RESEARCH PAPER | Engineering | Volume : 4 | Issue : 12 | Dec 2014 | ISSN - 2249-555X

Private Location Based Query Using Third Party Identity Diffuser: a Review

KEYWORDS: Location Privacy, Location-based Services, LBS, Privacy Preserving Approaches

Megha K. Chavda
PG Research Scholar, Department of Computer Engineering, Noble Group of Institutions, Junagadh,

Dr. Vipul Vekariya
Associate Professor, Department of Computer Engineering, Noble Group of Institutions, Junagadh,

ABSTRACT *Privacy Concerns in LBS exist on two fronts: location privacy and query Privacy. In this paper we investigate issues related to query privacy. In particular, we aim to prevent the LBS server from correlating the service attribute. An important privacy issue in Location Based Services (LBS) is to hide a user's identity while still provide quality location based services. Recently, highly accurate positioning devices enable us to provide various types of location-based services. On the other hand, because position data obtained by such devices include deeply personal information, protection of location privacy is one of the most significant issues of location-based services. Therefore, we propose a technique to anonymize position data. In our proposed technique, the personal user of a location-based service generates several false position data (dummies) sent to the service provider with the true position data of the user. Because the service provider cannot distinguish the true position data, the user's location privacy is protected. But from this method traffic will be increase. As a solution, a diffuser can be placed between mobile unit location based services. Diffuser will send dummy locations to LBS and true data exchange will only be happen between mobile unit and diffuser. The traffic between mobile unit and diffuser will be decrease.*

1. INTRODUCTION

Availability of low cost Smartphone with good processing capacity and equipped with various positioning technology have powers location based services (LBS). Popularity of LBS is dramatically increasing among mobile users day by day. Consumers are understand and adopting LBS worldwide. Study shows that there are 486.0 millions mobile location based service users worldwide by year 2012 [1]. There is 47.7 % change in users from previous year. Today's smart phones, tablets and connected devices are virtually all GPS enabled thus allowing for a myriad of LBS like Geo-fence services: friend/family tracking, Enterprise Fleet Tracking, Travel and Point of Interest (POI), Geo-tagging, Check-in Based Contest and Games, Local search, Local/Hyperlocal Content, etc.

Almost all of the above LBS use location server that knows about location of users in order to provide customized services. Sometimes verify authenticity of location server is not possible. However, Users of LBS have to share their location information with these location servers to use their services. Some unauthorized and un-trusted location server may leak or misuse location information of their subscriber these leads term location privacy. Several issues of misusing their location information by service provider are reported worldwide. Many researchers have work toward this problem. There are many approaches and techniques to preserve privacy in LBS, but there are some strengths and weaknesses in every approach. In this paper we have analyzed each approach and highlighted their strengths and weaknesses. As illustrated in Figure 1, these approaches can be classified into groups based on the techniques they use. The groups are cloaking, transformation, obfuscation, private information retrieval (PIR).

To protect against various privacy threats while using LBS, several studies have proposed different approaches to protect the privacy of users while interacting with potentially untrusted location servers, hence coining the term location privacy. In this paper, we present a taxonomy of approaches proposed for the location privacy problem. As illustrated in Figure 1, these approaches are based on anonymity/cloaking, transformation and private information retrieval (PIR) techniques. We study each group in more details and briefly show how each approach supports sample spatial queries used in LBS.

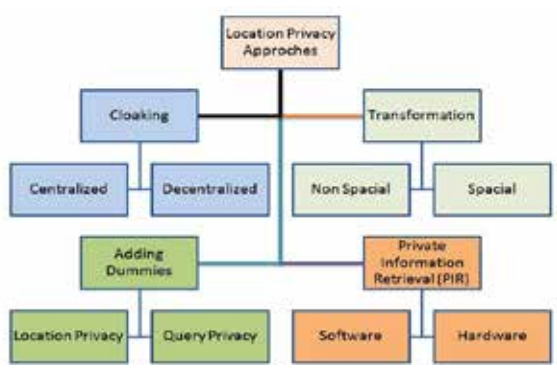

Fig -1: Location Privacy Approaches

This paper organized as follow. In section 2 studies group of cloaking and adversary attacks on cloaking, section 3 discuss various techniques of transformation, while section 4 and 5 discuss about obfuscation and private information retrieval (PIR) techniques and possible adversary attacks to break these techniques.

