ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

Rational k-Nearest Neighbour Queries with Location and Query Privacy

Arthi.S.S. [1], Dr.C.Sumithradevi [2]

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India
2. Assistant Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

Abstract—In mobile communication, spatial queries pose a serious threat to user location privacy because the location of a query may reveal sensitive information about the mobile user. In this paper, we study approximate k nearest neighbor (kNN) queries where the mobile user queries the location-based service (LBS) provider about approximate k nearest points of interest (POIs) on the basis of his current location. We propose a basic solution and a generic solution for the mobile user to preserve his location and query privacy in approximate kNN queries. The proposed solutions are mainly built on the Paillier public-key cryptosystem and can provide both location and query privacy. To preserve query privacy, our basic solution allows the mobile user to retrieve one type of POIs, for example, approximate k nearest car parks, without revealing to the LBS provider what type of points is retrieved. Our generic solution can be applied to multiple discrete type attributes of private location-based queries. Compared with existing solutions for kNN queries with location privacy, our solution is more efficient. Experiments have shown that our solution is practical for kNN queries.

Index Terms—Location based query, location and query privacy, private information retrieval, Paillier cryptosystem, RSA.

1. INTRODUCTION

Location-based services (LBS) are emerging as a major application of mobile geospatial technologies. In LBS, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. Spatial range queries and k-nearest-neighbor (kNN) queries are two types of the most commonly used queries in LBS. For example, a user can make a range query to find out all shopping centers within a certain distance of her current location, or make a kNN query to find out the k nearest gas stations. In these queries, the user has to provide the LBS server with her current location. But the disclosure of location information to the server raises privacy concerns, which have hampered the widespread use of LBS. Thus, how to provision location-based services while protecting user location privacy has recently become a hot research topic. The major objectives are,

- To give a solution for kNN queries which needs one PIR only, i.e., the mobile user sends his location (encrypted) to the LBS provider and receives the k nearest POIs (encrypted) from the LBS provider.
- To give a solution for the mobile user to preserve query privacy, i.e., finding out k nearest PIOs of the same type without revealing to LBS provider what type of POIs he is interested in. For example, solution allows the mobile user to find out k nearest car parks from the LBS provider without revealing to LBS provider that the type of POIs is car park.
- To take into account sequential queries. To give a solution for the mobile user to query a sequence of POIs without need of multiple executions of the whole protocol.
- To give a generic solution which can be applied to multiple discrete types attributes of private queries.

2. RELATED WORKS

Current main techniques to preserve location privacy for
LBS are as follows.

Information access control: User locations are sent to the LBS provider as usual. This technique relies on the LBS provider to restrict access to stored location data through rule-based polices. It supports three types of location-based queries: 1) user location queries (querying the location of a specific user or users, identified by their unique identifiers); 2) enumeration queries (querying lists of users at specific locations, expressed either in terms of geographic or symbolic attributes); 3) asynchronous queries (querying "event" information,
such as when users enter or leave specific areas). This technique requires the LBS provider to maintain all user locations. It is vulnerable to misbehavior of the LBS provider.

Mix zone: A trusted middleware relays between the mobile users and the LBS provider. Before forwarding the location-based queries of the users to the LBS, the middleware anonymizes their locations by pseudonyms. The basic idea is: when a user enters a mix zone, the middleware assigns him a pseudonym, by which the user queries LBS. The communication between the user and the LBS is through the middleware and the pseudonym changes whenever the user enters the mix zone. Recently, the mix-zone has been applied to road networks. This technique requires the middleware to anonymize user locations. It is vulnerable to misbehavior of the middleware.

k-anonymity: This technique ensures that a record could not be distinguished from k-1 other records. Instead of sending a single user's exact location to the LBS, k-anonymity based schemes collect k user locations and send a corresponding (minimum) bounding region to the

LBS as the query parameter. The collection of different mobile user locations is done either by a trusted thirdparty between the users and the LBS, or via a peer-to-peer collaboration among users. Because kanonymity is achieved, an adversary can only identify a location's user with probability no higher than 1=k. This technique relies on the third party or a peer user to collect different mobile user locations. It is vulnerable to misbehavior of the third party or the peer user. "Dummy" locations: The basic idea is when the mobile user queries the LBS, he sends many random other locations along with his location to the LBS provider to confuse his location such that the server cannot distinguish the actual location from the fake locations. Different from k-anonymity based schemes, this approach include fake or fixed locations, rather than those of other mobile users, as parameters of queries sent to the LBS provider. Fake dummy locations are generated at random, and fixed locations are chosen

from special ones such as road intersections. Either way, the exact user locations are hidden from the service provider. Although this technique does not rely on any third party, the LBS provider can restrict the user in a small sub space of the total domain, leading to weak privacy.

2.1 EXISTING SYSTEM

In general, the mobile user needs to submit his location to the LBS provider which then finds out and returns to the user the k nearest POIs by comparing the distances between the mobile user's location and POIs nearby. This reveals the mobile user's location to the LBS provider. In mobile communication, spatial queries pose a serious threat to user location privacy because the location of a query may reveal sensitive information about the mobile user.

