International Conference on "Advances In Computing, Communication And Intelligence" ICACCI-2014 At Mauritius
Special Issue of International Journal of Electronics, Communication & Soft Computing Science and Engineering, ISSN: 2277-9477

Privacy Protection: A Major Issue in Location Based Query Processing

Kshitija Patil Dr.Vinod Patil Dr. Vilas Thakare Dr. Varsha Tondre

***Abstract* :- With the growing availability of mobile devices, it is possible to stay connected while on the move. It becomes a common practice to find the nearest hospital or the nearest hotel using the location based services (LBS) like Mapquest or Google Maps. As LBSs become more common, privacy concern is becoming a hot issue. There is a major possibility of disclosing sensitive information about individuals, including health condition, lifestyle habits, political and religious affiliations, or may result in unsolicited advertisement (i.e., spam). A number of research papers have been published concerning the privacy issue in location dependent query processing.**

In this paper, the focus is on the problems in location based query processing and some of the methods presented by different researchers for privacy preservation are analyzed.

***Keywords* : LBS, anonymity, cloaking, location based query processing.**

I. INTRODUCTION

Mobile devices, a boon of modern communication infrastructure, make it possible to overcome the Geo- graphical constraints in communication. In mobile environment, mobile users (mobile units) are not attached to a fixed location all the time. As they move, accordingly their point of connection to the network changes. The attachment of different servers is handled in a way that the mobile unit gets continuous services while moving. Internet-enabled mobile devices and mobile positioning, have given rise to a new class of location-based applications and services. In LBS, mobile users present anywhere with location aware mobile devices are able to make queries about their surrounding at any time. Location-based services (LBS) deliver geographic information and geo-processing power to the mobile/static users in accordance with their current location. [1] Such, position data include deeply personal information; therefore, the protection of location privacy is one of the most significant problems in location-based services.

II. LOCATION BASED QUERY PROCESSING IN MOBILE ENVIRONMENT

Location plays an important role in mobile computing environment. It is a vital piece of information that relates to mobility. Mobility is the main feature of mobile environment. For accessing the Location based services, processing of spatial queries is getting more significance in mobile computing environment. GPS enabled mobile devices supports spatial query processing. Spatial queries are mobile queries that operate on the location information of mobile devices. Spatial queries are classified as: Location dependent query and Location aware query. Processing of spatial queries involves processing of location dependent and location aware queries. In spatial queries, the location information is specified in the query or query is used to retrieve location information of mobile device. Location dependent query can be targeted to static object as well as dynamic object.

III. LOCATION BASED SERVICES

LBS can be defined as the specialized, multi-tiered, component web GIS (Geographical Information System) applications which can be invoked, published and located across the wired/wireless Web [2]. Mobile objects in LBS are characterized by point geometry and always move along a specific path in a network. The location of the mobile devices can be determined by using GPS or mobile network triangulation. Such devices can report their locations to the LBS server through a wireless interface, or their locations can be obtained through ground-based radars or satellites. By processing data at the LBS server, location based services are provided to the users. Location based services include emergency services, navigation services, billing services etc. Services, like automatic vehicle location, fleet management, tourist services, transport management, traffic control and digital battlefield are all based on mobile objects and are included under LBS. The important feature of LBS is to access location dependent data. Figure 1 shows a general example of LBS. The working of LBS is as follows

1. An LBS user obtains the true position data of a user using a positioning device such as GPS.
2. The user sends the position data to a service provider.
3. The service provider creates a reply message that responds to the received position data and sends it to the user.
4. The user receives a reply message [3].

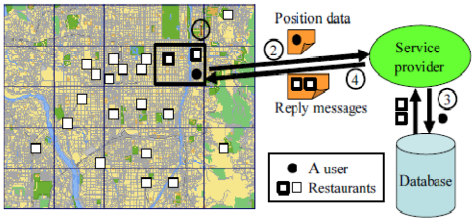

Fig. 1: Working of LBS.

IV. PRIVACY IN LOCATION BASED QUERY PROCESSING

There are two privacy issues in location-dependent queries:
(i) The user must hide his location.

ii) The user must hide his identity (e.g., username, IP address, etc).

Since LBSs exploit knowledge about where users are located, one of the big challenges in wide deployment of LBS systems is the privacy-preserving management of location-based data. Without safeguards, extensive deployment of location based services endangers location privacy of mobile users and exhibits significant vulnerabilities for abuse. Beresford et. al. defined location privacy as “the ability to prevent other parties from learning one’s current or past location” [4].

To hide one’s identity it is necessary to make him anonymous. Pfitzmann et. al. defined “anonymity” as “the state of being not identifiable within a set of subjects”[5] .