2. ANONYMITY

The main idea behind the class of anonymity/cloaking approaches is to blur a user's exact location in a larger cloaked region and to make her indistinguishable among the set of other (real or dummy) users located in the cloaked region. Depending on where the cloaking is taking place, these approaches can be grouped into two classes of centralised and decentralised cloaking.

Volume : 4 | Issue : 12 | Dec 2014 | ISSN - 2249-555X

2.1 Centralized Cloaking

Many existing approaches in location cloaking rely on the existence of a trusted location anonymiser which protects a user's private location and identity information from an untrusted location. The main idea in centralised cloaking is to put an anonymiser between the users and the location server to prevent the server from learning users' precise location information and identities.

The main idea behind centralized cloaking is to put a trusted location anonymiser between users and location based server[2]. Location anonymiser works like a proxy webserver, it receives query from many users and form one cloaked region and send this cloaked region to location based server instead of single user's location.Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here.

2.1.1 Architecture & Query Processing

Figure illustrates the system architecture for centralized cloaking framework. The framework consists of a location anonymiser and an untrusted location server which hosts a privacy-aware query processor. In order to enable location privacy, the anonymiser maintains the current locations of all subscribed users. Instead of sending the location query to the LBS, the user contacts the anonymiser, which generates a cloaked region enclosing the user as well as k – 1 other user in her vicinity.

The system architecture of centralized cloaking contain location anonymiser between LBS users and LBS server as shown in figure2.

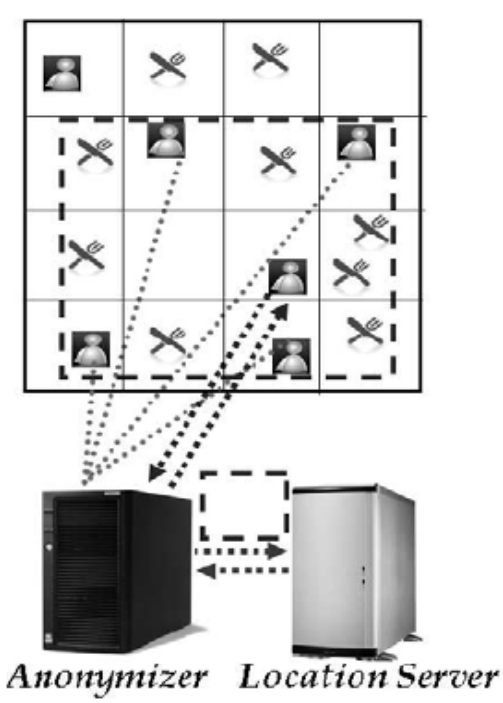

Fig -2: Architecture of centralized cloaking

With this technique LBS query issued to LBS server by user is executed via trusted location anonymiser. The location anonymiser augments a user's location to a cloaking region, which geographically covers not only the user who issues the query but also k – 1 other users, and then transmits the query to the LBS server. Since all the k users report the same cloaking region in their queries, the adversary cannot distinguish the location or service attribute of any user from the received queries.

As processing anonymised nearest neighbour queries is more complex than anonymised range queries, we focus on how nearest neighbour queries are processed with cloaking-based approaches. Among the central cloaking approaches that consider the query processing of the cloaked region, the end-to-end query resolution process can be divided in the following two phases. First, upon receiving a query, the anonymiser employs a cloaking algorithm to generate a cloaked region. While different algorithms are proposed for cloaking a user's location, the common objective is to blur a user's location in an area of size at least Amin and/or among a set of at least k – 1 other users. Depending on the approach, these parameters can be specified by each user independently, or are chosen as system parameters. During the second phase, the privacy-aware location server, which is modified to process a cloaked region query, generates a candidate list which is guaranteed to include the nearest neighbour of any point inside the cloaked region. This list is then transferred to the client side for further refinement to obtain the final result set.

