International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

An Efficient Privacy Preserving Query Solution for Smart Phones

V.Muni Babu & A Emmanuel Raju

[1]M.Tech Student, Department of CSE, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, A.P

[2]Assistant Professor, Department of CSE, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, A.P

Abstract— The prevalence of smart phones, location based services (LBS) have received noticeable attention and has become prominent and vital. Despite the use of LBS, it also poses a serious concern on user's location privacy. In this paper, we propose a safe tourist application for privacy preserving spatial range query. The aim is to outsource the location based service (LBS) data from the LBS provider to the cloud and from the cloud to the LBS user without any privacy breach. To achieve privacy preserving spatial range query, we propose the first predicate only encryption scheme for inner product range, which can be used to detect whether a position is within a given circular area in a privacy-preserving way. To avoid scanning of all POIs to find matched POIs, we further exploit the novel index structure named ss tree, which conceals sensitive location information with our IPRE scheme. In particular, for a mobile LBS user using an Android phone, around 0.9 second is needed to generate a query.

***Keywords*— Location based services (LBS), spatial range query, point of interest (POI), Inner product range (IPRE).**

I. INTRODUCTION

Around ten years ago, location-based services (LBS) were used in military only. Today, thanks to advance in communication technologies and information technologies, more kinds of location based services have appeared, and they are useful for not only organizations but also individuals. Mobile LBS are services enhanced with positional data, which are provided by mobile apps using GPS, D maps, and other techniques. Many mobile apps provide interesting and convenient lbs and functions. The mobile app Yelp recommends nearby shops, restaurants, *etc*. In the social network mobile app Loops, the users receive notifications whenever their friends are nearby. The mobile app Waze reports nearby traffic jams, gas stations and friends. Users can access these services via the desktop, mobile phone, Personal Digital Assistant pager, Web browser, or other devices. Diverse applications include fleet tracking, emergency dispatch, roadside assistance, navigation, and more. With overall view, the LBS applications can be categorized as:

❖ Navigation applications such as Route description, Turn-by-turn navigation.

- Safety and emergency applications like nearest medic center, Emergency calls, Warning about unsafe areas.
- Tracking applications such as Find a friend, Asset tracking etc.
- Information service applications like Traffic information, City Guide, Parking, Maps etc.
- Operator & Tariff applications like Traffic measurements, Network planning.

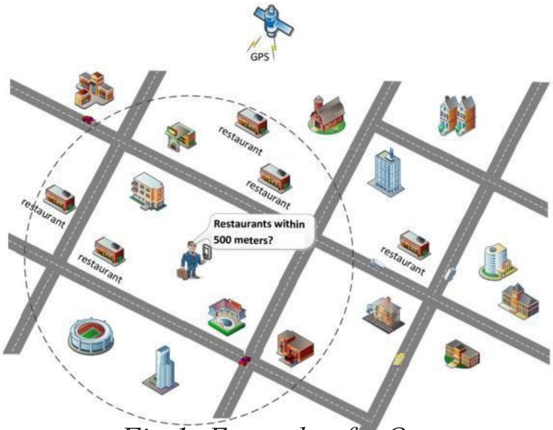

Fig 1: Example of a Query

While LBS are popular and vital, most of these services today including spatial range query require users to submit their locations, which raises serious concerns about the leaking and misusing of user location data. For example, criminals may utilize the data to track potential victims and predict their locations. For another example, some sensitive location data of organization users may involve trade secret or national security. Protecting the privacy of user location in LBS has attracted considerable interest. However, significant challenges still remain in the design of privacy-preserving LBS, and new challenges arise particularly due to data outsourcing. In recent years, there is a growing trend of outsourcing data including LBS data because of its financial and operational benefits. Lying at the intersection of mobile computing and cloud computing, designing privacy-preserving outsourced spatial range query faces the challenges below.

1. The LBS provider is not willing to disclose its valuable LBS data to the cloud. As illustrated in Fig. 2, the LBS provider encrypts and outsources private LBS data to the cloud, and LBS users query the encrypted data in the cloud. As a result, querying encrypted LBS data without privacy breach is a big challenge, and we need to protect not only the user locations from the LBS provider and cloud but also LBS data from the cloud.

2. Many LBS users are mobile users, and their terminals are smart phones with very limited resources. However, the cryptographic or privacy-enhancing techniques used to realize privacy-preserving query usually result in high computational cost and/or storage cost at user side.

