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

An efficient and Practical approach for preserving user privacy and protecting location data in the Location server

G.Madhu
MTech Student
Department of CSE
Sri Venkateswara Engineering College
Suryapet 508213

Y.Bharath Bhushan
Assistant Professor
Department of CSE
Sri Venkateswara Engineering College
Suryapet 508213

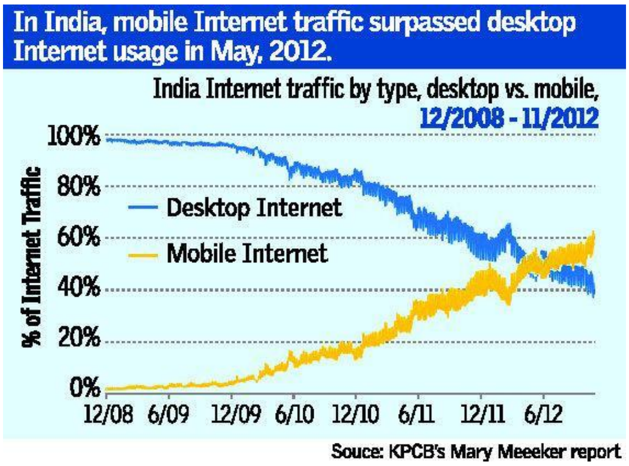
Abstract: ***Location-based services (LBS) are a general class of computer program-level services that use location data to control features. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses data on the geographical position of the mobile device. This has become more important with the growth of the smartphones. Location based system are used for finding out Point of Interests from a specific location. Typically a GPS coordinates are sent as an input to the location servers and based on the GPS coordinate the point of interests can be served back to the client from the location server. To solve problems associated with the location data. The user does not want to send his location data to the server directly, since doing so the server can find the user's location preferences and use that data for advertising the user's privacy is lost. The second part is like the server wants to protect its data from the user query. The server wants to return back only relevant data to the user. The server cannot send back sensitive data to the user. A main improvement upon prior solutions by using a two stage approach, where the first step is based on Symmetric key Transfer and the second step is based on Private data based on Symmetric key Retrieval, to achieve a secure solution for both parties. The solution is efficient and practical in many scenarios. Implement the solution using a real cloud location server and android mobile application.***

Keywords: ***LBS, GPS, Location based query, private information query, Advanced symmetric key, Private information Retrieval.***

Introduction:

A Smartphone is a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps. Aided by affordability of cheap Smartphones and availability of 3G and 4G networks the number of Smartphone users is supposed to reach around 1.75 billion users. Although the growth rate of mobile phone users has reached a threshold in developing countries, the burgeoning increase of users in Asia Pacific, Middle East & Africa is supposed to drive the number of mobile phone users to 4.5 billion users.

In 2012 around 1.58 billion users used their mobile phones for internet, which is around 67% of internet users. The number of users using mobile phones for internet grew by 21% to 1.91 billion users, which is around 74% of internet users. This number is further expected to increase by 17% in 2014 to 2.23 billion users, which is around 79% of total internet users. India is ranked fifth in number of smartphone users and has shown one of the highest year-on-year growth rates (in smartphones). It, however, ranks second in the addition of new users to the Internet over the last five years.



Souce: KPCB's Mary Meeeker report

With the tremendous growth of users in Wireless Technologies (WT), network size also increased. Providing security and privacy to these WT in network is most important factor. The most wireless technology here used is Mobile Technology (MT). Mobile technology is one of the progress factors on behalf of the people. People frequently require anonymity when they roam among the visited networks for their data. While roaming, preventing the resources from anonymous in network is a great issue and also identifying the anonymous in network after their attack requires more communication and computational cost, in recent computational capacity is limited under mobile terminology. To ensure connectivity for users roaming from one network to another, possibly provide roaming services in a secure and private manner.

Location Based Services:

LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine (a.k.a. ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence.

Today the question about LBS (Location Based Services) is not, "what they are inside of," but rather, "what they are not an active part of," and the answer is, "very little". They are a part of virtually all control and policy systems which work in computers today. They have evolved from simple synchronization based service models to authenticated and complex tools for implementing virtually any location based service model or facility.

LBS is the ability to open and close specific data objects based on the use of location and/or time as (controls and triggers) or as part of complex cryptographic key or hashing systems and the data they provide access to. Location based services today are a part of everything from control systems to smart weapons. They are actively used trillions of times a day and may be one of the most heavily used application-layer decision framework in computing today.