2.1.2 Strengths and Weaknesses

Centralized cloaking support various queries like KNN, range query and other spatial queries until location based server support queries based on cloaked region.[5] One of the key benefits of centralized cloaking approaches is the fact that the sophisticated anonymiser can perform various complex operations to enable an untrusted server to process complex queries. In other words, range, KNN and other types of spatial queries can be easily supported as long as the privacy-aware server is instructed to perform such queries on a cloaked region. Allowing an anonymiser to continuously monitor the exact location of all users greatly reduces the challenges associated with supporting queries over dynamic objects (e.g., a nearby friend).

Centralized cloaking has several drawbacks. The first drawback of such approaches originates from the fact that by design they require an anonymiser, as sophisticated as the location server itself, to act as a proxy between users and the server per query. Anonymiser is a single point of failure/attack and bottleneck, this approach has another important drawback. In many scenarios cloaking users' location information in a larger region or among k – 1 other user does not protect user's location information. This is due to the fact that based on user distributions in the space and the value of k (or similarly size of the cloaked region), precise user location can be derived using several techniques such as monitoring a sequence of queries over time, correlation attacks or reasoning about the possible location of the query point.

2.1 Decentralized Cloaking

Centralized cloaking approach has several drawbacks. To solve these drawbacks many researchers proposed non-centralized approach to construct cloaked region. The main intension behind decentralized approach is to re-

Volume : 4 | Issue : 12 | Dec 2014 | ISSN - 2249-555X

move centralized anonymiser between user and server and work without centralized anonymizer using same principle of cloaking.[4] Anonymising a user's query by a trusted anonymiser has several drawbacks. To address the drawbacks of centralized cloaking, several studies propose the non-centralised approach in constructing the cloaked region.

2.1.1 Architecture and query processing

The overall architecture of decentralized approach is depends on many LBS users as shown in figure 3. In this approach peer-to-peer spatial cloaking algorithm is use to form cloak region.

The approaches proposed by Chow et al. (2006) assume users communicate with each other to collaboratively form a cloaked region. The cloaked region in Chow et al. (2006) is constructed by having each user communicating with other users around its vicinity until it finds enough users to form a cloaked region which contains k users.[4] If enough users are not found, each request receiver recursively broadcasts the request until k users are found. Once cloaked region is constructed by LBS users, one user communicates with server on behalf of other users of cloaked region.

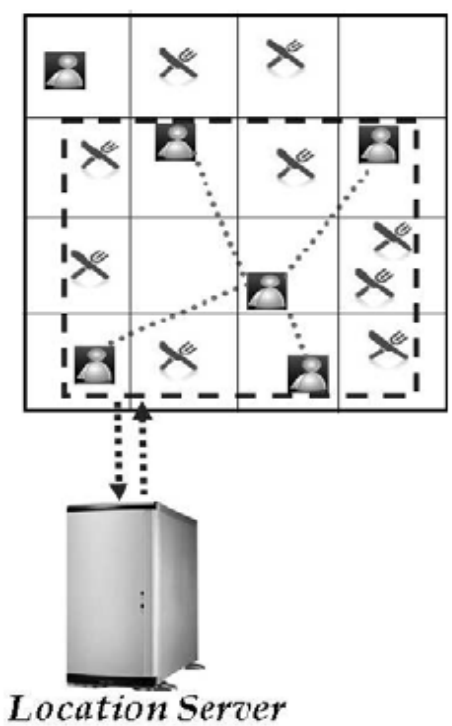

Fig -2: Architecture of Decentralized cloaking

In order to avoid a central anonymiser, the use of user-generated dummies to make a user's exact location indistinguishable in an anonymity set which contains the locations of the dummy users as well as the user's exact location. Depending on the availability of other users' location information to the user querying the system (via communicating with other users), two variants of generating dummies are proposed.