3. Spatial range query is an online service, and LBS users are sensitive to query latency. To provide good user experiences, the POI search performing at the cloud side must be done in a short time (e.g., a few seconds at most). Again, the techniques used to realize privacy-preserving query usually increase the search latency.

II.SYSTEM ANALYSIS

The necessity to protect the privacy of the user location has drawn more importance. However, symbolic challenges still exist in the design of privacy-preserving LBS and new challenges arise due to data outsourcing. Designing privacy-preserving outsourced spatial range query faces the challenges below:

- Querying encrypted LBS data
- The resource consumption in mobile devices
- The efficiency of POI searching
- Security

The revealing of user locations to LBS provider raises a priority of intrusion on location privacy that has hampered the widespread use of LBS. Thus, a way to fancy LBS with preservation of location privacy has been increasingly gaining attention. There are mainly two classes of approach to preserve location privacy for LBS:

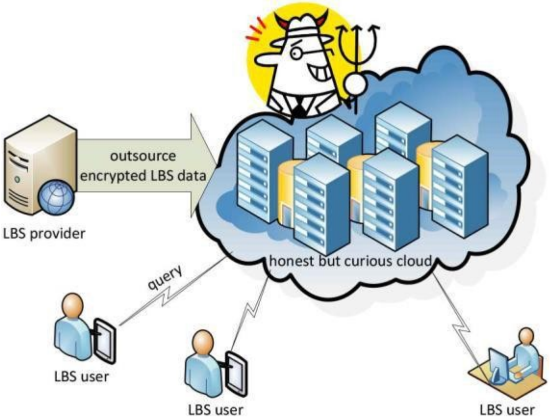

Fig 2: System model of LBS

- The primary is through data access management. It depends on the service suppliers to limit access to keep location information through rule-based polices.
- The second being to use a trustworthy middleware running between the clients and the service provider.

A user will specify for every location-based query, the privacy demand with a minimum spatial space of his interest to hide the location. The main contributions of this paper are two folds. IPRE scheme: which allows testing whether the inner product of two vectors is within a given range without disclosing the vectors. Privacy Preserving scheme: shows whether a POI matches a spatial range query or not.

Our solution consists of two algorithms:

1. System Setup and
2. Spatial Range Search.

A. System Setup:

The LBS provider initializes the system by the following steps.

Step 1) The LBS provider initializes the public parameter and keys of the proposed IPRE scheme as well as the key of a standard encryption scheme.

Step 2) The LBS provider builds an ˆ ss-tree for the LBS database.

Step 3) The LBS provider encrypts each POI record with the standard encryption scheme.

Step 4) The LBS provider outsources all encrypted POI records and the ˆ ss-tree to the cloud.

B. Spatial Range Search

Suppose an LBS user wants to find all POIs within a circular area, the privacy-preserving query is performed by the following steps.

Step 1) The LBS user generates two tokens for searching POI records with the proposed IPRE scheme.

Step 2) The user sends (Ks[0], Ks[1]) as a query to the cloud.

Step 3) The cloud searches ˆ ss-tree to find all leaf nodes matching the query from the user.

Step 4) The cloud returns the corresponding POI records of matched leaf nodes to the user.

Step 5) The LBS user decrypts received POI records with the shared key of the standard encryption scheme.

Under the outsourced LBS system, our design goal is to develop an efficient, secure and accurate, solution for privacy-preserving SRQ. Specifically for achieving following three objectives:

1. Efficiency

Spatial range query has extreme performance requirements. A good solution should not consume many resources of mobile LBS users, and the Point Of Interest search latency should be acceptable for online query.

2. Accuracy

It is advantageous that a query result contains the exact records that matching the query. False negatives would hurt user experience, while false positives would increase communication cost.

3. Security

The proposed solution should be resilient to cipher text-only attacks and known-sample attacks. An accurate and efficient solution for spatial range query already exists, which is resilient to cipher text-only attacks but not to known-sample attacks and more powerful attacks. The proposed solution should be more secure than available solution.

III.SYSTEM CONSTRUCTION

1) The LBS Provider has abundant of LBS data, which are POI records. The LBS provider allows authorized users (i.e., LBS users) to utilize its data through location-based queries. Because of the financial and operational benefits of data outsourcing, the LBS provider offers the query services via the cloud.

