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 POIs (Points Of Interest) 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, 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 second 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.

**Introduction:**

A few decades ago, location-based services (LBS) were used in military only. Today, thanks to advances in information and communication technologies, more kinds of LBS have appeared, and they are very useful for not only organizations but also individuals. Let’s take the spatial range query, one kind of LBS that we will focus on in this paper, as an example. Spatial range query is a widely used LBS, which allows a user to find POIs (Point Of Interests) within a given distance to his/her location, i.e., the query point. As illustrated in Fig. 1, with this kind of LBS, a user could obtain the records of all restaurants within walking distance (say 500 meters). Then the user can go through
these records to find a desirable restaurant considering price and reviews

**Existing system:**

In Existing System 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 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
Disadvantages:

✓ 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.

✓ 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.

Proposed System:

In proposed System we implemented 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 a novel predicate-only encryption scheme for inner product range named IPRE and a novel privacy-preserving index tree named \( \hat{ss} \)-tree. EPLQ’s efficacy has been evaluated with theoretical analysis and experiments, and detailed analysis shows its security against known-sample attacks and ciphertext-
only attacks. 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 ∗ss-tree may be applied to realize privacy-preserving query. Two potential usages are privacy-preserving similarity query and long spatial range query. In the future, we will design solutions for these scenarios and identify more usages.

Advantages:
- Efficiency
- Accuracy
- Security

Architecture:
Hardware Requirement:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech
- Ram : 512 Mb.
- MOBILE : ANDROID

Software Requirement:

- Coding Language : Java 1.7
- Tool Kit : Android 2.3 ABOVE
- IDE : Eclipse