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.
Existing system:
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

Disadvantage:

✓ Querying encrypted LBS data without privacy breach is a big challenge

✓ High computational cost and/or storage cost at user side.

✓ The techniques used to realize privacy-preserving query usually increase the search latency
Above Diagram represent System model of outsourced LBS

Proposed system:

First, we propose a novel predicate-only encryption scheme for inner product range named IPRE, which allows testing whether the inner product of two vectors is within a given range without disclosing the vectors.

Second, 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.

✓ Third, our techniques can be used for more kinds of privacy-preserving queries over outsourced data. In the spatial range query discussed in this work, we consider Euclidean distance, which is widely used in spatial databases.

Advantages:

✓ Our techniques have potential usages in other kinds of privacy-preserving queries

✓ Cost will be less compared to existing system

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 a novel predicate-only encryption scheme for inner product range named IPRE and a novel privacy-preserving index tree named 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.

**Hardware Specification:**

- 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 Specification:**

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