V. Privacy Protection Schemes in Location Based Query Processing

In LBS, mobile users present anywhere with location aware mobile devices are able to make queries about their surrounding at any time. In order to process location-dependent queries, the LBS need the exact location of the querying user. Therefore, privacy is not protected by replacing the real user identity with a fake one (i.e., pseudonym). An attacker, which may be the LBS itself, can infer the identity of the query source by associating the location with a particular individual.

There are a number of approaches in the literature to solve the problem of privacy protection with location based services, including:

- Cloaking;
- Generation of dummies;
- Private information retrieval (PIR).[6]

Most of the authors have based their work on K-anonymity. Some of the concept depends on hiding the user’s location among K-1 neighbors; require a permanent communication and remote monitoring of the users. This is a clear violation of the users’ privacy. The robustness of these approaches depends totally on having number of neighbors at the time of receiving the requests. Therefore, depending on a middleware is far from being a perfect solution to secure location-dependent queries. Thus, any secure solution is needed to communicate directly with the Location Based Server without any intermediate parties. some of the methods presented by different researchers for privacy preservation are

A. The New Casper: Query Processing for Location Services without Compromising Privacy

Casper is a new framework in which mobile and stationary users can entertain location-based services without revealing their location information. Casper consists of two main components, the location anonymizer and the privacy-aware query processor. The location anonymizer blurs the users exact location information into cloaked spatial regions based on user specified privacy requirements. In order to deal with the cloaked spatial areas, the privacy-aware query processor is embedded inside the location-based database server [7].

B. A Customizable k-Anonymity Model for Protecting Location Privacy

A customizable k-anonymity model for protecting privacy of location data has two unique features. It provides a customizable framework to support kanonymity with variable k. It allows a wide range of users to benefit from the location privacy protection with personalized privacy requirements. Second, a novel spatio-temporal cloaking algorithm, called CliqueCloak which provides location k-anonymity for mobile users of a LBS provider. The cloaking algorithm is run by the location protection broker on a trusted server. It anonymizes messages from the mobile nodes by cloaking the location information contained in the messages to reduce or avoid privacy threats before forwarding them to the LBS providers. The model enables each message sent from a mobile node to specify the desired level of anonymity as well as the maximum temporal and spatial tolerances for maintaining the required anonymity. [8].

C. Anonymous Communication Technique using Dummies for Location-based Services

A new anonymous communication technique to protect the location privacy of people using LBSs makes the use of dummies. In this technique, a user sends true position data with several false position data (‘dummies’) to a service provider. Then, it creates a reply message for each received position data. The user simply extracts the necessary information from the reply message. In this way, even if the set of position data is stored by the service provider. It cannot distinguish the true position data from the set of location data. The technique uses two dummy generation algorithms to prevent service providers from finding the true position data. They are:

1) Moving in a Neighborhood (MN)
2) Moving in a Limited Neighborhood (MLN)

This technique protects location privacy using *Anonymity Set* [3].

D. Privacy Protected Query Processing on Spatial Networks

Spatial query processing deals with processing of location information of mobile devices. A K-anonymity mechanism is proposed to preserve user privacy on Spatial Networks. Two novel query algorithms, PSNN and PSRQ have been presented for answering nearest neighbor queries and range queries on spatial networks without revealing private information of the query initiator. The main theme of the algorithms is to hide the exact mobile user location with a cloaked region. The cloaked region covers the query requester and at least K – 1 other users based on the K-anonymity concept. The spatial queries are executed based on both the cloaked region and the underlying networks. A candidate result set will be returned to the requesting user who filters out the exact answer. *[9]*

E. *The Mix Zone Model*

The mix zone model anonymizes user identity by restricting the positions where users can be located. The model provides:

1. A middleware mechanism to provide anonymised location information to third-party applications,
2. A quantitative run-time estimate of the level of anonymity provided by the middleware with a particular set of applications. The model assumes the existence of a trusted middleware system, positioned between the underlying location system and untrusted third-party applications. Applications register interest in a geographic space with the middleware; we refer to this space as an application zone.

Example spaces include hospital grounds, university buildings or a supermarket complex. Users register interest in a particular set of location-aware applications and the middleware limits the location information received by applications to location sightings of registered users located inside the application zone. Each user has one or more unregistered geographical regions where no application can trace user movements. Such areas are called as mix zones, because once a user enters such a zone, user identity is mixed with all other users in the mix zone. A boundary line is defined as the border between a mix zone and an application zone. Using mix zone model the user can make decisions about whether to disable some location-aware services or to alter their movements in order to gain increased privacy. [10]

F. *Privacy-Preserving Location-based Services for Mobile Users in Wireless Networks*

Sheng Zhong et.al. [11] Investigated privacy-preserving location based services for the three components that involved in providing location-based services. These are 1) the location-based service component 2) the localization component, and 3) the communications component. A security protocol is designed to implement the service without trusting the location server. This protocol consists of three phases: Initialization, Location Information Update, and Location Information Retrieval. The design is secure under a standard cryptographic assumption — the strong RSA assumption. The novel protocol provides location based services which do not require a user to trust a third party. This protocol enables user to control which entities can have access to user location information stored at an untrusted location server.