2) The Cloud has rich storage and computing resources. It stores the encrypted LBS data from the LBS provider, and provides query services for LBS users. So, the cloud has to search the encrypted POI records in local storage to find the ones matching the queries from LBS users.

3) LBS users have the information of their own locations, and query the encrypted records of nearby POIs in the cloud. Cryptographic or privacy-enhancing techniques are usually utilized to hide the location information in the queries sent to the cloud. To decrypt the encrypted records received from the cloud, LBS users need to obtain the decryption key from the LBS provider in advance.

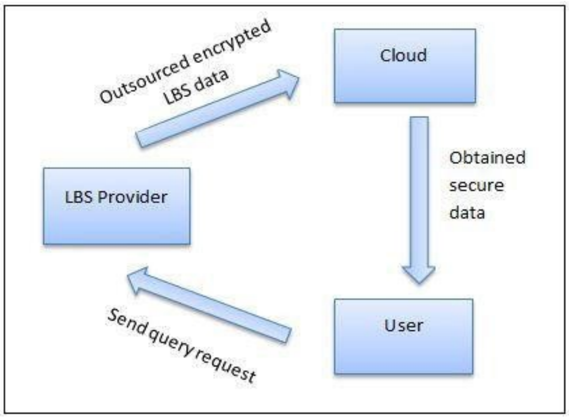

Fig 3: Structure of Proposed System

IV.CONCLUSION

In this paper, we have proposed EPLQ, an efficient privacy preserving spatial range query solution for smart phones, which preserves the privacy of user location, and achieves confidentiality of LBS data. To realize EPLQ, we have designed an IPRE and a novel privacy-preserving index tree named

ˆ **ss**-tree. Our techniques have potential usages in other kinds of privacy preserving queries. If the query can be performed **through comparing inner products to a given range, the proposed IPRE and ˆ**

ss-tree may be applied to realize privacy preserving query. Two potential usages are privacy-preserving similarity query and long spatial range query.

V.REFERENCES

[1]lichun li, rongxinglu, *senior member, ieee*, and chenghuang “EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data.” IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 2, APRIL 2016.

[2]T. K. Dang, j. Küng, and r. Wagner, “the shtree: a super hybrid indexStructure for multidimensional data,” in proc. 12th int. Conf. DatabaseExpert syst. Appl.(dexa’01), munich, germany, sep. 3–5, 2001,Pp. 340–349.

[3]A. Gutscher, “coordinate transformation a solution for the privacyProblem of location based services?” In *proc. 20th int. Parallel distrib.Process.Symp. (ipdps’06)*, rhodes

island, greece, apr. 25–29, 2006,P. 424.

[4]A. Khoshgozaran and c. Shahabi, “blind evaluation of nearest neighbor Queries using space ransformation to preserve location privacy,” in*Advances in spatial and temporal databases*. New york, ny, usa:Springer, 2007, pp. 239–257.

[5]G. Ghinita, p. Kalnis, a. Khoshgozaran, c. Shahabi, and k.-l. Tan,“private queries in location based services: anonymizers are not necessary,”In *proc. Sigmod*, 2008, pp. 121–132.

[6]W. K. Wong, d. W.-l. Cheung, b. Kao, and n. Mamoulis, “secureKnn computation on encrypted databases,” in *proc. Sigmod*, 2009,Pp. 139–152.

[7]M. L. Yiu, g. Ghinita, c. S. Jensen, and p.Kalnis, “enabling searchServices on outsourced private spatial data,” *vldb*j., vol. 19, no. 3,Pp. 363–384, 2010.

[8]B. Yao, f. Li, and x. Xiao, “secure nearest neighbor revisited,” in *proc.Ieee 29th int. Conf. Data eng. (icde’13)*, 2013, pp. 733–744.

[9]X. Yi, r. Paulet, e. Bertino, and v. Varadharajan, “practical *k* nearestNeighbor queries with location privacy,” in *proc. 30th int. Conf. DataEng. (icde)*, 2014, pp. 640–651.

[10] J. Shao, r. Lu, and x. Lin, “fine: a fine-grained privacy-preservingLocation-based service framework for mobile devices,” in *proc.IeeeInfocom*, 2014, pp. 244–252.

[11] B. Hore, s. Mehrotra, m. Canim, and m. Kantarcioglu, “secure multidimensional Range queries over outsourced data,” *vldb j.*, vol. 21, no. 3,Pp. 333–358, 2012.