The peer-to-peer spatial cloaking algorithm discussed above is shown to have significant privacy leaks for many user distributions since the user initiating the query is usually located close to the centre of the cloaked region. Hierarchical overlay network resembling a distributed B+ tree for constructing the cloaked region that overcomes the above drawback. However, it suffers from very slow response time. The authors propose a distributed method to find a random set of k adjacent users based on their 1-D Hilbert ordering. Finally, Duckham and Kulik (2005) propose a graph model to represent possible user's locations and denote the cloaked region by a set of vertices in the graph. The client progressively gives more information about her precise location until the query result set reaches her desired accuracy. This study does not consider the query processing.

2.1.1Strengths and Weaknesses

The major strength of decentralized approach is that it does not require centralized anonymizer between user and LBS server and still work same as centralized cloaking. It can perform all type of query operation similar to centralized cloaking.

The most obvious superiority of decentralised cloaking approaches to their centralised peers is avoiding a central trusted anonymiser. Similar to centralised cloaking, processing complex spatial queries is feasible as long as the privacy aware server can perform them on a cloaked region. Finally, processing a spatial query for each member of the anonymity set as proposed by Kido et al. (2005) and Duckham and Kulik (2005) further simplifies the framework since their proposed methods can be built on top of any of the conventional spatial query processing algorithms currently in use.

With these advantages of decentralized approach it increases privacy threat in some cases. Attacker can get location information of user from observing several snapshots of cloaked region in continue queries. Another drawback of decentralized approach is communication cost to form large cloaked region using peer-to-peer architecture. Finally, decentralized approach assumes that all users in cloaked region making process are trusted. In real world this assumption may not work.

3. TRANSFORMATION

Transformation technique is based on transforming the query into another form to prevent the server from learning information about the user's locations. They can be divided into two different groups: non-spatial and spatial transformation-based techniques. It is presented a class of approaches that do not employ cloaking techniques and anonymisers transformation-based approaches since they are based on transforming the query to prevent the server from learning information about the users locations. Although all approaches discussed in this section utilize transformation to protect user's private location information, based on the proposed transformation scheme, they can be divided into two different groups: non-spatial and spatial transformation-based techniques to achieve anonymity.

3.1 Non-spatial Transformation

The class of approaches under this category is mainly based on the shoulders of applied cryptographic protocols to achieve privacy (Indyk and Woodruff, 2006).[7]With these approaches, the query is evaluated in an encrypted space. Therefore, the transformation employed is some form of encryption.

Volume : 4 | Issue : 12 | Dec 2014 | ISSN - 2249-555X

3.1.1 Architecture and query processing

The class of non-spatial transformation techniques blinds the un-trusted party (i.e., the server or another user) by utilizing secure multi-party computation schemes.

The scheme proposed by Indyk and Woodruff (2006) involves a two-party computation protocol between Alice and Bob to privately evaluate the distance between Alice's point and other n points that Bob owns. After executing the protocol, Bob knows nothing about Alice's point and Alice only learns the nearest neighbor from Bob's points. Although the solution proposed is mainly of theoretical interest and does not focus on spatial queries or LBS, it can be considered as a method for protecting users' privacy in LBS. In other words, one can think of a privacy-aware LBS framework by treating Bob as an un-trusted server and Alice as a user interacting with the server.

Zhong et al. (2007) propose three solutions to what they define as the nearby-friend problem. The problem is defined as allowing users to learn information about their friends' locations if and only if their friends are actually nearby. The three protocols are all efficient in terms of the amount of computation and communication required by each party. Each protocol is an instance of a multi-party computation scheme with certain strengths and restrictions (in terms of number of messages transferred and the resilience to a malicious party).

3.1.2 Strengths and Weaknesses

The main advantage of this type of approaches under this category is that it provides perfect privacy. The framework of this approach is based on standard cryptographic protocol, so, it doesn't suffer from major privacy leak.

