Journal of Theoretical and Applied Information Technology
15th August 2018. Vol.96. No 15
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY: THE CURRENT TRENDS OF PRIVACY TECHNIQUES FOR PROTECTING THE LOCATION PRIVACY OF USERS IN LBS

[1]ABDULLAH ALBELAIHY, [2] JONATHAN CAZALAS, [3]VIJEY THAYANANTHAN
[1]King Abdulaziz University, Department of Computer Science, Saudi Arabia
[2]Florida Southern College, Department of Computer Science, Lakeland, Florida, USA
[3]King Abdulaziz University, Department of Computer Science, Saudi Arabia
E-mail: [1]aalbelaihy{at}stu.kau.edu.sa, [2] jcazalas{at}flsouthern.edu, [3] vthayanathan@kau.edu.sa

ABSTRACT

With GPS-enabled devices and data connectivity now ubiquitous, Location Based Services (LBSs) have seemingly penetrated all aspects of our lives. While profoundly valuable, these services expose the user to a litany of privacy and security issues. LBS users must reveal their location, and at times other sensitive personal information, in order to effectively use the service and receive accurate results. This paper presents a survey of the current trends of privacy techniques employed in protecting the location privacy of users in LBSs. The paper further highlights the efficacy, or otherwise, of each technique discussed in this paper, with each technique having been evaluated based on accuracy, quality, efficiency, flexibility, location privacy, and query privacy. The outcome of this study is a taxonomy of current privacy and security techniques, which will assist researchers and developers as they look to further protect the sensitive information of their customer base.

Keywords: *Privacy, Bloom filter, LBS, Oblivious transfer, Dummy locations, Zero knowledge.*

1. INTRODUCTION

Location-based services have become ubiquitous as the Internet of Things (IoT). Although the goal of IoT is to provide network communication services to any user, no matter the time, regardless of their location; through modern devices, like a GPS, the connection of all things can be achieved via RFID, Wi-Fi, 3G-4G networks, and Bluetooth, etc. are made easy. As such, locating the geographic positions of individual users with these devices is becoming more accurate and portable, and this can be achieved with low cost and low-powered devices.

Consequently, location-based services (LBSs) are gaining more popularity and provide more avenues to understand the environment better. By requesting a personalized location-based service from a particular LBS server, for the task to be provided, the user is required by the location-aware application to disclose his or her exact position, which requires that the content and relevant information about the user's location be revealed [1].

However, an issue concerning the privacy of the user has been raised in the course of tracking the user, as it has revealed relevant and important, private information about the user and their location [2]. According to [3], the information can be gained through the user's position at any point, and at any time. The more data disclosed about a user, the more the user is accurately profiled. The fact that individual users are becoming more adept at using smartphones and location-based services, it is becoming more difficult for individuals to give up using smartphones, and, therefore becomes reasonable to envision that more privacy of location information will be requested by users [4] [5] [6]. Hence, the challenge facing the service provider is the protection of the users' privacy and still delivering services based on the users' location [7].

Normally, location-based services require that the service providers know when a user is close to some points of interest POIs (e.g., restaurant locations), which is often used in "around-me" applications. Some find POI, using a point location to be interesting and useful. Considering any specific point on the Earth, location is seen as significant point by a provider; this point is specified using the longitude and latitude of the POI through collected map data. A name and description are typically included, and other information, like the altitude or phone number of the location. The POI has different categories, and GPS applications will usually use icons to show this on the map [3]. However, the situation requires that the location of the user be kept private, as long as the user is in no way near any POI and only gets revealed once they are close to POIs. Example: searching for the nearest Pizza Hut, when you ask your phone to find the nearest Pizza Hut; the server cannot answer the query unless you first tell the server where you are located. Therefore, you must reveal your location. What is the problem with this?

Adversaries: those who want to steal and use your location and identity in harmful ways. So it is a problem to reveal your information. As such, several techniques have been employed by past researchers to improve and ensure the optimal privacy of the queries submitted by mobile users in LBSs. The goal is to be able to provide accurate answers to user LBS queries while providing guarantees with respect to privacy and efficiency.

As expected, this goal raises several difficult research problems in privacy and security. The issue is any information leakage in a secure system is bad. If one bit is leaked per query, and thousands of queries are made, then it may be possible for the attacker to learn some information that should remain secret. Nevertheless, there is no study, offered previously according to our knowledge that explores the negative of leakage attacks (Malicious servers/nodes) on the LBS privacy protection approaches.

As such, several techniques have been employed by past researchers to improve and ensure the optimal privacy of the queries submitted by mobile users in LBSs.

This paper examines the approaches that might be used to increase privacy in a location-based server. These methods, i.e., Zero-Knowledge Proofs, Oblivious Transfer, Dummy locations, Mix zone, k-anonymity and Bloom Filters.

Even though a lot s of work has been done on these methods in a general cryptographic area, unlike that in the LBS area a little work has been done in terms of their application to LBS privacy. Each method has its own advantages and disadvantages.

Therefore, this paper aims to survey the recent trends of the techniques used to ensure the privacy of mobile users in LBS by highlighting the efficiency and deficiency of these techniques.

In general, our contributions are as follows:

- We introduced the current trends of privacy techniques employed in protecting the location privacy of users in LBSs and proposed privacy protection in LBS field.
- We examine the technologies that might be used to increase privacy in a location-based server system. These technologies are like Zero Knowledge Proofs, Oblivious Transfer, Dummy locations and Bloom Filters. While a great deal of work has been done on these technologies in a general cryptographic setting, relatively little work has been done in terms of their application to LBS privacy. Each technology has its own strengths and weaknesses, and each will be examined in turn.
- We highlight the efficiency and deficiency of each technique.
- We explore, analyze and evaluate the current trends of privacy techniques on the LBS privacy protection based on accuracy, quality, efficiency, flexibility, location privacy and query privacy.
- We suggest a new scheme based on a privacy algorithm scheme for LBS based on a modified Hilbert Curve algorithm, and it is purely peer-to-peer based.

The remainder of the paper is organized as follows. Section 2 shows the preliminaries contains the basic concepts of privacy, the trend of research on location privacy in LBSs and suggests a new scheme. The outcomes of trends of research are discussed in Section 3. Lastly, concluding remarks and future work is given in Section 4.

2. PRELIMINARIES

In this section of the paper, the basic concepts of privacy will be discussed in general, followed by the oblivious transfer and bloom filter techniques, which are the current trends in protecting mobile users' privacy in LBSs. This paper will further highlight the efficiency and deficiency of each technique discussed in this paper.