Some examples of location-based services are:

- Recommending social events in a city
- Requesting the nearest business or service, such as an ATM, restaurant or a retail store
- Turn by turn navigation to any address
- Assistive Healthcare Systems
- Locating people on a map displayed on the mobile phone
- Receiving alerts, such as notification of a sale on gas or warning of a traffic jam
- Location-based mobile advertising
- Asset recovery combined with active RF to find, for example, stolen assets in containers where GPS would not work

Related Work:

Hyo Jin Jo et al, studied the existing three-party roaming protocol mechanisms and analyze the required assistance of the home servers, and also studied the twoparty roaming protocols have weak security , weak anonymity, insecurity in the CK model, backward linkability, and leakage of the session key or inefficient operations. They were the problem in high authentication and revocation costs. Hence in two-party roaming protocols requires the revocation lists to revoke invalid users. A revocation list includes the revocation information associated with each Revoked User (RU). It uses group signature algorithms to authenticate users anonymously. However, these algorithms generally involve a high revocation cost, depending on the number of RU.

Preserving privacy under personal location is one of the greatest issues in wireless network. They where many approach proposed for the privacy preserving policy under personal location. In many research articles they focus only on anonymization of location techniques but failed to preserve privacy under the network. Some privacy policy may cause data leakage problem because of inefficient algorithms. Many approaches were implemented, which failed to prevent the internal data misuse and privacy preserving policy.

Yan Sun, Thomas F. La Porta and Parviz Kermani proposed a Location-Based Services System (LBSs) for location sharing in social networks. LBS system is used to secure the privacy of the user locations. It secures a user identity and locality within basic mobile communication services. This paper focuses on following aspects: User should be control the access to location information at different levels of granularity and with different levels of user control, user has to define the group of entities that are allowed to access its location information and the main goal of location information is to provide intelligent services to the other users and servers. LBS support location privacy control by the user. It supports user control and scalability. It provides Instant Messaging service for server and clients.

Yan Sun et al approaches is based on offering members of the location information group keys (GKs) that enables them to decrypt the location information. For this GK management this paper proposes a Rebalancing algorithm to maintain rekeying performance with GK management. This article supports the free coupling through a network, thus permit third-party control. This paper provides a protocol like suitable key distribution, Multimedia Internet Keying (MIKEY), and Logical Key Hierarchy (LKH) protocol. These protocols are used to maintain hierarchical location information dissemination for flexible location privacy control for effective message delivery and group management complexity. Hence it does not support the multicast communication. And they were computational cost is also high. They were user anonymity problem from this approach.

Monitoring personal location under untrusted server may cause the privacy problem for the user in wireless sensor network. For this issue Chi-Yin Chow, Mohamed F. Mokbel, and Tian propose a preserving privacy location monitoring system to provide better security to the user. Chi-Yin Chow et al propose a two innetwork algorithm, which are resource and quality-aware algorithms used to protect the location information of the user [4]. Both these algorithms are well established in kanonymity privacy model to indistinguishable among k person’s aggregate locations. Each aggregate location is a cloaked area. This approach provides a high quality for monitoring services for the locations of system user. Hence this approach provides a high quality location monitoring.

The resource-aware algorithm is one which is used to reduce communication and computational cost, while the quality-aware algorithm is used to reduce the size of cloaked areas in order to generate more accurate aggregate locations. Here they use spatial Histogram model to analyze the aggregate locations from sensor node to estimate the monitored objects. Hence this approach reduces the quality of monitoring services; it requires high quality services for larger areas and less privacy protection.

Chunlin Jiang , Weijia Jia and Ke Gu proposed a anonymous authentication protocol based on anonymous proxy signature for wireless communication systems. With the rising number of wireless network with numerous users requires anonymous authentication while roaming among different areas in different networks. Roaming user does not like to identify and tracker their own information to other user, they also want to secure their information while roaming from home network to foreign network.

Chunlin Jiang et al proposed five properties for strong anonymity they were (a) Server Authentication: a user is confident on their identity of the visited server. (b) Subscription Validation: Visited server validates the identity of the home server of the user. (c) Key Establishment: Random session key is established by the user and the visited server which the key is only known to them. In this case, the home server should not acquire the session key. (d) User Anonymity: By this anonymity no one can tell the identity of the user (e) User Untraceability: no one is able to identify any previous protocol runs which have the same user involved including the visited server. So it is hard to tackle these issues because of limited computation and limited storages.

