**EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data**

**ABSTRACT:**

With the pervasiveness of smart phones, location based services (LBS) have received considerable attention and become more popular and vital recently. However, the use of LBS also poses a potential threat to user’s location privacy. In this paper, aiming at spatial range query, a popular LBS providing information about points of interest (POIs) within a given distance, we present an efficient and privacy-preserving location-based query solution, called EPLQ. Specifically, to achieve privacy preserving spatial range query, we propose the first predicate-only encryption scheme for inner product range (IPRE), which can be used to detect whether a position is within a given circular area in a privacy-preserving way. To reduce query latency, we further design a privacy-preserving tree index structure in EPLQ. Detailed security analysis confirms the security properties of EPLQ. In addition, extensive experiments are conducted, and the results demonstrate that EPLQ is very efficient in privacy preserving spatial range query over outsourced encrypted data. In particular, for a mobile LBS user using an Android phone, around 0.9 s is needed to generate a query, and it also only requires a commodity workstation, which plays the role of the cloud in our experiments, a few seconds to search POIs.

**EXISTING SYSTEM:**

* Recently, there are already some solutions for privacy preserving spatial range query.
* 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.

**DISADVANTAGES OF EXISTING SYSTEM:**

* *Challenge on querying encrypted LBS data*. The LBS provider is not willing to disclose its valuable LBS data to the cloud. 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.
* *Challenge on the resource consumption in mobile devices*. 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.
* *Challenge on the efficiency of POI searching*. 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.
* *Challenge on security*. LBS data are about POIs in real world. It is reasonable to assume that the attacker may have some knowledge about original LBS data.With such knowledge, known-sample attacks are possible.

**PROPOSED SYSTEM:**

* In this paper, we propose an efficient solution for privacy-preserving spatial range query named EPLQ, which allows queries over encrypted LBS data without disclosing user locations to the cloud or LBS provider.
* To protect the privacy of user location in EPLQ, we design a novel predicate-only encryption scheme for inner product range (IPRE scheme for short), which, to the best of our knowledge, is the first predicate/predicate-only scheme of this kind. To improve the performance, we also design a privacypreserving index structure named ˆ *ss*-tree. Specifically, the main contributions of this paper are three folds.
* We propose IPRE, which allows testing whether the inner product of two vectors is within a given range without disclosing the vectors. In *predicate encryption*, the key corresponding to a predicate *f* can decrypt a ciphertext if and only if the attribute of the ciphertext *x* satisfies the predicate, i.e., *f*(*x*) = 1. *Predicate-only encryption* is a special type of predicate encryption not designed for encrypting/decrypting messages. Instead, it reveals that whether *f*(*x*) = 1 or not. Predicate-only encryption schemes supporting different types of predicates have been proposed for privacy-preserving query on outsourced data.
* We propose EPLQ, an efficient solution for privacy preserving spatial range query. In particular, we show that whether a POI matches a spatial range query or not can be tested by examining whether the inner product of two vectors is in a given range. The two vectors contain the location information of the POI and the query, respectively. Based on this discovery and our IPRE scheme, spatial range query without leaking location information can be achieved. To avoid scanning all POIs to find matched POIs, we further exploit a novel index structure named ˆ *ss*-tree, which conceals sensitive location information with our IPRE scheme.
* Our techniques can be used for more kinds of privacypreserving queries over outsourced data. In the spatial range query discussed in this work, we consider Euclidean distance, which is widely used in spatial databases. Our IPRE scheme and ˆ *ss*-tree may be used for searching records within a given weighted Euclidean distance or great-circle distance as well.Weighted Euclidean distance is used to measure the dissimilarity in many kinds of data, while great-circle distance is the distance of two points on the surface of a sphere.

**ADVANTAGES OF PROPOSED SYSTEM:**

* To the best of our knowledge, there does not exist predicate/predicate-only scheme supporting inner product range. Though our scheme is used for privacypreserving spatial range query in this paper, it may be applied in other applications as well.
* Experiments on our implementation demonstrate that our solution is very efficient.
* Moreover, security analysis shows that EPLQ is secure under known-sample attacks and ciphertext-only attacks.
* Using great-circle distance instead of Euclidean distance for long distances on the surface of earth is more accurate. By supporting these two kinds of distances, privacy-preserving similarity query and long spatial range query can also be realized.

**SYSTEM ARCHITECTURE:**



**MODULES:**

* System Construction Module
* LBS User
* LBS Provider
* Privacy-Preserving Spatial Range Query

**MODULES DESCSRIPTION:**

**System Construction Module**

* 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. However, the LBS provider is not willing to disclose the valuable LBS data to the cloud. Therefore, the LBS provider encrypts the LBS data, and outsources the encrypted 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. To decrypt the encrypted records received from the cloud, LBS users need to obtain the decryption key from the LBS provider in advance.

**LBS 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.

**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.

**Privacy-Preserving Spatial Range Query**

* In EPLQ, user queries and the sensitive location information are encrypted with IPRE scheme. A query consists of two tokens associated with two predicate vectors, which contains the LBS user’s location information. The LBS user generates two tokens for searching
* POI records with the proposed IPRE scheme. The two tokens associated with the query area should be generated. Let Ks[0] and Ks[1] be the generated two tokens.
* The user sends a query to the LBS Service Provider. The LBS Service Provider searches to find all leaf nodes matching the query from the user. The LBS Service Provider returns the corresponding POI records of matched leaf nodes to the user. The LBS user decrypts received POI records with the shared key of the standard encryption scheme.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL

**REFERENCE:**

Lichun Li, Rongxing Lu, *Senior Member, IEEE*, and Cheng Huang, “EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data”, **IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 2, APRIL 2016.**