2.1 The Basic Concepts of Privacy

Protecting the privacy of mobile users in LBSs has been revealed by previous researchers that the anonymity of the real locations of mobile phone users was majorly used. Recently, several privacy techniques have been trending for location privacy protection of mobile users. For example, in this paper [8], there is an academic study entailing interactive hashing.

The paper begins by introducing the notion of interactive hashing as a cryptographic primitive while differentiating it from the specifics of the implementations it may present. In this regard, this paper showed application-independent information ideal conditions that must be ideally satisfied by the interactive hashing. Moreover, Author provides in detail an analysis of a standard implementation of interactive hashing that meets all the conditions of our definition. From the analysis, get that it represents improvements in restricted contents than in previous attempts. In spite of its generality, the interactive hashing offers a simpler proof of security, which establishes security from a dishonest sender hence reducing his or her probability of cheating.

To prove that a sender who tries to manipulate the protocol in a way that makes it possible for output strings to have a uniquely desirable property would represent a fraction of all the strings from which the probability of both outputs will be from the set.

Also, showed the power of interactive hashing as a cryptogrammic tool by looking into the protocols achieving oblivious transfer and which characteristically depends heavily on interactive hashing.

2.2 The trend of Research on Location Privacy in LBSs

According to [9], the real information of mobile users can be concealed from k-anonymity into k-1 of other users. Entropy-based metrics have also been used in ensuring the privacy protection of mobile phone users. Voronoi graph partition on road networks is another method to achieve privacy, query sending, and k-anonymity [10].

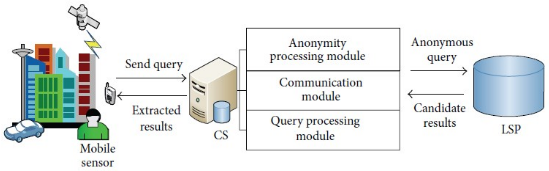

Figure 1: A central-center less architecture.

The structure of privacy-preserving scheme consists of three parts: as shown in Figure 1, a mobile user is denoted as uk. This architecture in involves achieving cooperative k-anonymity based on the prediction of users' movements to construct a cloaking region that will efficiently reduce the continuous query. Hence, a query algorithm is provided without having the real location of the user, which is substituted by a continuous anchor sequence to the LBS provider. This is one of the advantageous, as this technique can provide an accurate result about candidate sets returned by LBSs. Also, the algorithm provides a lasting solution to the uneven distribution problem in the space twist.

However, perturbation and location obfuscation has been used in preserving the location privacy of mobile phone users. In Figure 2, it is a path of the dividing area inside a number of parts. A set of points is specified already and for each point there will be a corresponding area depending of all points closer to that point from any other point. The drawback of this method is the ability of adversaries compromise the intermediate server.

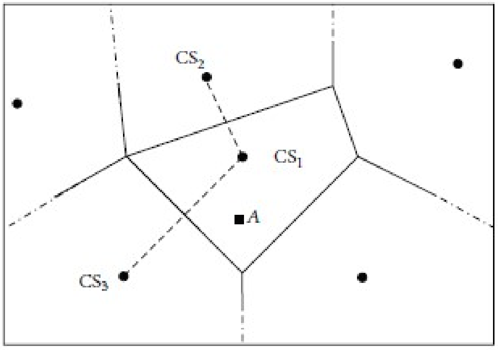

Figure 2: Voronoi graph partition.

These methods include spatio-temporal cloaking boxes as well as spatial cloaking boxes. Moreover, location entropy is also considered as the most useful technique for protecting user's privacy of LBS. Further, this research approach suggested the policy based schemes to make sure the protection of information privacy of users. Location obfuscation, as well as perturbation schemes, have also been suggested in [11].

Mobile users' communication is enjoyed at the expense of their privacy; to help with this, it has been proposed that short-range communication-based areas use a spatial cloaking algorithm. Based on the drawbacks of the existing peer-to-peer based communication and spatial cloaking based communication, a variance based attack on spatial cloaking was used in achieving k-anonymity within a group [12]. Also, the method also provided in [13] the use of dummy locations based on entropy metrics to achieve k-anonymity; more so, to address the issues of location queries submitted to untrusted location-based services (LBSs) by mobile users. Furthermore, grid base and R-tree algorithms, termed as "CliqueCloak," which requires different k-anonymity for each user, has been used. However, the algorithm in [13], it takes a lot of time to construct the clique graph, this algorithm is limited in use. While, the technique in [14], faces a limitation, as a stage of warm-up is required, and hence, the protection of users' privacy is not guaranteed throughout the entire time.

According to the study of [15][16], it has been revealed that the PIR, i.e. Private Information Retrieval technique also used for providing more powerful as well as more generalized scheme of blinding the un-trusted or malicious location server within the conversion of spatial query processing into a number of private database retrievals with the help of location servers. It has been found that the use of PIR protocol assists in allowing the client for secretly requesting the record which has been stored on a malicious server without exposing the retrieved record to the malicious server. As a result, rather blurring the queries of users, PIR is used for the protection of the queried content. Also, one more important point is there remains no information which leaks to adversaries over scrutinizing the requested records from the malicious server. The use of cloaking method may assist in protecting the location of the user over hiding the information of the user. In this context, cloaking method assists in enabling location-based services during the provision of security solutions but without the need of a trusted 3rd party. The drawback of this method is the hardware manufacturers could compromise the location privacy.

Wherefore, all the response time to the user is boosted by this algorithm. "CliqueCloak" is the method which supports in constructing the graph for all of the requests, which have not been yet anonymized. In this method, when any new request is received through the server, so it endeavors for identifying the clique including certain existing requests also new request. Hence, they cloak these requests together in a similar location.

There are many of disadvantages to using this CliqueCloak method. First with the limitation of the effectiveness of this method this the main drawback of this technique. Hence, this technique shows it difficult to find the anonymity group for such requests which hold large K values [17]. Besides to this, the cost required for the search of clique over the graph is high, that's mean could be another main drawback of CliqueCloak. Moreover, there are still some requests, which are not capable of being anonymized. These requests are dropped when their existence expires. Then, there is a good thing of making effective as well as careful use of CliqueCloak technique to attain main goals of this technique.

The research of [18] considers that the model of Clique Cloak is considered as the personalized k-anonymity model which helps in allowing the smartphones users to regulate their anonymity levels. Nevertheless, it has been found that this method makes the use of location anonymizer for the generation of the cloaking location. It depicts the anonymizer as the performance bottleneck and crucial point of failure.