Privacy Issues:

The European Union also provides a legal framework for data protection that may be applied for location-based services, and more particularly several European directives such as: (1) Personal data: Directive 95/46/EC; (2) Personal data in electronic communications: Directive 2002/58/EC; (3) Data Retention: Directive 2006/24/EC. However the applicability of legal provisions to varying forms of LBS and of processing location data is unclear.

One implication of this technology is that data about a subscriber's location and historical movements is owned and controlled by the network operators, including mobile carriers and mobile content providers. Mobile content providers and app developers are a concern. Indeed, a recent MIT study by de Montjoye et al. showed that 4 spatio-temporal points, approximate places and times, are enough to uniquely identify 95% of 1.5M people in a mobility database. The study further shows that these constraints hold even when the resolution of the dataset is low. Therefore, even coarse or blurred datasets provide little anonymity.

Beside the legal framework there exist several technical approaches to protect privacy using privacy-enhancing technologies (PETs). Such PETs range from simplistic on/off switches to sophisticated PETs using anonymization techniques, e.g., related to k-anonymity. Only few LBS offer such PETs, e.g., Google Latitude offered an on/off switch and allows to stick one's position to a free definable location. Additionally, it is an open question how users perceive and trust in different PETs. The only study that addresses user perception of state of the art PETs is. Another set of techniques included in the PETs are the Location obfuscation techniques, which slightly alter the location of the users in order to hide their real location while still being able to represent their position and receive services from their LBS provider.

Privacy protection is especially meaningful and challenging in such an environment. Privacy protection for the roaming user is one of the increasing factors for people that care about their privacy. A roaming user's privacy is like a movement model, extracting information, network usage habit, etc. should be protected from possible enemy intend to break users' privacy. Protecting the privacy of the roaming user in wireless network have to solve the following problems have to protect the user identity, user data, user location information and user likability between the home and foreign server.

EXISTING SYSTEM:

The Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBS has to ensure that LS's data is not accessed by any unauthorized user. During the process of transmission the users should not be allowed 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 also prevent users from accessing content to which they do not have authorization.

DISADVANTAGES OF EXISTING SYSTEM:

- 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,

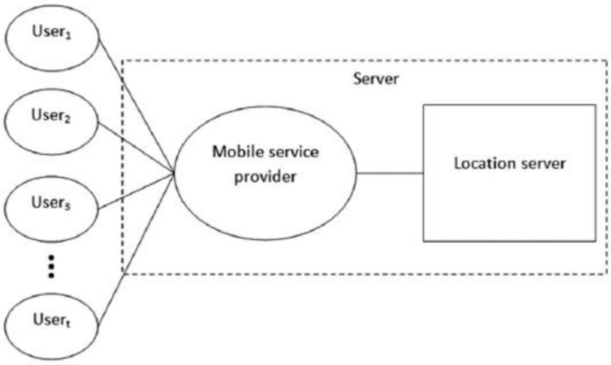
PROPOSED SYSTEM:

- In this paper, we propose a novel protocol for location based queries that has major performance improvements with respect to the approach by Ghinita at el. And. Like such protocol, our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using 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 user executes a communicational efficient PIR, to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.
- Our 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. In other words, users cannot gain any more data than what they have paid for. We remark that this paper is an enhancement of a previous 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.

SYSTEM ARCHITECTURE:



Implementation Modules:

1.Sysetem Model
2.Protocols Description
i. Global Initialisation
ii. Oblivious Transfer Based Protocol
3. Security Analysis
i. User's security
ii. Server's security
4. Private Information Retrieval Protocol

System Model:

The users in our model use some location-based service provided by the location server *LS*. Each record describes a POI, giving GPS coordinates to its location (*xgps*, *ygps*), and a description or name about what is at the location. We assume that the mobile service provider *SP* does not interfere with the communications between the user and the location server. This means that the mobile service provider does not collude with the location server to attack the privacy of the user. As a consequence of this assumption, the user is able to either use GPS (Global Positioning System) or the mobile service provider to acquire his/her coordinates. Since we are assuming that the mobile service provider *SP* is trusted to maintain the connection, we consider only two possible adversaries. One for each communication direction. We consider the case in which the user is the adversary and tries to obtain more than he/she is allowed. Next we consider the case in which the location server *LS* is the adversary, and tries to uniquely associate a user with a grid coordinate.

Protocols Description

Before describing our protocol we introduce the system model, which defines the major entities and their roles. The description of the protocol model begins with the notations and system parameters of our solution.

