A SECURE DYNAMIC GRID SYSTEM FOR LOCATION BASED SERVICES USING K-NEAREST NEIGHBOUR TECHNIQUES

S. Priya[1], D. Shobana[2] and S. Menaka[3]

ABSTRACT

Location based services (LBS) are services offered through a mobile phone and take into account the device's geographical location. LBS typically provide information or entertainment. Location-based services (LBS) need users to unceasingly report their location to a doubtless untrusted server to get services supported their location, which may expose them to privacy risks. Sadly, existing privacy preserving techniques for LBS have many limitations, like requiring a fully-trusted third party, giving restricted privacy guarantees and acquisition high communication overhead. (1) The system solely requires a semi-trusted third party, accountable for effecting easy matching operations properly. This semi-trusted third party will not have any data a couple of user's location. (2) Secure shot and continuous location privacy is secured beneath our outlined adversary models. (3) The communication price for the user doesn't rely on the user's desired privacy level , it solely depends on the number of relevant points of interest within the section of the user. (4) Though we have a tendency to solely target vary and k-nearest-neighbor queries in this work, our system is simply extended to support different spatial queries while not dynamic the algorithms go past the semi-trusted third party and also the information server, provided the desired search space of a spatial question is abstracted into spatial regions. Experimental results show that our DGS is a lot of economical than the progressive privacy-preserving technique for continuous LBS.

Keywords : location privacy, cryptography, location-based services, Point Of Interest.

I. INTRODUCTION

In today's world of mobility and ever present Internet connectivity, an increasing number of people use location based services (LBS) to request information relevant to their current locations from a variety of service providers. This can be the search for nearby points of interest (POIs) (e.g., restaurants and hotels), location aware advertising by companies, traffic information tailored to the highway and direction a user is traveling and so forth. The use of LBS, however, can reveal much more about a person to potentially untrustworthy service providers than many people would be willing to disclose. By tracking the requests of a person it is possible to build a movement profile which can reveal information about a user's work (office location), medical records (visit to specialist

[1] Research Scholar(CS), Sri Krishna Arts and Science College College, Coimbatore - 641 008.

[2] Assistant Professor, Department of Information Technology, Sri Krishna Arts and Science College College, Coimbatore - 641 008.

[3] Assistant Professor, Department of Commerce, Vivekanandha College of Arts and Science College, Coimbatore - 641 008.

Clinics), political views (attending political events), etc. Nevertheless, LBS can be very valuable and as such users should be able to make use of them without having to give up their *location privacy*.

A number of approaches have recently been proposed for preserving the user location privacy in LBS. In general, these approaches can be classified into two main categories. (1) *Fully-trusted third party* (TTP). The most popular privacy-preserving techniques require a TTP to be placed between the user and the service provider to hide the user's location information from the service provider (e.g., [1]–[8]). The main task of the third party is keeping track of the exact location of all users and blurring a querying user's location into a cloaked area

that includes k " 1 other users to achieve k - anonymity. This TTP model has three drawbacks. (a) All users have to continuously

report their exact location to the third party, even though they do not subscribe to any LBS. (b) As the third party knows the exact location of every user, it becomes an attractive target for attackers. (c) The k-anonymity-based techniques only achieve low regional location privacy because cloaking a region to include k users in practice usually results in small cloaking areas. (2) *Private information retrieval (PIR) or oblivious transfer (OT).*

II. System Architecture

Fig. 1 depicts the system architecture of our dynamic grid system (DGS) designed to provide privacy-preserving continuous LBS for mobile users. Our system consists of three main entities, *service providers*, *query servers* and *mobile users*. We will describe the main entities and their interactions, and then present the two spatial queries, i.e., range and k-nearest-neighbor (NN) queries, supported by our system.

Service providers (SP)**:** Our system supports any number of Independent service providers. Each SP is a spatial database management system that stores the location information of a particular type of *static* POIs, e.g., restaurants or hotels, or the store location information of a particular company, e.g., Starbucks or McDonald's. The spatial database uses an existing spatial index (e.g., R-tree or grid structure) to index POIs and answer range queries (i.e., retrieve the POIs located in a certain area).