Furthermore, [19] asserted that privacy-preservation and content protection of location-based queries could be protected using a two-stage approach based on oblivious transfer and private retrieval information. This system as shown in Figure 3, allows the user, through oblivious transfer, to privately determine their location using private grids, while the second communicational efficient PIR was used in the second stage for retrieval of appropriate blocks in the private grid. However, the technique in [20] develops a novel authentication technique that serves as an alternative for preserving privacy in LBS having fewer storage and communication overheads. Notably, a unified framework was produced to handle privacy concerns for several queries on LBSs. However, despite the efficiency of the authentication technique and the unified framework, other privacy preservations in LBSs, such as trip planning, were not considered in the approach and which limits the extent of privacy this technique can provide.

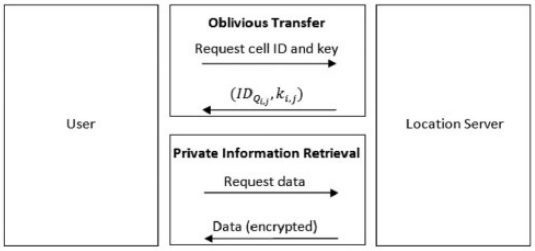

Figure 3: System overview.

Aside from the earlier mentioned location protection technique in LBS, zero-knowledge proofs (ZK) are naturally used to enhance the strengths or protocols towards achieving security, despite compromises [21]. It allows participants to prove that messages sent are correctly generated in the protocol without disclosing the secret data. Zero-knowledge proofs (ZK) are shown regarding zkS(M;N). The S in the zero-knowledge proof in the Boolean formula was developed through cryptography and is represented as zkn:m:S (N1 and NN;M1 and Mm) are part of two separate strings of terms, while location-holders a_i and b_j indicates the terms of Mi and Ni, respectively. The private component, Mi, will not be revealed, while the public component, Ni, also known as the verifier, can be revealed. This component needs to be revealed after the instantiation of the location-holder, "S(M/a)(N/b)" is shown to be true, then the verification of zero-knowledge proofs are regarded as successful. For example, zero knoledge zk_check(a1;b1) _a2 (sign(m; k);m; vk(k)) proves that the knowledge of a signature can be successfully verified with a key vk(k). It should be noted that neither signature sign_(m; k), nor the message m, was revealed in the proof [22].

Zero-knowledge proofs are different from the traditional technique of cryptography that only secures and authenticates communication privacy as it has been deployed in modern applications such as LBSs. Zero-knowledge proofs have advantages over the primitive techniques of security and privacy, as they can verify a user while still ensuring that the user remains anonymous [20]. Also, Zero-knowledge can prove the certificate reception from a trusted server without disclosing the real content, as in the Direct Anonymous Attestation (DAA) protocol [21]. Even though a (ZK) is desirable in protecting the privacy of the user and the content of the message sent to the server, computer-assisted support to use (ZK) in designing security protocols is not available. Hence, the vulnerability of this protocol still prevails [23].

Also, Bloom Filter Technique (BF) has recently prevailed as a better location protecting technique, as it uses a probabilistic data structure that allows testing for a set of components without revealing more than a single bit of information about the set [3]. If A is a putative element of a set S, then a Bloom Filter provides a probabilistic algorithm for determining if A is an element of S without any explicit recursion over the elements of S [24]. Furthermore, a Bloom Filter has the property of never having false negatives, so that an assertion of "A is not a member of S" is always an accurate assertion, assuming that the algorithm performing the test is benign. False positives are possible, however, so that an assertion of "A is a member of S" is only probabilistically correct depending on the number of bits used to implement the BF. While false positives are being risked, the Bloom Filter has a strong space advantage over other data structures to represent sets, such as hash tables [3].

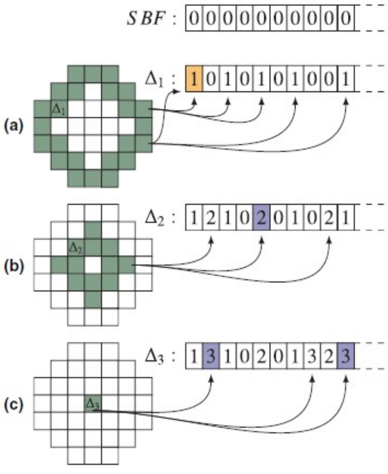
SBF : 0 0 0 0 0 0 0 0 0 0
(a)
Δ_1
Δ_1 : 1 0 1 0 1 0 1 0 0 1
(b)
Δ_2
Δ_2 : 1 2 1 0 2 0 1 0 2 1
(c)
Δ_3
Δ_3 : 1 3 1 0 2 0 1 3 2 3

Figure 4: Spatial Bloom Filter.

Furthermore, [3] [25] addressed the issues related to the protection of users' location information by using a (BF), which is a compact data structure for representing sets. The Spatial Bloom Filter (SBF) is an extension of the original Bloom Filter. It was created to help protect the privacy of users by managing spatial and geographic information. Further, this creation is done by using multi-party protocols that preserve the privacy of information based on a location that is recognized by public encryption patterns. This developed protocol has been efficient by enabling the privacy of the exact location of mobile users.

Figure 4. Parts $\triangle_1$, $\triangle_2$ and $\triangle_3$ are used to build a SBF. Hash functions 1,2 and 3 are used to link every element into the filter, except the first ten elements of the SBF are shown.

In (a), two elements in bloom filter joined to $\triangle_1$ are processed through the hash functions, leading to six 1 value elements to be written into the SBF. Thus, the same way in (b) and (c) respectively.

Previously in [3], was not only used proximity testing but also privately tested to see if a user was within a set of an arbitrary shape and size. Thus, both the proximity and general problem were solved through an intelligent conformation of areas. This confirmation is different from the other works done on privacy issues in LBS, which aim to provide protection based on the traces created by the user's movement over time and the associated attacks. Rather, [3] implemented a primitive cryptographic protocol that prevents the creation of a user's location traces. In fact, the location of the user is concealed, while the presence of the user is only known by the service providers in a limited number of Areas of Interest (AoIs).

While some privacy applications in LBSs rely solely on tracking a user's movement and require a set AoI to find the user's location, some have attempted to solve the issue of location privacy using the Bloom Filter technique. Using an intelligent conformation to these areas, the study was able to precisely identify how far a user is from an AoI. One can use a Spatial Bloom Filter, which has its advantages, including ensuring location privacy, as this has been an issue. It does, however, still provides information about the proximity of the user to a certain point of interest or the user's presence within a predefined point of interest, even though the AoI is not disclosed to the users.