G. *Privacy Preserving Scheme for Location-Based Services*

A homomorphic encryption scheme [12] is used to build a fully secure system. It allows users to benefit from location-based services while preserving the confidentiality and integrity of their data. This novel system consists of search circuits that allow an executor (i.e. LBS server) to receive encrypted inputs/requests and perform a blind search to retrieve encrypted records that match the selection criterion. A querier can send the user's position and the service type he/she is looking for, in encrypted form, to a server and then the server would respond to the request without any knowledge of the contents of the request and the retrieved records. The encryption schemes enable to retrieve data without violating the privacy of the users as shown in figure 2.

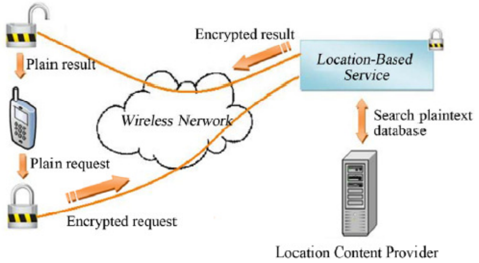

Fig.2 :Architecture of secure Location-Based Service.

H. *Privacy-Conscious Location-Based Queries in Mobile Environments*

Location cloaking is another approach to protect user location privacy in LBS [13]. When the user issues a location-based spatial query (e.g., a range query or a kNN query), the system cloaks the user's current location into a cloaking region based on the user's privacy requirement. The location-based spatial query is thus transformed into a region-based spatial query before being sent to the LBS server. The region-based query is evaluated by the LBS server and returns a result superset, which contains the query results for all possible location points in the cloaking region. The result superset is refined to generate the exact results for the query location.

I. *Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking*

A customizable k-anonymity model for protecting privacy of location data provides a customizable framework to support k-anonymity with variable k. It allows a wide range of users to benefit from the location privacy protection with personalized privacy requirements. In [14] a novel spatio-temporal cloaking algorithm, called CliqueCloak provides location k-anonymity for mobile users of a LBS provider. The cloaking algorithm is run by the location protection broker on a trusted server. It anonymizes messages from the mobile nodes by cloaking the location information contained in the messages to reduce or avoid privacy threats before forwarding them to the LBS provider(s). The model enables each message sent from a mobile node to specify the desired level of anonymity as well as the maximum temporal and spatial tolerances for maintaining the required anonymity.

J. Private Information Retrieval Techniques for Enabling Location Privacy in Location-Based Services

Location privacy schemes in [15] are based on hardware based and computational PIR protocols. The first approach superimposes a regular grid on the data and uses PIR to privately evaluate range and k-NN queries. The second technique supports approximate and exact nearest neighbor query evaluation by utilizing various 1-D and 2-D partitions to index the data. Then it restructures partitions into a matrix which can be privately queried using PIR. The first approach relies on hardware-based PIR techniques, the second one employs computational PIR protocols to provide location privacy [16]. SPIRAL: A Scalable Private Information Retrieval Approach to Location Privacy is stated in [17] which also make the use of PIR.

VI. ANALYSIS OF THE PRIVACY PROTECTION SCHEMES

After analyzing the above schemes it is seen that the methods are mainly based on following approaches

1) Anonymity approach
2) Cloacking approach
3) Encryption approach
4) Private Information Retrieval approach

It is seen that the Casper achieves high quality location-based services while providing anonymity for both data and queries [7]. The location k-anonymity model with multi-dimensional cloaking and tunable k parameter can achieve high guarantee of k anonymity. It provides high flexibility to location privacy threats without significant performance penalty [8]. The technique of sending true position data with several false position data ('dummies') to a service provider protects location privacy using Anonymity Set and can be applied in practical LBSs [3].

The query processing solutions discussed by most of the researchers are based on Euclidean metrics. But in real life, mobile users cannot move freely in space because they are usually constrained by underlying networks (e.g., cars on roads, trains on tracks, etc.). Therefore, the K-anonymity mechanism proposed in [9] proves better for spatial networks.

Using mix zone model [10], the user can make decisions about whether to disable some location-aware services or to alter their movements in order to gain increased privacy. It is possible because once a user enters such a zone; user identity is mixed with all other users in the mix zone. A boundary line is defined as the border between a mix zone and an application zone. Thus, the model prevents third party to identify user's identity.

A novel protocol proposed by sheng z. et.al. provides control to user himself. A user can control which entities may have access to his location information stored at an untrusted location server. The design uses the efficiency of a location server but does not suffer from associated privacy issues. The protocols have low computation and message overheads and are suitable for personal mobile devices [11].

