IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 5, May 2017

Efficient Query Processing on Outsourced Encrypted Data in Cloud with Privacy Preservation

Lakshmi A[1], Mandara Nagendra[2], Shreeraksha L[3], Chandru A S[4]

BE Student, Dept. of Information Science and Engineering, NIE Institute of Technology, Mysore, Karnataka, India[1,2,3]

Assistant Professor, Dept. of Information Science and Engg, NIE Institute of Technology, Mysore, Karnataka, India[4]

Abstract: With 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 a few decades ago, location-based services (LBS) were used in military only. Today, thanks to advance in communication and information technologies, added location based services have appeared, and they are purposive for not only organizations but also individuals. Mobile LBS are services enhanced with positional data, which are provided by mobile apps using GPS, Dmaps, and other techniques.

A location-based service (LBS) is a software-level service that uses location data to control features. LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine (ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services.

The mobile app Foursquare recommends nearby shops, restaurants, etc. The mobile app Loopt helps discover friends nearby. The mobile app Waze reports nearby traffic jams. The app MapQuest is a navigation app.

Spatial range query is a widely used LBS, which allows a user to find points of interest (POIs) within a given distance to his/her location. As illustrated in Fig. 1, with this kind of LBS, a user could obtain the records of all restaurants within walking distance (say 500 m). Then, the user can go through these records to find a desirable restaurant considering price and reviews.

Fig. 1: Example of spatial range query

DOI10.17148/IJARCCE.2017.6596

While LBS are prominent 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.

II. COMPARATIVE STUDY

Our work is related to not only privacy-preserving LBS but also privacy-preserving query over outsourced encrypted data. We review the works pertinent to privacy-preserving spatial range query.

T. K. Dang, j. Küng, and r. Wagner [2]- This paper provides the solutions designed based on coordinate transformation would be vulnerable to known sample attacks.

G. Ghinita, p. Kalnis, a. Khoshgozaran, c. Shahabi [4]- To enforce security and privacy on such a service model, we need to protect the data running on the platform. Unfortunately, traditional encryption methods that aim at providing "unbreakable" protection are often not adequate because they do not support the execution of applications such as database queries on the encrypted data. So this framework does not require a trusted third party, since privacy is achieved via Cryptographic techniques and also doesn't require an anonymizers or Collaborating trustworthy users.

W. K. Wong, d. W.l.Cheung, b. Kao [5]- General problem of secure computation on an encrypted database and propose a SCONEDB(secure computation on an encrypted database) model, which captures the execution and security requirements so database can be secure.

J. Shao, r. Lu, and x. Lin [6]- Fine-grained privacy-preserving location-based service adopts the data-as-a-service (daas) model, where the lbs provider publishes its data to a third party(e.g., cloud server) who executes users' lbs queries, a cipher text-policy anonymous attribute-based encryption technique to achieve fine-grained access control, location privacy, confidentiality of the lbs.

III. 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:

- 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.

IV. PRIVACY PRESERVING SCHEME

Our solution consists of two algorithms: system setup and 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.

V. SYSTEM MODEL

A system model is the conceptual model as a result of system modelling that describes and represents a system.
As shown in Fig.2, the system model of outsourced LBS consists of LBS provider, the cloud and LBS user.
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.

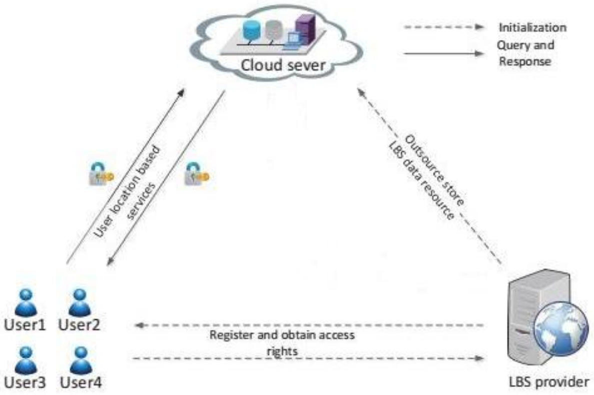
Cloud sever
Initialization
Query and Response
User location based services
Outsource store LBS data resource
User1
User2
User3
User4
Register and obtain access rights
LBS provider

Fig. 2: System Model of outsourced LBS

The LBS provider is not willing to disclose its valuable data to cloud. So encrypts the LBS data and sends the encrypted LBS data to the cloud.
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.
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. LBS users need to obtain the decryption key from the LBS provider in advance to decrypt the encrypted records received from the cloud.

VI. RELATED WORKS

A. Solutions Applicable to Outsourced LBS

Privacy-preservation based on coordinate Transformation: the coordinates of queries and POIs in the original coordinate system are transformed to new coordinates in a new coordinate system. After the transformation, the distance information of any two points is still preserved. This is applied in Client server environment in road networks, location monitoring services in wireless sensor network.

Privacy-preserving POI query based on Private Information Retrieval (PIR): Only PIR-based solutions can protect the privacy in both public LBS and outsourced LBS. PIR help the users to keep sensitive information from being leaked in an SQL query. It hides the sensitive constants contained in the redicates of a query. It avoids server collusion.

B. Solutions for Public LBS Only

Privacy-preserving LBS based on anonymous communication: here, one or more third parties relay messages between users and the LBS provider. This approach hides the linkage between user identities and messages from the LBS provider. The query area would be exposed to the LBS provider, but the user sending the query is hidden among a set of users. This is applied in document sharing, media players, and map browsers.

Privacy-preserving LBS based on location obfuscation: To prevent the LBS provider from knowing users' precise locations, users submit low precision locations or fake locations along with real locations. These solutions offer a weak level of privacy. It mainly concentrates on LBS which wants to know the distance travelled by user for providing their services and also used in navigation applications.

Privacy-preserving LBS based on spatial cloaking: this solution combine anonymous communication and location obfuscation techniques together. To the LBS provider, a user cannot be identified from a set of users in a cloaking area, and the cloaking area instead of users' precise locations are sent to the LBS provider. This is used to blur user location information before it is submitted to the location based database server, in order to preserve user location privacy in LBS.

VII. 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.

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 sh-tree: a super hybrid indexStructure for multidimensional data," in proc. 12th int. Conf. DatabaseExpert syst. Appl. (dexa' 01), munich, germany, Pp. 340–349,sep. 3–5, 2001.

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

[4] 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, pp. 121–132, 2008.

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

[6] J. Shao, r. Lu, and x. Lin, "Fine: a fine-grained privacy-preserving Location-based service framework for mobile devices," in proc. Ieee Infocom, pp. 244–252,2014.

DOI10.17148/IJARCCE.2017.6596