There are two main methods which are used for mapping the cloaking region. These methods with quadtree mapping and other called Various-Size- Grid Hilbert Curve (VHC) mapping [26] [27]. Specifically, this method helps in resolving the issue related to the POIs density and which varied with respect to geographic zone.

In [28], Information Access Control is a technique which is used to provide the location privacy for LBS users. This technique depends on providing the LBS provider a mechanism for the LBS users to control the access to their location data. To achieve that, LBS providers enforce the access policies used to control the access to the users' location data. The drawback of this technique is that the LBS providers could be the potential adversaries who misuse the location data of the users. Information flow in the system and the procedures are shown in Figure 5. These procedures are for a push scenario. While in a pull scenario, non/expiring offers are stored up at the location-based service till the customer calls them. Merchants send information to the LS and runs the query, then send the IDs to the wireless networks to customers.

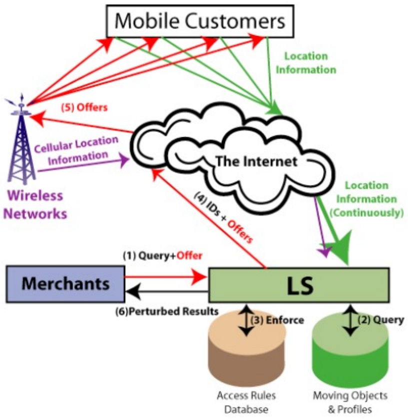

Figure 5: Information Access Control technique.

Mix zone is a technique which depends on the intermediate server to hide the user location [29].The intermediate server assigns a pseudonym to the user when he enters a mixing zone. That pseudonym is used by the user to send the queries to the LBS server via the intermediate server. A new pseudonym is assigned to the user when his mix zone is changed,. One of the application areas of the Mix zone technique is the road networks. The vulnerability of the intermediate server to be compromised by the adversaries is considered as the drawback of this technique.

Using dummy locations is another technique in the area of location privacy [30, 31]. In this technique, the mobile user confuses the LBS server by sending many of his queries many times, one of them contains his real location, and the others contain fake locations. The drawback of this technique is the ability of the adversaries to utilize the side information to analyze the user's sent locations and identify the dummy ones.

Authors in [32] focused on current challenges associated with managing the privacy protection and LBS accuracy based on population and road density. They also focused on other problems related to violating which may occur when a user's location privacy based contained in the LBS query payload and the device's IP address. They proposed context-aware for LBS system with integrated protection for both data privacy and communication anonymity. They utilized this solution on Google Maps, a popular LBS system which was proven to be valid in providing efficient privacy protection, LBS accuracy, and communication QoS (Quality-of-Service).

While the authors in [33], Investigated with the query linking on privacy. Specifically, the goal is to preserve mobile users' privacy within LBS mobile, and their location data could be available; moreover, when the adversary attacks should include the sensitive information of mobile user launching the query must not be disclosed to an adversary. So, provide a new query linking privacy preserving algorithm named (V-DCA) to continuous LBS by taking the user's rapidity, also acceleration. As well as, the consecutive cloaked groups to provide a new cloaked area, which reduces the complex algorithm with fulfilling the privacy needs. As for the simulation results showed that the (V-DCA) could preserve the privacy of mobile users, and provide the perfect quality of service (QoS).

Privacy-preserving data exchange algorithms are an area of very active research. While recent breakthroughs such as FHE provide the promise of extremely strong privacy guarantees, such approaches are hopelessly inefficient at this time. In [34], the application of tamper-proof hardware for universally composable secure computation. The result that obtained as a consequence of an efficient oblivious transfer protocol where two parties individually create and exchange a single stateless token yields the most practical and well-organized approach for tamper-proof tokens. Moreover, it implies that interested parties can always perform the secure computation of arbitrary function without the exchange of additional tokens. The result motivated to investigate the least number of stateless tokens that are required for universally composable OT or secure computation. So, in turn, prove that the protocol is optimal for the construction making of black-box use of the tokens. Also, managed to illustrate that non-black box method can be employed to acquire a construction using a single stateless token. A new form of social networking services has emerged. The mobile Online Social Networks mOSNs, in conjunction with IoT, enables a more user-friendly way to create and preserve social exchange has been enabled for users. Location-based and social network services are provided through mOSN Services, these location-based services show points of interest, like restaurants, that are close to a user's current location, stores, and social events. Also, the privacy of location information of users can easily be compromised by malicious attackers during information leakage as current mOSNs are being centrally controlled; hence, enjoying a convenient service without leaking sensitive information has become the common task facing researchers.

As a result, a Bloom Filter has also been used as an effective privacy location sharing mechanism for protecting mobile users' information and has been regarded as BMobishare, which was proposed by [35]. This mechanism enhances the privacy of the users' location via the Bloom Filter technique as shown in Figure 6, by hiding sensitive exchanges of data in such a way that the data exchange cannot be obtained by both sides involved in the exchange. Similar to Mobishare, BMobishare employed the use of dummy query information to protect a user's real identity which is achieved by hiding sensitive private information of the user by ensuring that no individual information of the user is leaked to other parties.

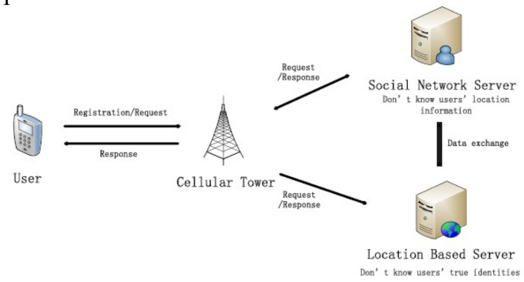

Figure 6: System architecture.

On the other hand, the local map contains the basic information on the likelihood of user's query. Assuming the local map is partitioned into an exact set of cells (i.e., n×n cells), then, the likelihood of the user submitting location-based query represents a query in a certain set from that particular cell.

Two different types of models, active and passive models, are considered in this study due to the varying abilities of these models. Any model can be regarded as passive in as much as the communication channels, and the network can be eavesdropped or compromised by collecting users' sensitive information. For a model will be regarded as active, if it is capable of compromising the LBS server through which it will collect information from the server and used for an attack such as inference. Due to its ability, all users' information can be obtained, and the query sent by every user is monitored. Also, both the historical and current data of every particular user can be captured, as well as the idea of the location privacy protection of the system.

A typical query submitted to the LBS by a mobile user includes a user identifier, the precise location, and interest of the query and the range of the query. Sensitive user information may be revealed to the public during the process of making the request. Therefore, to protect the privacy of the user, a peer-to-peer (P2P) spatial cloaking algorithm method has been widely used, although it has several drawbacks. However, the motivation of this study is drawn from the bottleneck of the performance of the system and the privacy concern of the existing spatial cloaking based solutions, as a result of the location anonymizer used in the prevailing approaches [36].

