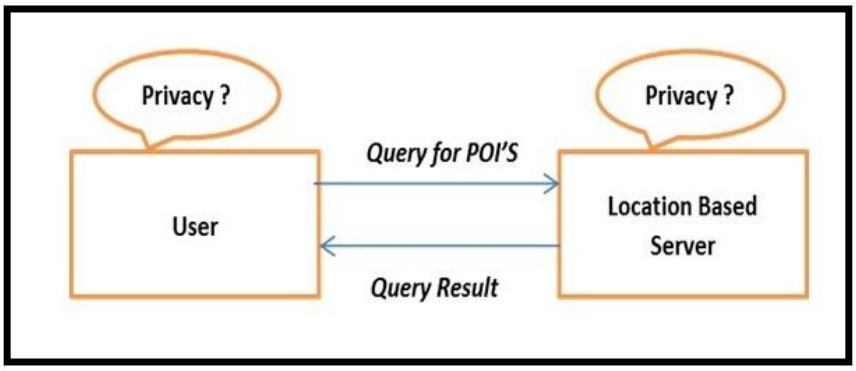



**Figure 1.Location Based Service**

## 2. Motivation

1948 Universal Declaration of Human Rights declares that everyone has a right to privacy at home, with family, and in correspondence. Other pieces of more recent legislation follow this principle. But location-aware applications begin to track our movements in the name of convenience, how can we protect our privacy? Technologies for locating and tracking Individuals are becoming increasingly commonplace, and they will become more pervasive and ubiquitous in the future. Location- aware applications will have the potential to follow your every move, from leaving your house to visiting the doctor's office, recording everything from the shelves you view in a supermarket to the time you spend beside the coffee machine at work We must address the issue of protecting location information before the widespread deployment of the sensing infrastructure.

## 3. Literature Review

A. Beresford and F. Stajano [1] define the concept of mix zones for the privacy of user's location, as aware application will have the potential to follow the user move. The security of the user is kept up constantly changing the username or pseudonym within some mix zone, but this does not provide full protection to the user's privacy.

B. Palnisamy and L. Liu [2] define the concept of mixzones on road networks. This framework is to protect location privacy of mobile user's travelling on road network the new concept of Mobimix is also used to break up the continuity of user's location. The practical approach of this technique is difficult to achieve in practice.

C. Bettini, X. Wang, and S. Jajodia [3] define the concept of k-anonymity as a method for privacy preserving. By using generalization algorithm the concept of K-anonymity implemented, K-anonymity is a wide-spread general privacy concept not restricted to location privacy. It provides the guarantee that in a set of k objects (mobile users), the target object is non-identifiable from the other k – 1 objects.

B. Gedik and L. Liu [4] describe a personalized k-anonymity model for protecting location privacy. This model allows each user using mobile to define and modify the definition at the granularity of single messages.

M. Gruteser and D. Grunwald [5] define the spatial and temporal cloaking. A quad tree based algorithm is introduced to guarantee k-anonymous location information through reduction in location resolution.

L. Sweeney [6] with the concept of k-anonymity it adds one concept of ANONYMISER which is trusted third party. A user sends its location, query and K to the anonymiser, which is a trusted third party in centralized systems or a peer in decentralized systems. The anonymiser removes the ID of the user. TTP regenerate cloak for user location by making K- anonymiser spatial region in which number of k-1 users are involved. Then anonymiser sends the K-ASR and query to the LBS sever, which calculates the candidate results respect to the cloaked region and sends them back to the anonymiser. Then the anonymiser which knows the locations of all the users calculates the actual results and sends them back to the user.

S. Mascetti and C. Bettini [7] define the concept of location based services this allows the user to set their level of privacy based on the value of k.

M. Mokbel, C. Chow and W.Aref [8] introduce the Casper, framework in which mobile users can use location based services without disclosing the location information of user. Casper has two main components the location anonymiser and privacy aware query processor.

L. Marconi, R. Dipietro, B. Crispo and M. Conti [9] define a feeling based model, where focused on a preserving users privacy in location based services. In this model the importance is given to time shown that how it affect the privacy in location based services.

T. Xu and Y.Cai [10] defines a feeling based privacy model by introducing a concept of public region, this technique prevents location information with restricted spaces such as home and office by correlating with restricted spaces, an adversary may be able to identify the users in a cloaking box. Instead of specifying a k, they propose that the user specifies a cloaking region that they feel will protect their privacy and the system sets the number of cells for the region based on the popularity of the area. The popularity is computed by using historical footprint database that the server collected.

X. Chen and J. Pang [11] proposed a new privacy metric that captures the user's privacy with respect to location based services. A spatial generalization algorithm is used to compute regions satisfying user's privacy requirements. The main aim is to protect user's location and query privacy. Algorithms suffer from a specific attack known as "outlier problem", wherever attackers have the generalization algorithms and users' abstraction distribution as a part of their data.