Global Initialization:

A user *u* from the set of users *U* initiates the protocol process by deciding a suitable square cloaking region CR, which contains his/her location. All user queries will be with respect to this cloaking region. The user also decides on the accuracy of this cloaking region by how many cells are contained within it, which is at least the minimum size defined by the server. This information is combined to form the public grid *P* and submitted to the location server, which partitions its records or superimposes it over pre-partitioned records. This partition is denoted *Q* (note that the cells don't necessarily need to be the same size as the cells of *P*). Each cell in the partition *Q* must have the same number *rmax* of POI records. Any variation in this number could lead to the server identifying the user. If this constraint cannot be satisfied, then dummy records can be used to make sure each cell has the same amount of data. We assume that the *LS* does not populate the private grid with misleading or incorrect data, since such action would result in the loss of business under a payment model.

Oblivious Transfer Based Protocol:

The purpose of this protocol is for the user to obtain one and only one record from the cell in the public grid *P*. We achieve this by constructing a 2-dimensional oblivious transfer, based on the ElGamal oblivious transfer , using adaptive oblivious transfer3 proposed by Naor et al. The public grid *P*, known by both parties, has *m* columns and *n* rows. Each cell in *P* contains a symmetric key *ki,j* and a cell id in grid *Q* i.e., (*IDQi,j*, *ki,j*), which can be represented by a stream of bits *Xi,j* . The user determines his/her *i, j* coordinates in the public grid which is used to acquire the data from the cell within the grid. The protocol is initialized.

Security Analysis:

User's security:

The user does not want to disclose the cell *Pi,j* which contains his/her location to the server. Two assumptions must be maintained in order to effectively render location private. The server must not be able to determine which cell the user is querying in the oblivious transfer protocol, and the server must not be able to determine which cell the user is querying in the private information retrieval protocol. The oblivious transfer assumption is based on the discrete logarithm assumption. This essentially means that given *gx* (*mod p*), where *p* is a large prime and *g* is a generator of some cyclic group, it is computationally infeasible to determine *x*. In our case, if the user supplies (*gr*1, *g*−*iyr*1) and (*gr*2, *g*−*jyr*2) to the server, then the server is unable to determine *i* and *j*. If the discrete logarithm assumption holds, then we claim this is secure.

Server's security:

The server's security is based on keeping the boundaries of its records private. Since disclosing this information may enable the user to infer more information about the database than he/she is allowed. In our solution this information is protected by the oblivious transfer protocol. The user is forced to retrieve one and only one record from the public grid *Pi,j* All other times, the result will be indistinguishable from random. Under the discrete logarithm problem assumption, it is computationally intractable to determine any exponent from the cipher text. Hence, the user is only able to determine one and only one result.

Private Information Retrieval Protocol:

The oblivious transfer based protocol there are 3 major steps: the user's query, the server's response, and the user decoding. The average time required for each of these major components are presented in Table IV.

Based on these experimental results, most of time is taken by the generation of the user's query. This is due to the primality testing of *Q*0 and *Q*1. This requirement must be satisfied, otherwise . The average of the response time and the decoding time are much smaller in comparison. We assume that the server has much more computational power at its disposal. Hence, if there are many users, the server can use parallel processing to increase the throughput of the protocol. The main concern is keeping the query time for the user as low as possible, and on average the user query time is reasonable, given the amount of data that is exchanged in one round of the protocol.

Conclusion:

In this paper we have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is used for a user to privately determine his/her location using oblivious transfer on a public grid. The second step involved a private information retrieval interaction that retrieves the record with high communication efficiency. We analysed the performance of our protocol and found it to be both computationally and communicationally more efficient than the other existing solutions.

REFERENCES:

[1] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, Fellow, IEEE "Privacy-Preserving and Content-Protecting Location Based Queries" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 5, MAY 2014

[2]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.

[3]G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearest neighbour queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010.

[4]B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in Proc. ICDE, Hannover, Germany, 2011, pp. 494–505.

[5]G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacy preserving matching of spatial datasets with protection against background knowledge," in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12

[6] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearest neighbour queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010

[7]R.Paulet,M.GolamKaosar,X.Yi,andE.Bertino,"Privacypreserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53

[8] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against locationbased personal identification," Proc. Secure Data Management, Lecture Notes in Computer Science, W. Jonker and M. Petkovic, Eds., 2005, vol. 3674, pp. 185 - 199.

[9] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965 - 981, 1998.

[10] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," Proc. Pervasive Computing, Lecture Notes in Computer Science, H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, vol. 3468, pp. 243 - 251