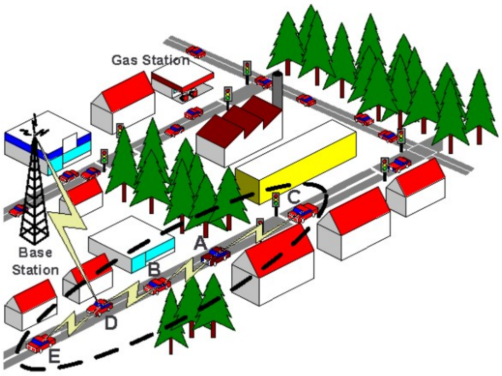

Figure 7: peer-to-peer (P2P).

In Figure 7, D is the mobile user and chosen as an agent. After that, the mobile user which is A sends its query, for example, the nearest gas station? along with its cloaked spatial area to the agent. Then the agent sends the query to the location-based database over a base station. Figure 8, shows the system architecture for the suggested P2P spatial cloaking which consists of two main parts: first with mobile clients, second with the location-based database. For every mobile client has (privacy profile with the level of own privacy within two parameters, k-anonymous and Amink denotes minimum resolution of the cloaked spatial area).

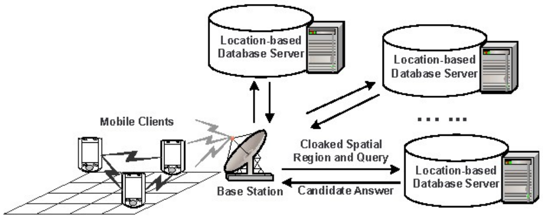

Figure 8: System architecture.

Among the existing solutions, only a few provide a fine-grained balance between location privacy and system overhead in today's smartphones. Also, existing solutions are used in achieving k-anonymity where a bigger region is being provided. However, the solution is limited due to its requirement for a warm-up phase which could not always protect at all times.

Moreover, in this study [37] has shown that grid depended cloaking algorithms may be divided into two main categories including Hilbert Curves as well as Quad-tree curve. While with this study in [26] has proposed, the promising quad-tree based on the cloaking algorithm. It has been shown by the study that space is made up of partition into quadrants unless the number of points in each quadrant attains the K value in the quadtree-based algorithm. Hence, the time complexity is supposed by this algorithm and which is considered as the main drawback or in other word limitation. So, the time complexity takes place when the observations pass all through the tree.

On the other hand, the study of [15] has suggested with another quadtree based cloaking algorithm which is called NewsCasper. An anonymizer supports in maintaining a hash table by user ids by this algorithm [16] [38], user ids over this algorithm. These user's ids point to the minimum level quadrant in which the user lies. So that, the location of each and each of user may be accessed directly by preventing top-down access for the Quadtree. Hence, generated cloaking location shows to be large which is considered as the main issue of Quadtree algorithm.

Thus, it is because quadtree algorithm splits the space into several quadrants. As a result of this, dealing with more POIs candidates is important, and which degrades query processing performance [26] [27]. To overcome the problems linked to Quadtree-based algorithms. Besides to this, in [39] has further suggested the Hilbert-Curve based cloaking algorithm. PRIVE, as well as MOBIHIDE, are the two main frameworks and which have been suggested by this cloaking algorithm. In the previous research, Hilbert Curve will be used [40].

The main benefit related to the use of Hilbert Curve is that it helps in guaranteeing the user's anonymity and helps in generating small cloaking location as compared to Quadtree. Anyway, the main drawback related to Hilbert Curve is that the cloaking location can be raised needlessly due to the extension related to adjacent cells by the use of sequential identifiers of Hilbert Curve [27] [41].

To achieve the objective of this study, a modified Hilbert Curve is proposed to present an effective k-anonymity protection which is illustrated in Figure 9 and 10 below.

In Figure 9, presents the standard Hilbert Curve [42], which covers the entire local map based on the user's query distribution, while in figure 10, show the modified "previous suggestion" of Hilbert Curve based on the probability levels [43].

The modified Hilbert Curve was necessary, based on the fact that the distribution of the user's query in the local map may not be uniformly distributed. A better grain is usually obtained with higher query probabilities; therefore, a set of dots in the modified Hilbert Curve will be obtained as shown in "Figure 10" (modified Hilbert Curve).

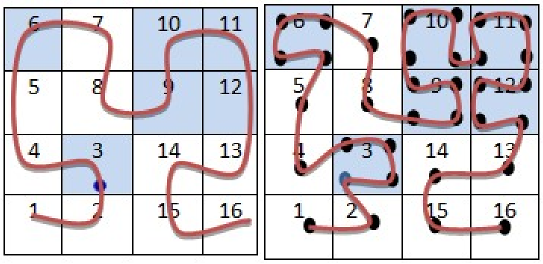

Figure 9: Standard Hilbert Curve [42].

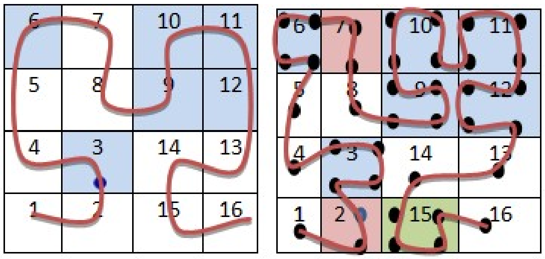

Figure 10: "Modified" of Hilbert Curve within query probability [43].

Furthermore, Hilbert Curve can be recognized through neighboring dots in the predicted area; this closes in on the initial area that was decided for a certain dot, the adjacent dot around can easily be determined. This property can be used by a Hilbert Curve to construct a cloaking region in the LBS.

To arrive at this, the value of the modified Hilbert Curve should be separated into k segments, where the value of k is undefined. It should be noted that actual location of the user can be found in one segment; hence, K – 1 should be chosen from the other K – 1 segment. In this manner, the large area in the local map under the limited k can be covered by the chosen candidate. Therefore, the K – 1 candidate is gotten at hand to achieve k-anonymity, while the needed cloaking region is guaranteed. Even though dummy locations can be generated for each chosen location of the candidates, it cannot assure the effectiveness of k-anonymity.