It is seen that strong protection for user information can be attained, if the server is made capable of retrieving location related information without being aware of the user's position or the point of interests he/she is requesting. The homomorphic encryption [12] schemes enable to retrieve data without violating the privacy of the users.

After studying the optimal mobility-aware cloaking algorithms in [13], it is seen that the algorithm is robust against trace analysis attacks without compromising much on query latency or communication cost. MaxAccu Cloak algorithm gets a100% query accuracy while MinComm Cloak algorithm achieves a good balance between communication cost and query accuracy [14]. In Private Information Retrieval approach [15], PIR is used to prevent the untrusted location server from learning user locations. The trusted computing is used to ensure users that, the PIR algorithm and other services provided by the server are only performing intended operations.

VII. CONCLUSION

The cryptographic based techniques provide perfect privacy but they result in very costly spatial query processing schemes. The anonymity and cloaking-based approaches used to address the problem of location privacy cannot provide stringent privacy guarantees without incurring costly computation and communication overhead. These methods require a trusted intermediate anonymizer to protect a user's location information during query processing. The study of the various methods and algorithms shows that the location k-anonymity model with multi-dimensional cloaking and tunable k parameter can achieve high guarantee of k anonymity and high flexibility to location privacy threats without significant performance penalty.

REFERENCES

[1]. Dragan H. Stojanovic and Slobodanka J. Djordjevic-Kajan, "Processing Continuous Range Queries on Mobile Objects in Location-Based Services", 2012.

[2]. Pfoser D., Theodoridis Y., Jensen C.S., "Novel Approaches in Query Processing for Moving Object Trajectories", Proceedings 26th VLDB Conference, (2000), pp 395–406, 2000.

[3]. H. Kido, Y. Yanagisawa and T. Satoh, "An Anonymous Communication Technique Using Dummies for Location- Based Services," Proceedings of the International Conference on Pervasive Services of the IEEE ICPS 05, Santorini, pp. 88-97 ,11-14 July 2005.

[4]. R. Beresford and F. Stajano, "Location privacy in pervasive computing", IEEE Pervasive Computing, 2(1), pp 46–55, 2003.

[5]. A. Pfitzmann and M. Kohntopp. Anonymity, unobservability, and pseudeonymity: a proposal for terminology. In International workshop on Designing privacy enhancing technologies, Springer-Verlag New York, Inc., pp 1–9, 2001.

[6]. Youssef Gahi, Mouhcine Guennoun, Zouhair Guennoun, Khalil El-Khatib, " Privacy Preserving Scheme for Location-Based Services", Journal of Information Security, vol.3, No. 2 pp 105-112, April 2012.

[7]. M. F. Mokbel, C. Y. Chow and W. G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proceedings of the VLDB 2006, Seoul, pp 763-774, 12-15 September 2006,.

[8]. B. Gedik and L. Liu, "A Customizable k-Anonymity Model for Protecting Location Privacy," Technical Report, Georgia Institute of Technology, Atlanta, 2004

[9]. Wei-Shinn Ku, Roger Zimmermann, Wen-Chih Peng‡ Sushama Shroff, " Privacy Protected Query Processing on Spatial Networks", IEEE 23rd International Conference on Data Engineering 2007 , pp 215 – 220, April 2007 .

[10]. R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-aware Services", In Proc. of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW04), pp 127 – 131,March 2004.

[11]. Sheng Zhong, Li (Erran) Li†, Yanbin Grace Liu, Yang Richard Yang," Privacy-Preserving Location-based Services for Mobile Users in Wireless Networks", http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.112.7902.

[12]. Youssef Gahi, Mouhcine Guennoun, Zouhair Guennoun, Khalil El-Khatib, " Privacy Preserving Scheme for Location-Based Services", Journal of Information Security, vol.3, No. 2, pp 105-112, April 2012.

[13]. J. Xu, J. Du, X. Tang, " Privacy-Conscious Location-Based Queries in Mobile Environment", IEEE Transaction on Parallel and Distributed System, Vol. 21, pp 313–326, March 2009.

[14]. Gruteser, M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking, In MobiSys '03 Proceedings of the 1st international conference on Mobile systems, applications and services, ACM New York, pp 31-42, 2003.

[15]. Ali Khoshgozaran and Cyrus Shahabi," Private Information Retrieval Techniques for Enabling Location Privacy in Location-Based Services?", Privacy in Location-Based Applications Lecture Notes in Computer Science Vol. 5599, pp 59-83, 2009.

[16]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary", In *SIGMOD '08: Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, New York, NY, USA, pp 121–132, 2008.

[17] Khoshgozaran A., Shirani-Mehr, H. ,Shahabi, C., "SPIRAL: A Scalable Private Information Retrieval Approach to Location Privacy", DMW 2008, Ninth International Conference on Mobile Data Management Workshops, pp 55- 62, April 2008