B. Hoh and M. Gruteser [12] present a path perturbation algorithm that continuously collect location sample from a large group of users. When two users met at one location, this algorithm can cross paths in area. So adversary would confuse the paths of different users. If two users move in parallel, the path perturbation algorithm perturbs the parallel segment into crossing segment. But this algorithm technique is unable to protect time-series location information.

P. Kalnis, G. Ghinita, K. Mouratidis and D. Papadias [13] Presents the idea of trusted anonymiser to group the user according to a cloaking region thus making it harder for the location server to identify an individual but a common problem with general cloaking region technique is that they may exist some semantic information about the geography of the location that gives away the users location.

M. Damiani, E. Bertino, and C. Silvestri [14] define the concept of PROBE Framework for personalized cloaking and private locations. It provides a set of

obfuscation methods which have very small storage requirements and that are suited for use of small devices such as cell phones

T. Hashem and L. Kulik [15] presented a scheme whereby a group of trusted users construct an ad-hoc network and the task of querying the LS is delegated to a single user This idea improves on the previous work by the fact that there is no single point of failure. If a user that is querying the LS suddenly goes offline, then another candidate can be easily found. However, generating a trusted ad-hoc network in a real world scenario is not always possible.

M. Duckham and L. Kulik [16] present a model of obfuscation and Negotiation for location privacy. This model provides a computationally efficient mechanism for balancing a user's need for high quality information services against that user need for location privacy. To provide a service of satisfactory quality negotiation is used in location privacy.

H. Kido, Y. Yanagisawa, and T. Satoh [17] for avoiding the use of a trusted anonymiser define the method dummy location. The basic idea is to confuse the location of the user by sending many random other locations to the server, such that the server cannot distinguish the actual location from the fake location this incurs both processing and communication overhead for the user device.

John Krumm [18] had done survey on computation location privacy means computation based privacy mechanism where computational algorithm is used for compromising and protecting location data. This algorithm treats location data as geometric information not as general data.

G. Ghinita, P. Kalmis, A. Khashgozaram, C. Shababi, K. Tan [19] introduces a scheme called private information retrieval (PIR) location scheme. The basic idea is to employ PIR to enable the user to query the location database without compromising the privacy of user .Existing system requires clocked region and a TTP, but it doesn't need of anonymiser and privacy is achieve through cryptographic techniques. Here server forms the region regarding to POI and while answering to query, server first send regions to user. The user finds the region that contains him and utilizes PIR to request all points within that region. So, the server does not know which region was retrieved.

B. Chor O. Goldreich, E. Kushilevitz and M. Sudan [20] investigate whether by replicating the database more efficient Solutions to the private retrieval problem can be obtained. Each Individual server holding a replicated copy of the database gets no information on the identity of the item retrieval by the user. This scheme used the replication to gain substantial saving.

E. Kushilevitz and R. Ostrovsky [21] present a single database computationally – Private Information Retrieval Scheme where replication of data is not necessary in order to retrieve, in a private and communication efficient manner, information from a database.

G. Ghinita, P. Kalnis, M. Kantarcioghu and E. Bertino [22] present a technique for private location based queries with database protection. This protocol consists of two stages. In the first stage, the user and server use homomorphic encryption to allow the user to privately determine whether his/her location is contained within a cell, without disclosing his/her coordinates to the server. In the second stage, PIR is used to retrieve the data contained within the appropriate cell.

G. Ghinita, P. Kalnis, M. Kantarcioghu and E. Bertino [23] proposed hybrid techniques for approximate and exact private queries, which provide protection for both the user and the service provider. A cryptographic protocol is used in this technique. It does not support to more complex types of queries.

P. Pallier [24] proposed the homomorphic encryption scheme to privately compare two integers is the Paillier encryption scheme. The Paillier encryption scheme is known to be additively homomorphic and multiplicatively-by-a-constant homomorphic. This means that we can add or scale numbers even when all numbers are encrypted. Both features are

used to determine the sign (most significant bit), and hence the user is able to determine the cell in which he/she is located, without disclosing his/her location.

## 4. Comparative Study

**Table1. Comparisons of Existing Models**

| Sr.No | Techniques | Performance Evaluation | | |
|---|---|---|---|---|
| | | Privacy | Computation Overhead | Communication Overhead |
| 1 | Mix zone | Average | ---------- | High |
| 2 | K-anonymity | Average | Normal | ---------- |
| 3 | Spatial Generalization Algorithm | Normal | High | ---------- |
| 4 | Path Confusion | High | Normal | High |
| 5 | Dummy Location | High | High | Normal |
| 6 | Private Information Retrieval | High | Normal | Normal |

In above table we have done the comparative study of different techniques related to privacy preserving. We have discussed the limitation of some techniques which we are trying to overcome in existing system. By implementing the Authentication model with two protocols such as private information retrieval and oblivious transfer. Our proposed model will contains two protocols namely oblivious transfer phase and private information retrieval first.