We suggested a new scheme based on [42] [43], and it is purely peer-to-peer based. The mobile users of the scheme will communicate on an LBS server with each other within a collaborative group using either a Wi-Fi, Bluetooth, Ad-hoc network via 3G/4G cellular phones. Every mobile user within this scheme will maintain a buffer to record users' information exchange. First, the modified Hilbert Curve algorithm will run through the users that need LBS, and then a dummy algorithm, with a fine-grained local substitution algorithm will build a cloaking region; hence, this region will be sent to the LBS server. The flow of data for this proposed algorithm is shown in "Figure 11" below.

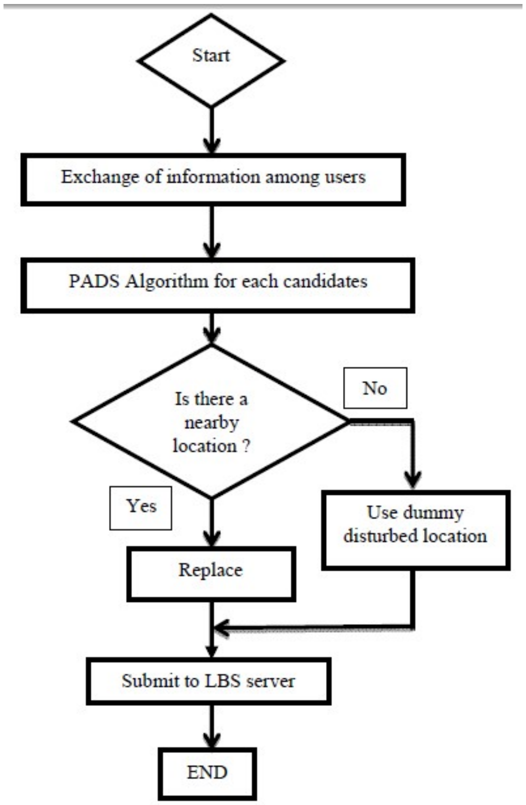
Start
Exchange of information among users
PADS Algorithm for each candidates
Is there a nearby location ?
No
Yes
Use dummy disturbed location
Replace
Submit to LBS server
END

Figure 11: Proposed data flow algorithm.

A privacy algorithm scheme for LBS was proposed in this study based on a modified Hilbert Curve algorithm, this algorithm provides the assurance of k-anonymity for its users, while still controlling the system overhead. Through this algorithm, a spatial cloaking scheme protects information found through location-based services, these queries are typically sent to these services by the mobile user, but sensitive user information may be leaked to (location anonymizer) during the process of making the request. Although the k-anonymity technique has been widely used, it has setbacks due to the bottleneck of the performance of the system and the privacy concern of the existing k-anonymity based solutions.

Hence, this scheme has proposed the use of a modified Hilbert Curve to improve the privacy of the LBS. However, the study recommends that future researchers should endeavor to conduct a security analysis, simulation set-up and evaluate the proposed algorithm to ensure the privacy efficiency of the proposed scheme.

3. THE OUTCOMES OF TRENDS OF RESEARCH

The outcomes of trends of research in the "Table 1", based on the requirements are as follows [44]:

- Accuracy As expressed through the privacy profile, the anonymization process satisfies the user requirements.
- Quality An adversary, cannot get any information about a user's specific location from these services.
- Efficiency An anonymous location should be calculated in an efficient and scalable way.

- Flexibility The privacy profile of a user can be changed as needed and at whatever time by the individual user.
- Location Privacy, The user of an LBS, should hide his or her location information and query information in order to take full advantage of the services.
- Query Privacy The users do not mind to or binding to reveal their locations. therewith, users want to hide their queries.

Table 1: THE OUTCOMES OF TRENDS OF RESEARCH.

Techniques	Accuracy	Quality	Efficiency	Flexibility	Location Privacy	Query Privacy
K-anonymity [9] [36]	×	✓	✓	×	✓	✓
Voronoi graph[10]	✓	✓	✓	×	✓	✓
Spatial cloaking[12]	✓	×	✓	×	✓	✓
CliqueCloak algorithm [13]	×	✓	✓	✓	✓	✓
Oblivious Transfer[19]	✓	✓	✓	×	✓	✓
PIR [19]	×	×	×	✓	×	✓
PIR [16]	×	✓	✓	×	✓	×
A novel authentication technique[20]	×	×	✓	✓	×	✓
Zero knowledge proofs [21] [22]	×	✓	✓	×	✓	✓
Zero knowledge proofs [23]	×	✓	✓	✓	✓	✓
Bloom Filter [3] [24]	✓	✓	✓	✓	✓	✓
Spatial Bloom Filter[25]	✓	✓	✓	✓	✓	✓
BMobishare[35]	×	✓	✓	✓	✓	✓
Hilbert Curve algorithm [42]	×	✓	✓	×	✓	✓
Modified Hilbert Curve algorithm [43]	✓	✓	✓	×	✓	✓
Various-Size- Grid Hilbert Curve (VHC) mapping [26][27]	×	✓	✓	×	✓	✓
Information Access Control[28]	✓	×	✓	×	✓	×
Mix zone [29]	✓	×	×	×	✓	×
Dummy locations [30][31]	✓	✓	×	✓	✓	✓
V-DCA[33]	×	✓	×	×	✓	×
Quad-tree based on the cloaking algorithm [26]	✓	×	✓	×	✓	✓
NewsCasper[15]	✓	✓	×	✓	×	✓

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. DISCUSSION AND LIMITATIONS

To show the positive impact of information leakage on the privacy of LBS users and the high negative impact , so the major positive is related to option (high positive impact), we rank the strength of the discussed information leakage according to the (✓) option got over the protection goals.

When the factor has(high positive impact (✓) and doesn't guides to leaked the privacy. When the factor has a high negative impact (×) and guides to leaked the privacy. Table 2, gives a description both of measurements.

Table 2: Measurements.

Option	Description
✓	High positive impact and doesn't guide to leaked the privacy
×	High negative impact and guide to leaked the privacy

In Figure 12, we can realize that the Bloom Filter has a high positive impact in 1st rank, then zero-knowledge protocol and oblivious transfer as a 2nd rank, cloaking algorithm 3rd rank, at last, information access control and mix zone with 4th rank and 5th rank respectively.

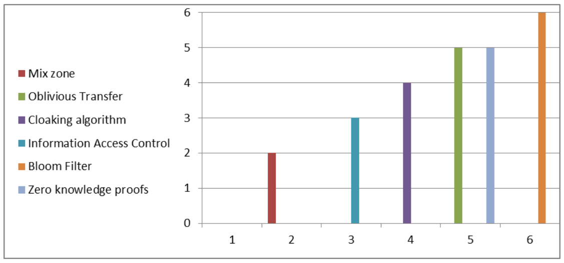

Figure 12: Ranking of information leakage group A.