However, with the above decentralized approaches, the privacy threats are even more significant as the server knows the exact location of the user is provided in the anonymity set. Therefore, monitoring a sequences of queries can easily reveal valuable information to the server about the real location of the user. More importantly, in cloaking approaches, users should in fact trade-off their privacy with the accuracy of the query result or the efficiency of the query processing because a larger anonymity set (or similarly, the cloaked region) may result in a significantly larger query result set which includes many unnecessary data points that should be filtered. Furthermore, forming a large anonymity set prohibitively increases the communication cost between the users in the peer-to-peer architecture. Alternatively, decreasing k (or the size of the cloaked region) will directly increase the probability of identifying the user's location. Therefore, preserving users' location information might not always be possible regardless of the size of k (or the cloaked region). Finally, decentralized techniques assume all users subscribed to a service are trusted in order to collaboratively create the cloaked region. This assumption might be far from reality in typical LBS frameworks.

The major drawback of non-spatial transformations is their high computation or communication complexity when being used for spatial query processing. Further, it cannot support all type of query.

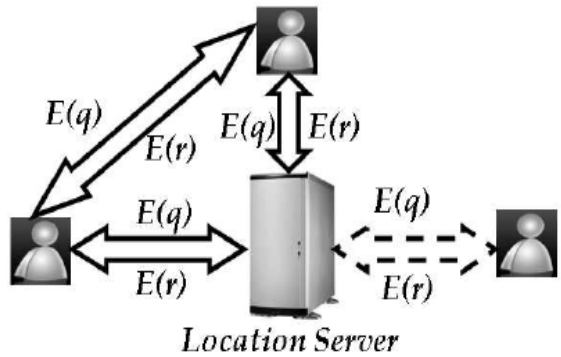

Fig -4: Location Server Algorithm

3.2 Spatial Transformation

The main idea behind the techniques under this category is to somehow blind the server from learning the exact query location while still preserving the locality of objects.

3.2.2 Architecture

Lin(2006) proposed one architecture for anonymous LBS with a transformation based approach through the several intermediate agents. The main idea behind this architecture is to modify users and query location information through the use of various geometric transformations such as translation, rotation and scaling. The architecture utilizes several agents interposed between users and service providers to perform the transformations. The agents serve as intermediaries and do not store user information since their only responsibility is to transform information received from other users or the server (Figure 4). To preserve privacy, users randomly choose the agent to perform the transformation.

3.2.2 Strengths and Weaknesses

The main advantage of spatial transformation is that it preserves locality of object. The framework of Lin (2006) supports wide range of spatial queries such as KNN and range queries. Algorithm also answers exact result for spatial queries.

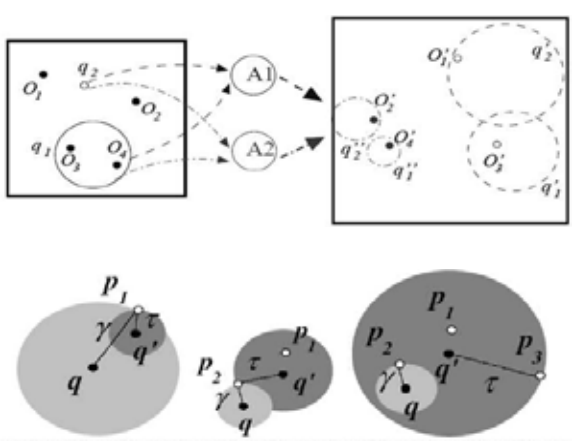

Fig -5: Architecture of Spatial transformation
Image Source: Lin(2006)

This approach also suffers for some weaknesses which is common in all solid geometric transformation. A careful comparison of the original dataset with the transformed version can reveal significant amount of information to the server to reverse the transformation. This approach also requires trusted intermediate agents because users have

Volume : 4 | Issue : 12 | Dec 2014 | ISSN - 2249-555X

to share their location information to the agents this may brings several issues of trust.

4. ADDING DUMMIES

The main idea behind the techniques under this category is to disguise user's location or query by adding some random noise or false location data ('dummies') into real location. LBS user sends several dummies with real location to LBS server so an adversary cannot identify which is true location of user among several dummy locations. There are two privacy preserving approach using dummies: location privacy and query privacy.