Mobile users: Each mobile user is equipped with a GPS-enabled device that determines the user's location in the form (xu, yu). The user can obtain snapshot or continuous LBS from our system by issuing a spatial query to a particular SP through QS. Our system helps the user select a query area for the spatial query, such that the user is willing to reveal to SP the fact that the user is located in the given area. Then, a grid structure is created and is embedded inside an encrypted query that is forwarded to SP; it will not reveal any information about the query area to QS itself. In addition, the

communication cost for the user in DGS does not depend on the query area size. This is one of the key features that distinguish DGS from the existing techniques based on the fully-trusted third party model.

Supported spatial queries: DGS supports the two most popular spatial queries, i.e., range and k-NN queries, while preserving the user's location privacy. The mobile user registers a continuous range query with our system to keep track of the POIs within a user-specified distance, *Range*, of the user's current location (xu, yu) for a certain time period, e.g., "*Continuously send me the restaurants within one mile of my current location for the next one hour*".

The mobile user can also issue a continuous k-NN query to find the k-nearest POIs to the user's current location (xu, yu) for a specific time period, e.g., "*Continuously send me the five nearest restaurants to my current location for the next 30 minutes*". Since a snapshot query is just the initial answer of the continuous one, DGS also supports snapshot range and k-NN queries.

Query servers (QS): QS is a semi-trusted party placed between the mobile user and SP. Similar to the most popular infrastructure in existing privacy-preserving techniques for LBS, QS can be maintained by a telecom operator.

2.1 ADVERSARIAL MODELS

We now discuss adversarial models regarding QS and SP, and then present the formal security proof of our DGS malicious QS or SP will try to break a user's privacy by working with the data available to them within the described protocol. We do not consider QS or SP with access to external information not directly related to the protocol.

2.1.1 User Anonymity

As described above, both QS and SP will try to De-Anonymize a user by using the information contained in the protocol (although they still faithfully follow the protocol itself). While QS does not have any information about a user that would allow it to narrow down the list of users that would fit a specific query, SP has access to the plaintext query of a user.

2.1.2 Other Attacks

In this subsection we discuss a few other attacks and explain how they relate to our proposed system.

IP localization: One possible attack involves QS trying to determine the position of a user through IP localization (i.e., using

a database which can map IP addresses to locations). Because of how mobile phone networks are setup (considering that our system is aimed at mobile users using mobile phone networks), however mobile phones cannot be located with useful accuracy.

Timing attacks. Another set of attacks might use timing information if QS can observe the traffic close to the originating user. However if QS can observe such traffic, the location privacy of the user is very likely already compromised, even without timing attacks. Furthermore, we consider this to be out of the scope of our work.

Query server as client. QS might try to also act as a client in an attempt to gain some information which could help to localize a user. QS has no information to launch such an attack, however, not even an approximate location of the user. Also, the number of POIs returned to a client does not allow QS to make any inferences, because it knows neither the query area nor the grid parameters. A large number of POIs could either mean a dense region or a large query area, depending on the grid parameters, which are unknown to QS.

Network traffic finger printing: An attack which makes inferences based on the statistics of encrypted network connections is not applicable to our system. The attack as described in the paper is equivalent to determining which QS a user is using. This information does not need to be secret and communication with QS is highly uniform across different query servers (unlike website traffic), very likely making them for all practical purposes indistinguishable.

III. Dynamic Grid System (DGS)

In this section, we will describe how our DGS supports privacy preserving continuous range and k-NN queries. This section is organized as follows: Section 3.1 describes the details of our DGS for processing continuous range queries and incrementally maintaining their answers, and Section 3.2 extends DGS to support k-NN queries.

3.1 Range Queries

Our DGS has two main phases for privacy-preserving continuous range query processing. The first phase finds an initial (or a snapshot) answer for a range query (Section 3.1.1), and the second phase incrementally maintains the query answer based on the user's location updates (Section 3.1.2).

3.1.1 Range Query Processing

As described in a continuous range query is defined as keeping track of the POIs within a user-specified distance Range of the user's current location (xu, yu) for a certain time period.

3.1.1 Incremental Range Query Answer Maintenance

After the user gets the initial response for a range query from QS, she can find the initial (or snapshot) query answer locally. Then, incremental answer updates can be performed to maintain the answer when the user's location changes.