As well in Figure 13, show that the CliqueCloak algorithm and Voronoi graph both of them at the same level in 1st rank, then the spatial cloaking and K-anonymity as a 2nd rank, cloaking algorithm 3rd rank, PIR [16] in 3rd rank, at last with PIR [19] got the 4th rank .

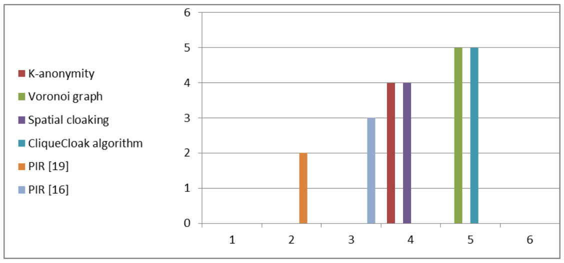

Figure 13: Ranking of information leakage group B.

Moreover, in Figure 14, we can see that the Spatial Bloom Filter has a high positive impact in 1st rank, then BMobishare and Modified Hilbert Curve algorithm as a 2nd rank, Hilbert Curve algorithm and zero knowledge protocol in 3rd rank, at last with a novel authentication technique with 4th rank.

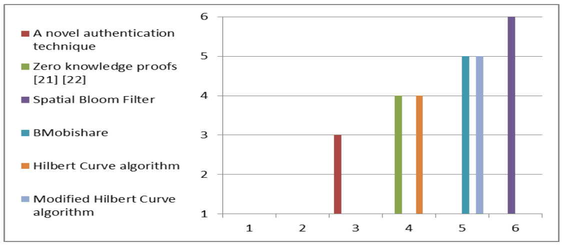

Figure 14: Ranking of information leakage group C.

While in Figure 15, the Dummy locations have a high positive impact in 1st rank, then Various-Size- Grid Hilbert Curve (VHC) mapping and NewsCasper as a 2nd rank, finally with V-DCA as a 3rd rank.

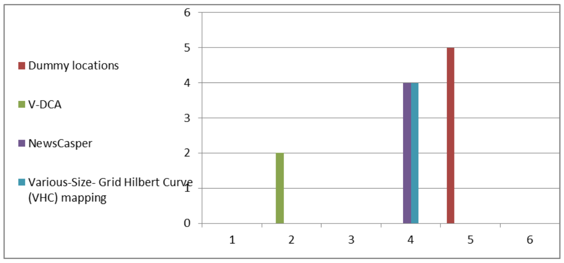

Figure 15: Ranking of information leakage group D.

Many GPS within LBS applications are used to determine the current location. If the service wants to cover more, you must rely on many site technologies.

Further investigations are needed to assess the behavior of LBS under various positioning techniques and information leakage. Actually, this is what we are trying hard to present in this study. The problem of this paper to explore the limitations of the LBS systems that we need to develop to be more intelligently and accurately. As a conclusion, further investigation is needed to assess user privacy and information leakage within LBS.

5. CONCLUSION AND FUTURE WORK

We have presented a survey of the current trends of privacy techniques employed in protecting the location privacy of users in LBSs. As well as further highlighted the efficiency and deficiency of each technique discussed in this paper and we found that the Bloom Filter has a high positive impact on reducing leakage of information, so that we set in the 1st rank, then zero-knowledge protocol and oblivious in the group A, while in the group B the CliqueCloak algorithm and Voronoi graph both of them at a same level in 1st rank. As for group C the Spatial Bloom Filter has a high positive impact in the 1st rank, then BMobishare and Modified Hilbert Curve algorithm as a 2nd rank. Ultimately with group D, the Dummy locations have a high positive impact on 1st rank. On the other hand, the mixing zone of group A, PIR [19] of group B, novel authentication technique of group C and V-DCA of group D, each of them has a negative impact on reducing leakage of information.

Having attempted to address the security efficiencies and deficiencies found in the current location-based application techniques, we evaluated the current trends of privacy techniques on the LBS privacy protection based on accuracy, quality, efficiency, flexibility, location privacy and query privacy, it could be deduced in this paper that zero knowledge, the Bloom Filter, dummy locations and the Hilbert Curve are currently being used for securing the location privacy of mobile users.

We suggested a modified Hilbert Curve and recommended that future researchers should endeavor to conduct a security analysis, simulation set-up and evaluate the proposed algorithm use of a modified Hilbert Curve to ensure the privacy efficiency of the proposed scheme.

Even though zero-knowledge proof and the Hilbert Curve are desirable in protecting the privacy of the user and the content of the message sent to the server, there is a lack of computer-assisted support in using ZKPs when designing security protocols, is still a major limitation of the protocols.

For future work, we plan to evaluate the current trends of privacy techniques on the LBS privacy protection based on Location Tracking, Query Tracking, Trajectory Privacy, and Database Privacy.

REFRENCES:

[1] R. Cramer, I. Damgård, and J. B. Nielsen, "Secure multi party computation and secret sharing: An information theoretic approach," Book Draft, 2012.

[2] A. J. Blumberg, and P. Eckersly, "On locational privacy and how to avoid losing it forever," 2009.

[3] L. Calderonia, P. Palmierib, and D. Maioa,"Location privacy without mutual trust: The spatial bloom filter," Computer Communications, vol. 68, pp. 4–16, 2015.

[4] L. Kulik, "Privacy for real-time location based services," SIG SPATIAL Special vol. 1,no. 2,pp. 9–14.

[5] X. Shu, and D. D. Yao, "Data leak detection as a service, in: A. D. Keromytis, R. D. Pietro (Eds.), Security and privacy in communication networks, 8th International ICST Conference, Secure Comm, LNCS, 106, Springer, 222–240, 2012.

[6] S. V. Watzdorf, and F. Michahelles, "Accuracy of positioning data on smartphones. In: Loc Web, ACM 2010.

[7] X. Pan, and X. Meng, "Preserving location privacy without exact locations mobile services," Front. Comput. Sci. vol. 7, no. 3, pp. 317-340.

[8] C. Cachin, C. Crépeau, J. Marcil, and G. Savvides,"Information-Theoretic Interactive Hashing and Oblivious Transfer to a Storage-Bounded Receiver," vol. 61, no. 10, pp. 5623–5635, 2015.

[9] L. Sweeney, "k-anonymity: a model for protecting privacy," Int. J.Uncertain. Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557–570,Oct. 2002.

[10] C. Ma, C. Zhou, and S. Yang, "A voronoi-based location privacy-preserving method for the continuous query in LBS," Int. J. Distrib. Sens. Networks, vol. 2015, 2015.