User publicly determines his location using GPS coordinates and then he determines private location in a public grid using oblivious transfer .After getting cell id and related symmetric key from server, user fires query using PIR. 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

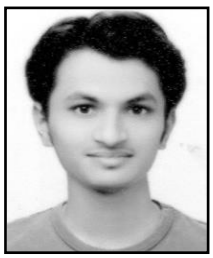
## 5. Conclusion

In this Paper we have done review on Privacy preserving techniques for Location Based Queries. Where we have seen various techniques for user's privacy and location based queries. We have studied all the references to develop a protocol both for user and server for their privacy assurance. We propose an authentication model which contains a two stage, where we will try to minimize the issues in previous works.

## References

[1] A. Beresford and F. Stajano, "Location privacy in pervasive comput", IEEE Pervasive Computing., vol. 2, no. 1, **(2003)**, pp. 46–55.
[2] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks", Proc. ICDE, Hannover, **(2011)**; Germany.
[3] C. Bettini, X. Wang and S. Jajodia, "Protecting privacy against location-based personal identification", Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M. Petkovic, Eds., **(2005)**; Trondheim, Norway.
[4] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model", Proc. ICDCS, Columbus, **(2005)**; OH, USA.
[5] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking", Proc.1st Int. Conf. MobiSys, **(2003)**.
[6] L. Sweeney, "k-Anonymity: A model for protecting privacy", Int. J. Uncertain, Fuzziness Knowl. Based Syst., vol. 10, no. 5, **(2002)**, pp. 557–570.
[7] S. Mascetti and C. Bettini, "A comparison of spatial generalization algorithms for lbs privacy preservation", Proc. Int. Mobile Data Manage., **(2007)**; Mannheim, Germany.
[8] M. F. Mokbel, C. Y. Chow and W. G. Aref, "The new Casper: Query processing for location services without compromising privacy", Proc. VLDB, **(2006)**; Seoul, Korea.
[9] L. Marconi, R. Pietro, B. Crispo and M. Conti, "Time warp: How time affects privacy in LBSs", Proc. ICICS, **(2010)**; Barcelona, Spain.
[10] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services", Proc. 16th ACM CCS, **(2009)**; Chicago, IL,USA.
[11] X. Chen and J. Pang, "Measuring query privacy in location-based services", Proc. 2nd ACM CODASPY, **(2012)**; San Antonio, TX, USA.
[12] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion", Proc. 1st Int. Conf. SecureComm, **(2005)**.
[13] 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, **(2007)**, pp. 1719–1733.
[14] M. Damiani, E. Bertino and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations", Trans. Data Privacy, vol. 3, no. 2, **(2010)**, pp. 123–148.
[15] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks", Proc. 9th Int. Conf. UbiComp, **(2007)**; Innsbruck, Austria.
[16] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy", Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., **(2005)**.
[17] H. Kido, Y. Yanagisawa and T. Satoh, "An anonymous communication technique using dummies for location-based services", Proc. Int. Conf. ICPS, **(2005)**.
[18] J. Krumm, "A survey of computational location privacy", Pers. Ubiquitous Comput., vol. 13, no. 6, **(2009)**, pp. 391–399.
[19] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi and K. L. Tan, "Private queries in location based services: Anonymizers are not necessary", Proc. ACM SIGMOD, **(2008)**; Vancouver, BC, Canada,.
[20] B. Chor, E. Kushilevitz, O. Goldreich and M. Sudan, "Private information retrieval", J. ACM, vol. 45, no. 6, **(1998)**, pp. 965–981.
[21] E. Kushilevitz and R. Ostrovsky, "Replication is not needed: Single database, computationally-private information retrieval", Proc. FOCS, **(1997)**; Miami Beach, FL, USA.
[22] G. Ghinita, P. Kalnis, M. Kantarcioglu and E. Bertino, "A hybrid technique for private location-based queries with database protection", Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., **(2009)**; Aalborg, Denmark.
[23] 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, **(2010)**, pp. 1–28.
[24] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes", Proc. EUROCRYPT, **(1999)**; Prague, Czech Republic.

## Authors



**Roshan S. Deshmukh**, he is a master student in the Department of Computer Science and Engineering at Prof Ram Meghe College of Engineering and Management in Badnera-Amravati, India. He received his bachelor's degree in computer science from SGB Amravati University. The most topics interest includes Data Mining, Information Retrieval & Databases Technology.

**Dinesh G. Harkut**, he received B.E. (Computer Science & Engineering) & M.E. (Computer Science & Engineering) from SGB Amravati University in 1991 and 1998 respectively. He completed his master's in Business Management and obtained his Ph.D. from SGB Amravati University in Business Management in 2013 while serving as a full-time faculty in the Dept. of Computer Science & Engineering at Prof Ram Meghe College of Engineering & Management, Badnera – Amravati. His research interests are Embedded Systems and RTOS.