3.2 K-Nearest-Neighbor Queries

Similar to continuous range queries, the privacy-preserving query processing for continuous k-NN queries has two main phases. The first phase finds an initial (or snapshot) answer (Section 3.2.1), while the second phase maintains the correct answer when the user moves by using incremental updates (Section 3.2.2). However, unlike range queries, the required search area of a k-NN query is unknown to a user until the user finds at least k POIs to compute a required search area, i.e., a circular area centered

at the user's location with a radius from the user to the k-th nearest POI. Thus, the privacy-preserving query processing protocol of k-NN queries is slightly different.

3.2.1 Incremental k-*NN Query Answer Maintenance*

After the user computes an initial (or snapshot) k-NN query answer, the incremental answer update phase allows to maintain the answer as the user moves around. Similar to range queries, the incremental answer maintenance phase has four steps. The first two steps are the same as the cache region step and the incremental request generation step as in Section 3.1.2. In the third step (i.e., request processing) performed by the QS, since QS has already cached the encrypted POIs, together with their corresponding encrypted identifiers calculated by SP in Step 4 of the query processing phase, it does not need to contact SP. It can simply forward the encrypted POIs matching one of the encrypted identifiers in Se to the user. In the last step (i.e., answer refinement) performed by the user, she decrypts the received POIs and sorts the ones located within the required search area according to their distance to the user in ascending order. The k-nearest POIs to the user constitute the new query answer.

IV. Results And Discussion

In this section, we evaluate the performance of our DGS for both continuous range and k-NN queries through simulations.

Baseline algorithm : We implemented a continuous spatial cloaking scheme using the *fully-trusted third party model* (TTP) [2].

TTP relies on a fully-trusted location anonymizer, which is placed between the user and the service provider (SP), to blur a querying user's location into a cloaked area that contains the querying user and a set of K " 1 other users to satisfy the user specified K anonymity privacy requirement. To preserve the user's continuous location privacy, the location anonymizer keeps adjusting the cloaked area to contain the querying user and the K " 1 users.

Performance metrics : We measure the performance of our DGS and the TTP scheme in terms of the average computation time per query on the client side, at the query server (QS) (or the location anonymizer for the TTP scheme), and at SP.We also measure the average communication cost per query between the user and QS, as well as the communication cost between QS and SP.

Parameter settings : Unless mentioned otherwise, the experiment considers 20,000 mobile users and 10,000 POIs. The default query distance for range queries is 2km, and the default requested number of POIs for k-NN queries is k = 10. Since our DGS provides more secure continuous location privacy than the TTP scheme, we only consider a moderately high K-anonymity level for the TTP scheme, where K = 200 [2], to give a fair comparison.

Grid system : The grid system is created by laying a grid over a query area that is defined by its 4 corners. The grid divides the query area into non-

overlapping, equal-sized cells (in terms of latitude/ longitude). While the grid system does not require a specific coordinate system, for convenience we use WGS84 in our prototype. WGS84 is the coordinate system used for the Global Positioning System (GPS), and hence most easily applicable to mobile devices that contain a GPS receiver

Points of interest(POI): The POIs are generated randomly, by placing them onto vertices of the road map used in the experiment. For example, to generate 10,000 POIs, the prototype randomly picks a vertex of the road map as the location of a POI, repeating this 10,000 times.

V. Conclusion & Future Work

In this Paper we proposed a dynamic grid system (DGS) for providing privacy-preserving continuous LBS.DGS does not require any fully-trusted third party (TTP); instead, we require only the much weaker assumption of no collusion between QS and SP.DGS provides better privacy guarantees than the TTP scheme, and the experimental results show that DGS is an order of magnitude more efficient than the TTP scheme, in terms of communication cost.

Spatial cloaking techniques have been widely used to preserve user location privacy in LBS. Most of the existing spatial cloaking techniques rely on a fully-trusted third party (TTP), usually termed *location Anonymizer*, that is required between the user and the service provider (e.g., [1]–[8]). When a user subscribes to LBS, the location anonymizer will blur the user's exact location into a cloaked area such that the cloaked area includes at least k – 1 other user to satisfy k-anonymity. The TTP model has four major drawbacks. (a) It is difficult to find a third party that can be fully trusted. (b) All users need to continuously update their locations with the location anonymizer, even when they are not subscribed to any LBS, so that the location anonymizer has enough information to compute cloaked areas. (c) Because the location anonymizer stores the exact location information of all users, compromising the location anonymizer exposes their locations. (d) k-anonymity typically reveals the approximate location of a user and the location privacy depends on the user distribution. In a system with such *regional location privacy* it is difficult for the user to specify personalized privacy requirements.