2.1.1 Disadvantages

- Existing do not support LBS queries with multiple POI type attributes,
- Low privacy
- They are vulnerable to misbehavior of the third party.
- They offer little protection when the service provider/middleware is owned by an untrusted party.
- Current PIR-based LBS queries only allow the mobile user to find out k nearest POIs regardless of the type of POIs.
- Current PIR-based LBS queries allow the mobile user to retrieve only one POI after a protocol execution

2.2. PROPOSED SYSTEM

It proposes approximate k nearest neighbor (kNN) queries where the mobile user queries the location-based service (LBS) provider about approximate k nearest points of interest (POIs) on the basis of his current location. We propose a basic solution and a generic solution for the mobile user to preserve his location and query privacy in approximate kNN queries. The proposed solutions are mainly built on the Paillier public-key cryptosystem and can provide both location and query privacy. To preserve query privacy, our basic solution allows the mobile user to retrieve one type of POIs, for example, approximate k nearest car parks, without revealing to the LBS provider what type of points is retrieved. The generic solution can be applied to multiple discrete type attributes of private location-based queries.

2.2.1 Advantage of Proposed System

- The mobile user sends his location (encrypted) to the LBS provider and receives the k nearest POIs (encrypted) from the LBS provider.
- Greatly improves the efficiency of sequential queries.
- The previous work fixed the number of nearest neighbors k. The current work allows any number of nearest neighbors' k up to K, where K is a constant.
- The previous work defined location privacy which implied query privacy. The current work defines location and query privacy separately.
- The previous work used the Rabin cryptosystem to prevent the mobile user to retrieve more than one data per query and did not allow sequential queries without multiple executions of the whole protocol.
- The current work uses RSA to achieve the data privacy and support sequential queries.

The current work adds a generic solution for multiple discrete type attributes of private location-based queries.

3. METHODOLOGY

Location-based services (LBS) are emerging as a major application of mobile geospatial technologies. In LBS, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. Spatial range queries and k-nearest-neighbor (kNN) queries are two types of the most commonly used queries in LBS. For example, a user can make a range query to find out all shopping centers within a certain distance of her current location, or make a kNN query to find out the k nearest gas stations. In these queries, the user has to provide the LBS server with her current location. But the disclosure of location information to the server raises privacy concerns, which have hampered the widespread use of LBS. Thus, how to provision location-based services while protecting user location privacy has recently become a hot research topic.

Assume, for example, that a user wishes to find the nearest night clubs to his/her location. To conceal this information, the user may choose to transmit the query through an anonymizing network (e.g., Tor [1]) that hides his/her real IP address. Nevertheless, simply removing the IP address is not sufficient to protect the user's identity, which can be inferred from the coordinates of the query and background knowledge (e.g., the user's home address). Hence, truly private services necessitate location privacy, i.e., the LBS should be oblivious of the query location. Additionally, location privacy is desirable independently of the concealment of the user identity. For instance, consider a mobile user who asks for the nearest night clubs, but wishes to hide that he/she has visited the specific area. In this case, the user requires location privacy even if the provider can infer his/her identity.

The embedding of positioning capabilities (e.g., GPS) in mobile devices facilitates the emergence of locationbased services (LBS), which is considered as the next "killer application" in the wireless data market. LBS allows clients to query a service provider (such as Google or Bing Maps) in a ubiquitous manner, in order to retrieve detailed information about points of interest (POIs) in their vicinity (e.g., restaurants, hospitals, etc.).

The LBS provider processes spatial queries on the basis of the location of the mobile user. Location information collected from mobile users, knowingly and unknowingly, can reveal far more than just a user's latitude and longitude. Knowing where a mobile user is can mean knowing what he/she is doing: attending a religious service or a support meeting, visiting a doctor's office, shopping for an engagement ring, carrying out non-work related activities in office, or spending an evening at the corner bar. It might reveal that he is interviewing for a new job or "out" him as a participant at a gun rally or a peace protest. It can mean knowing with whom he/she spends time, and how often. When location data are aggregated it can reveal his/her regular habits and routines - and when he deviates from them. [7] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC).

A study of approximate k nearest neighbor (kNN) queries has been conducted where the mobile user queries the locationbased service provider about approximate k nearest points of interest on the basis of his current location. In general, the mobile user needs to submit his location to the LBS provider which then finds out and returns to the user the k nearest POIs by comparing the distances between the mobile user's location and POIs nearby. This reveals the mobile user's location to the LBS provider. To analyze the security of our solutions, it defines a security model for private kNN queries. The security analysis has shown that our solutions ensures both location privacy in the sense that the user does not reveal any information about his location to the LBS provider and query privacy in the sense that the user does not reveal what type of POIs he is interested in to the LBS provider. In addition, these solutions have data privacy in the sense that the LBS provider releases to the user only k nearest POIs per query. The proposed model considers a location-based service scenario in mobile environments, as shown in Fig. 1, where there exist the mobile user, the location-based service provider, the base station and satellites, each playing a different role.