4.1Location Privacy

Location privacy means adversary cannot distinguish true location of user. In this technique a user sends true position data with several false position data ('dummies') to a service provider, who creates a reply message for each received position data.

4.1.1 Architecture

Kido(2005) proposed architecture for anonymous use of LBS using dummies. In this architecture anonymity is generated at user side so there is no need of trusted third party. User sends several location dummies with true position data.

e.g. Assume Lx = (X1, Y1) shows location of a user at time t. A message S from the user to request a service is of the form:

S = (u,L1,L2, _ _ _ , Lk)

Where u shows a user ID and (L1,L2, _ _ _ , Lk) shows a set of position data that includes one true position data and k-1 dummy locations. This request is sent to service provider. On the other hand, a service answer message R from the service provider to the user is of the form:

R = ((L1,D1), (L2,D2), _ _ _ , (Lk,Dk))

Where (D1,D2, _ _ _ ,Dk) shows the reply of the service request corresponding to the locations (L1,L2, _ _ _ ,Lk). Here other k-1 locations sent with the actual location of user are considered as noise data/dummies consisting of false position data. On getting the reply in the above mentioned form user filters the data required according to his true location. The user simply extracts the necessary information from the reply message. Hence user's true location is kept hidden from location server. In this manner, even if the service provider stores the set of position data, it cannot distinguish the true position data from the set of fake position data.

Fig -6: Preserving location privacy using dummies

Image source: Kido(2005)

4.1.2 Strengths and Weaknesses

In other privacy preserving approach trusted third party anonymiser or middleware is required which creates many problems, While this technique doesn't required any middleware because anonymity is generated only at client side.This technique sends dummies with true position data, so it increases communication cost of LBS.

4.2Query Privacy

Query privacy means adversary cannot identify real point of interest from query. Query privacy can be achieved by sending several fake point of interest(POI) with real POI in user's query.

4.2.1 Architecture

Authors in [9] proposed architecture named as DUMMY-Q, for query privacy protection which operates solely on the user side and does not require any trusted third party. The key idea is to confuse the adversary by issuing multiple counterfeit queries with varying service attributes but the same (real) location, henceforth referred to as dummy queries, along with each real query issued by the user. Aim of the proposed technique is to prevent the LBS server from correlating the service attribute. Authors in [9] claimed that in case of continuous LBS scenarios effectiveness of location obfuscation using spatial generalization aided by anonymization has been abated. So a query-perturbation-based scheme that protects query privacy in continuous LBS even when user identities are revealed is proposed.

4.2.2 Strengths and Weaknesses

This technique can preserve query privacy even in continues LBS without any middleware because it generate anonymous query at user side.

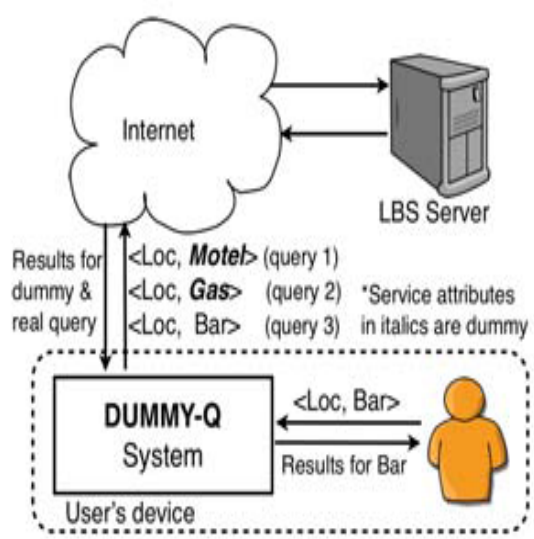

Fig -7: Preserving Query privacy in DUMMY-Q

Image source: Pingley, Aniket, et al.(2011)

This technique requires sending several dummy service attribute for single query search so it increase communication cost.