References

[1] B. Bamba, L. Liu, P. Pesti, and T.Wang, *"Supporting anonymous location queries in mobile environments with PrivacyGrid,"* in *WWW*, 2008.

[2] C.-Y. Chow and M. F. Mokbel, *"Enabling private continuous queries for revealed user locations,"* in *SSTD*, 2007.

[3] B. Gedik and L. Liu, *"Protecting location privacy with personalized kanonymity : Architecture and algorithms," IEEE TMC*, vol. 7, no. 1, pp. 1–18, 2008.

[4] M. Gruteser and D. Grunwald, *"Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking,"* in *ACM MobiSys*, 2003.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, *"Preventing location-based identity inference in anonymous spatial queries,"* *IEEE TKDE*, vol. 19, no. 12, pp. 1719–1733, 2007.

[6] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, *"The new casper: Query processing for location services without compromising privacy,"* in *VLDB*, 2006.

[7] T. Xu and Y. Cai, *"Location anonymity in continuous location-based services,"* in *ACM GIS*, 2007.

[8] *"Exploring historical location data for anonymity preservation in location-based services,"* in *IEEE INFOCOM*, 2008.

[9] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, *"Private queries in location based services: Anonymizers are not necessary,"* in *ACM SIGMOD*, 2008.

[10] M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, *"Efficient oblivious augmented maps: Location-based services with a payment broker,"* in *PET*, 2007.

[11] S. Wang and X. S. Wang, *"AnonTwist: Nearest neighbor queryingwith both location privacy and k-anonymity for mobile users,"* in Proc. 10th Int. Conf. Mobile Data Manag.: Syst. Services Middelware, 2009, pp. 443–448.

[12] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, *"A hybrid technique for private location-based queries with database protection,"* in *Proc. Adv. Spatial Temporal Databases*, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.

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

[14] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, *"Private queries in location based services: Anonymizers are not necessary,"* in *Proc. ACM SIGMOD*, Vancouver, BC, Canada, 2008, pp. 121–132.

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

[16] M. Gruteser and D. Grunwald, *"Anonymous usage of location based services through spatial and temporal cloaking,"* in *Proc. 1st Int. Conf. MobiSys*, 2003, pp. 31–42.

[17] T. Hashem and L. Kulik, *"Safeguarding location privacy in wireless ad-hoc networks,"* in *Proc. 9th Int. Conf. UbiComp*, Innsbruck, Austria, 2007, pp. 372–390.

[18] B. Hoh and M. Gruteser, *"Protecting location privacy through path confusion,"* in *Proc. 1st Int. Conf. SecureComm*, 2005, pp. 194–205.

[19] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, *"Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

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

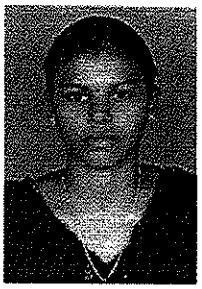
[21] J. Krumm, *"A survey of computational location privacy," Pers. Ubiquitous Comput.*, vol. 13, no. 6, pp. 391–399, Aug. 2009.

[22] E. Kushilevitz and R. Ostrovsky, *"Replication is not needed: Single database, computationally-private information retrieval,"* in *Proc. FOCS*, Miami Beach, FL, USA, 1997, pp. 364–373.

Author's Biography

Mrs. S.Priya, Research Scholar, Department of Computer Science at Sri Krishna Arts and Science College affiliated to Bharathiar University, Coimbatore.

Mrs. D.Shobana, Assistant Professor, Department of Information Technology at Sri Krishna Arts and Science College affiliated to Bharathiar University, Coimbatore.



Mrs. S.Menaka, Assistant Professor, Department of Commerce at Vivekanandha College of Arts and Science affiliated to Periyar University, Namakkal.