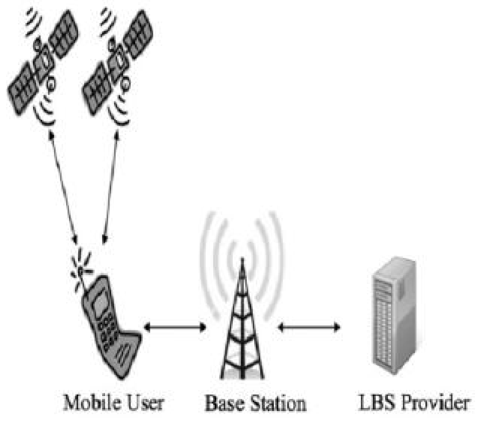

Fig. 1 Location Based Service

.

- The mobile user sends location-based queries to the LBS provider (or called the LBS server) and receives location-based service from the provider.
- The LBS provider provides location-based services to the mobile user.
- The base station bridges the mobile communications between the mobile user and the LBS provider.
- Satellites provide the location information to the mobile user.

3.1 MODULES

MOBILE USER

In this Module, the mobile user sends location-based queries to the LBS provider (or called the LBS server) and receives location-based service from the provider. The mobile user queries the location based service provider about approximate k nearest points of interest on the basis of his current location. In general, the mobile user needs to submit his location to the LBS provider which then finds out and returns to the user the k nearest POIs by comparing the distances between the mobile user's location and POIs nearby. This reveals the mobile user's location to the LBS provider.

BASE STATION

In this Module, the base station bridges the mobile communications between the mobile user and the LBS provider. The base station sends the user query to LBS Server and LBS response to the Mobile users. We assume that the mobile user can acquire his location from satellites anonymously, and the base station and the LBS provider do not collude to comprise the user location privacy or there exists an anonymous channel such as Tor2 for the mobile user to send queries to and receive services from the LBS provider.

LBS PROVIDER

In this Module, the LBS provider provides location-based services to the mobile user. LBS allows clients to query a service provider in a ubiquitous manner, in order to retrieve detailed information about points of interest (POIs) in their vicinity (e.g., restaurants, hospitals, etc.). The LBS provider processes spatial queries on the basis of the location of the mobile user. Location information collected from mobile users, knowingly and unknowingly, can reveal far more than just a user's latitude and longitude.

CONSTRUCTION OF PRIVATE KNN QUERY PROTOCOL

In this module, basic construction of private kNN query protocol has been given. Before execution of any private kNN protocol, an initialization occurs in the LBS server. First of all, the LBS server divides the location-based database D (a geographic map) into cells with the same size, for example, 1 km width and 1 km length, denoted as grid ¼ 1 km. Based on the center of each cell, given a type of POIs, the LBS server collects K nearest POIs of the type. It is assumed that POI types are coded into 1; 2; . . .;m which is published to the public. Examples of POI types includes: Churches, Schools, Post offices / postboxes, Telephone boxes, Restaurants, Pubs, Car parks, Speed cameras, Tourist attractions and etc.

4. CONCLUSION

The system has presented a basic and a generic approximate kNN query protocols. Security analysis has shown that these protocols have location privacy, query privacy and data privacy. Performance has shown that the basic protocol performs better than the existing PIRbased LBS query protocols in terms of both parallel computation and communication overhead. Experiment evaluation has shown that the basic protocol is practical.

FUTURE WORK

Location-Based Service (LBS) is a service that provides the information and the number of uses in social network as in security that is accessible through mobile network and finds the geographical location of the mobile device using that location .It is used in different contexts such as entertainment, indoor object search, health. One of its most powerful aspects is that it provides spatial patterns. It evolved from simple based service models to complex tools for implementing any location based service model or facility. The important thing about this service is the data about subscribers location is owned and controlled by the network operators, including mobile carriers and mobile content providers. The privacy of the user in different distributed networks is considered by using location-based query algorithm efficiently. It proposes an algorithm which offers the location query services simultaneously to multiple users thus improving the performance of the server and satisfy the request of users' location. thefuture work is to implement our protocol on mobile devices.

REFERENCES

[1] M. Bellare and P. Rogaway. Optimal asymmetric encryption – how to encrypt with RSA. In Proc. Eurocrypt 1994.

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

[3] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing 2(1), 2003.

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

[5] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31 (4): 469-472, 1985.

[6] Y. Elmehdwi, B. K. Samanthula, W. Jiang. Secure k-nearest neighbor query over encrypted data in outsourced environments. In Proc. ICDE 2014.

[7] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[8] 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 2008.

[9] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino. Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection. GeoInformatica 15(14): 699-726, 2010.

[10] G. Ghinita, R. Rughinis. An efficient privacy-reserving system for monitoring mobile users: making searchable encryption practical. in Proc. ACM CODASPY 2014.

[11] Haibo Hu, Jianliang Xu, Chushi Ren, and Byron Choi, Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism, In Proc. ICDE 2011.

[12] A. Khoshgozaran and C. Shahabi. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In Proc. SSTD 2007.

[13] H. Kido, Y. Yanagisawa, and T. Satoh. An anonymous communication technique using dummies for location-based services. In Proc. ICPS 2005, pages 88 - 97.