Table -1:

Comparison of different classes of proposed approaches for location privacy

Volume : 4 | Issue : 12 | Dec 2014 | ISSN - 2249-555X

Technique	Reference	Query type	Major strengths	Major weaknesses
Centralized cloaking	Mokbel et al. (2006), Gruteser and Grunwald (2003), Gedik and Liu (2005a, 2005b) and Du et al. (2007)	Range/ KNN	Spatial query support, support for querying dynamic data	Major privacy leaks, trusting a third party, privacy/quality of service trade-off
Decentralized Cloaking	Duckham and Kulik (2005), Kido et al. (2005), Ghinita et al. (2007b, 2007c) and Chow et al. (2006)	Range/ KNN	No need for a centralized anonymiser, Stronger privacy support compared to centralized cloaking	Costly communication complexity, assuming all users are trusted, privacy leaks, privacy/ quality of services trade-off
Non-spatial Transformation	Indyk and Woodruff (2006)and Zhong et al. (2004, 2007)	Customized two-party computation queries (private distance approximate, private co-location comparison, etc.)	Perfect privacy guarantee, very efficient customized Queries	Prohibitive linear computation or communication complexity for classic spatial queries
Spatial Transformation	Lin (2006), Khoshgozaran and Shahabi (2007) and Yiu et al.	Range/ KNN	Efficient spatial query processing, support for querying dynamic objects	Privacy leaks under certain object distribution, privacy/ quality of service trade-off
Dummy Queries	H. Kido (2005), IEEE	All types of Queries	Perfect privacy guarantee, Reliable	Network Traffic Overhead, High computation and communication complexity
Third Party identity diffuser	Proposed	All types of queries	Security, Avoiding location of individual, Avoid network overhead	Third party Identity diffuser required

5. CONCLUSION

This paper presented three distinct classes of approaches proposed for protecting users' location information in LBS. The first class of approaches, based on cloaking and anonymity techniques, offer flexible schemes to support privacy-aware location servers responding to various spatial queries. However, they suffer from multiple privacy leaks under certain user or query distributions. The second classes of approaches are based on transforming the queries to blind the server from knowing a user's location while evaluating location queries. With these approaches, users have to trade-off their privacy with the quality of service they receive from location-based services. Finally, the third class of PIR approaches addresses all privacy concerns of the previous approaches. However, they incur expensive computations or rely on a trusted platform to execute the queries. Table 1 summarizes the properties of each category of approaches. Each table column represents the dominant properties shared among the proposed approaches under each category. Location privacy research is still in its infancy. While creative solutions have been proposed to solve the location privacy problem, there are still many challenges to be addressed. Devising a framework that while ensuring perfect privacy, can very efficiently respond to various spatial queries dealing with both static and dynamic objects is still an open problem and far from what the existing approaches offer.

REFERENCE M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", 2003, MobiSys, pp.31–42 | [2] W. S. Ku, Y. Chen and R. Zimmermann, " Privacy Protected Spatial Query Processing for Advanced Location Based Services", Springer Science+Business Media, LLC. 2008 | [3] A. Masoumzadeh, J. Joshi, "An Alternative Approach to k-Anonymity for Location-Based Services", Procedia Computer Science 5 (2011) 522–530 | [4] Mokbel, M., Chow, C. and Aref, W. (2006) 'The new Casper: query processing for location services without compromising privacy', VLDB, pp.763–774. | [5] Chow, C., Mokbel, M. and Liu, X. (2006) 'A peer-to-peer spatial cloaking algorithm for anonymous location-based service', GIS, pp.171–178. | [6] Indyk, P. and Woodruff, D. (2006) 'Polylogarithmic private approximations and efficient matching', TCC, pp.245–264. | [7] Kido, H., Yanagisawa, Y. and Satoh, T. (2005) 'An anonymous communication technique using dummies for location-based services', IEEE International Conference on Pervasive Services, p.1248. | [8] A. Pingley, N. Zhang, X. Fu, H.-Ah Choi, S. Subramaniam, and W. Zhao "Protection of Query Privacy for Continuous Location Based Services", IEEE INFOCOM, 2011. | [9] Mobile Marketing Association, "MOBILE LOCATION BASED SERVICES MARKETING WHITEPAPER", October, 2011. |