[11] K. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," Wireless Communications, IEEE, vol. 19, no. 1, pp. 30–39, 2012.

[12] B. Niu, X. Zhu, Q. Li, J. Chen, and H. Li, "A novel attack to spatial cloaking schemes in location-based services," Futur. Gener. Comput. Syst., vol. 49, pp. 125–132, 2015.

[13] B. Niu, Q. Li, X. Zhu, and H. Li, "A [1]spatial cloaking scheme for privacy-aware users in Location-Based Services," Proc. - Int. Conf. Comput. Commun. Networks, ICCCN, 2014.

[14] M. Gruteser and D. Grunwald, "Anonymous usage of location- based services through spatial and temporal cloaking," in Proc. of ACM MobiSys, 2003.

[15] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in Proc. Of ACM PETS 2003.

[16] Um, J. H., Kim, H. D., & Chang, J. W. (2010, August). An advanced cloaking algorithm using Hilbert curves for anonymous location based service. In Social Computing (SocialCom), 2010 IEEE Second International Conference on (pp. 1093-1098). IEEE.

[17] Z. Xiao, X. Meng, and J. Xu, "Quality Aware Privacy Protection for Location based Services," In Proc. of Database Systems for Advanced Applications, vol.4443, (April 2007), 434-446.

[18] B. Gedik and L. Liu, "Protecting location privacy with personalized kanonymity: Architecture and algorithms," IEEE Transactions on Mobile Computing, vol. 7, no. 1, pp. 1–18, Jan. 2008.

[19] R. Paulet, M. G. Kaosar, X. Yi, and E. Bertino, "Privacy-preserving and content-protecting location based queries," IEEE Trans. Knowl. Data Eng., vol. 26, pp. 1200–1210, 2014.

[20] T. Hashem, S. Datta, T. U. Islam, M. E. Ali, L. Kulik, and E. Tanin, "A Unified Framework for Authenticating Privacy Preserving Location Based Services," Second Int. ACM Work. Manag. Min. Enriched Geo-Spatial Data - GeoRich'15, pp. 13–18, 2015.

[21] E. Brickell, J. Camenisch, and L. Chen: Direct anonymous attestation. In Proc. 11th ACM Conference on Computerand and Communications Security, pp. 132 -145, ACM Press, 2004.

[22] M. Backes, M. Maffei, and D. Unruh. Zero-knowledge in the applied pi-calculus and automated verification of the direct anonymous attestation protocol. In IEEE Symposium on Security and Privacy, pp. 158–169, 2008.

[23] B. Smyth, L. Chen, and M. D. Ryan. Direct anonymous attestation: ensuring privacy with corrupt administrators. In Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks, pages 218–231. Springer-Verlag, 2007.

[24] B. Chazelle, J. Kilian, R. Rubinfeld, and A. Tal, "The bloomier filter: an efficient data structure for static support look up tables', in SODA, SIAM, pp.30–39, 2004.

[25] P. Palmieri, L. Calderoni, and D. Maio, "Spatial Bloom Filters : Enabling Privacy in Location-aware Applications."2015.

[26] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. Of IEEE ICPS 2005, 2005, pp. 88 – 97.

[27] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in Proc. Of IEEE INFOCOM 2014.

[28] M. Youssef, V. Atluri, and N. R. Adam Preserving mobile customer privacy: An access control system for moving objects and custom proles. s.l. : In Proc. MDM 2005.

[29] Mobimix, B. Palanisamy and L. Liu, Protecting location privacy with mix-zones over road networks. s.l. : In Proc. ICDE 2011.

[30] P. Shankar, V. Ganapathy, and L. Iftode, Privately querying location-based services with SybilQuery. s.l. : In Proc. Ubicomp 2009.

[31] O. Han, H. Zhao, Z. Ma, K. Zhang, and H. Pan, Protecting Location Privacy Based on Historical Users over Road Networks .. s.l. : In Proc. WASA 2014.

[32] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "A context-aware scheme for privacy-preserving location-based services," Computer Networks, vol. 56, pp. 2551-2568, 2012.

[33] L. Sweeney, "k-anonymity: a model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002.

[34] S. Geol Choi, J. Katz, D. Schr¨oder, A. Yerukhimovich, and H-S. Zhou, "(efficient) universally composable oblivious transfer using a minimal number of stateless tokens," presented at the 11th Theory of Cryptography Conference (TCC), In Lindell, 2014.

[35] N. Shen, J. Yang, K. Yuan, C. Fu, and C. Jia, "Computer Standards & Interfaces An efficient and privacy-preserving location sharing mechanism," Comput. Stand. Interfaces, 2015.

[36] C. Y. Chow, M. F. Mokbel, and X. Liu, A peer-to-peer spatial cloaking algorithm for anonymous location-based services. s.l. : In Proc. ACM GIS 2006.

[37] Niu, B., Li, Q., Zhu, X., & Li, H. (2014, August). A fine-grained spatial cloaking scheme for privacy-aware users in Location-Based Services. In Computer Communication and Networks (ICCCN), 2014 23rd International Conference on (pp. 1-8). IEEE.

[38] C.-Y. Chow, M. F. Mokbel, and X. Liu, “A peer-to-peer spatial cloaking algorithm for anonymous location-based service,” in Proc. Of ACM GIS 2006.

[39] V. Garg and M. Jhamb, "A Review of Wireless Sensor Network on Localization Techniques," International Journal of Engineering Trends and Technology (IJETT)-Volume4Isssue4-April, 2013.

[40] S. Mudda and S. Giordano, "Mobile P2P queries over temporal data," in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on, 2014, pp. 278-283.

[41] I. Bilogrevic, M. Jadliwala, K. Kalkan, J.-P. Hubaux, and I. Aad, “Privacy in mobile computing for location-sharing-based services,” in Proc. Of ACM PETS 2011.

[42] B. Niu, Q. Li, X. Zhu, and H. Li, “A Fine-Grained Spatial Cloaking Scheme for Privacy-Aware Users in Location-Based Services,” in Proc. of 24th ICCCN, 2014.

[43] A. Albelaihy and J. Cazalas, "A Fine-Grained Spatial Cloaking With Query. Probability Levels for Privacy in LBS," International Journal of Computer Networks and Applications (IJCNA), vol. 2, no. 5, pp. 212-221, 2015.

[44] M. F. Mokbel, "Privacy-Preserving Location Services." In IEEE International Conference on Data Mining, IEEE ICDM 2008, Pisa, Italy, Dec 2008.