International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Privacy Preserving Spatial Range Query Over Outsourced Encrypted Data

[1] Shaik Nahida Begum, [2] N.B.S. Vijay Kumar, [3] A. Sandhya Rani
[1]*M.Tech Student, Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA , A.P, India*
[2]*Assistant Professor, Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA, A.P, India*
[3]*Assistant Professor & HOD, Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA, A.P, India*

Abstract: *The 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.*

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. The techniques used to realize privacy-preserving query usually increase the search latency.

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 and an efficient solution for privacy-preserving spatial range query. In particular, we show that whether a POI matches aspatial range query or not can be tested by examining whether the inner product of two vectors is in a given range. This 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.

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 cipher text-only attacks. 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 and two potential usages are privacy preserving similarity query and long spatial range query.

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, Dmaps, 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 Loopt, 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.

The time of advance technologies and services, location access is one of the important feature. The accessing of the location via using several technologies has made it life easy at the industrial as well as the domestic level. The

Location based services is one of the software level service which is used to determine the Point of interest (POIs) within the given range of the individual's distance. The LBS helps in determining the location of any person, object or any activity which is being held at a particular location. The Industrial sectors has greatly benefited from the use of LBS software especially in the operational and banking sectors usually helping out to determine the locations of ATMs, online wire transfer, etc. Due to its tremendous benefits to the industrial, social and individual level it has become ever growing trend in the recent times to outsource the use of LBS. There always comes a bane with the boon using the advanced technologies. In most of the LBS software it is necessary for users to submit their locations, which increases the concerns on issues about leaking and misusing the user location data. This loophole of the LBS has led to several social calamities in criminal activities, Trade secrets and as high as to national security. With the ever growing use of the LBS it has become absolutely essential to protect the privacy of user location. With the outsourcing of the LBS in the recent times it has raised several challenges.

II. RELATED WORK

1) Anonymity can provide a high degree of privacy, save service users from dealing with service providers privacy policies, and reduce the service providers requirements for safe guarding private information. We construct public-key systems that support comparison queries. On encrypted data as well as more general queries such as subset queries. These systems support arbitrary conjunctive queries without leaking information on individual conjuncts. In addition, we present a general framework for constructing and analyzing public-key systems supporting queries on encrypted data.

2) In Secure KNN computation on encrypted database, service providers like Google and Amazon are moving into the Software as a Service business. They turn their huge infrastructure into a cloud-computing environment and aggressively recruited businesses to run applications on their respective platforms. To enforce security and privacy on such the service model, we need to provide protection to the data running on the platforms. 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.

3) A. Gutscher proposes Private, a distributed architecture for anonymous location-based queries, which addresses the problems of existing systems. (i) Develop a superior K-ASR construction mechanism that guarantees query anonymity even if the attacker knows the location of all user. (ii) Introduce a distributed protocol used by mobile entity to self-organize into a fault-tolerant overlay network. In Private, K-ASRs are built in a decentralized fashion, therefore the bottleneck of the centralized server is avoided. Since the state of the system is distributed, Private is resilient to attacks. This approach hurts the accuracy and timeliness of the responses from the Server. B.Hoh the challenge of providing strong privacy guarantees while maintaining high data accuracy of time-series location data. Specifically, the key contributions of this work are: 1. Introduction of a novel time-to-confusion metric to evaluate privacy in a set of location traces. 2. Development of an uncertainty-aware privacy algorithm that can guarantee a specified maximum time-to-confusion.

III. 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.

IV. 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 privacy preserving 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 privacy preserving 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.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

SYSTEM ARCHITECTURE

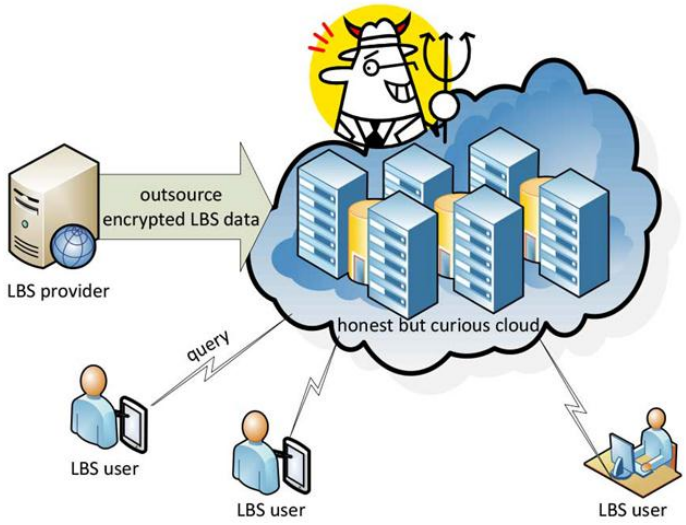

Fig 1: system Architecture

IMPLEMENTATION

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.

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed EPLQ, an efficient privateness keeping spatial range question answer for smart phones, which preserves the privateness of person vicinity, and achieves confidentiality of LBS statistics. To understand EPLQ, we have designed an IPRE and a singular privateness-maintaining index tree named ˆ ss-tree. EPLQ's efficacy has been evaluated with theoretical analysis and experiments, and exact evaluation shows its security in opposition to recognized-pattern assaults and ciphertext-only attacks. Our strategies have potential usages in other kinds of privateness keeping queries. If the query can be achieved thru evaluating internal merchandise to a given range, the proposed IPRE and ˆ ss-tree may be carried out to recognize privateness-keeping query. Two capacity usages are privateness-maintaining similarity question and long spatial variety query. In the destiny, we can design solutions for these eventualities and discover more usages.

References

[1] A. Gutscher, "Coordinate transformation—A solution for the privacy problem of location based services?" in *Proc. 20th Int. Parallel Distrib. Process. Symp. (IPDPS'06)*, Rhodes Island, Greece, Apr. 25–29, 2006, p. 424.

[2] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure kNN computation on encrypted databases," in *Proc. SIGMOD*, 2009, pp. 139–152.

[3] 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.

[4] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical *k* nearest neighbor queries with location privacy," in *Proc. 30th Int. Conf. Data Eng. (ICDE)*, 2014, pp. 640–651.

[5] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *J. ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[6] F. Olumofin and I. Goldberg, "Revisiting the computational practicality of private information retrieval," in *Financial Cryptography and Data Security*. New York, NY: Springer, 2012, pp. 158–172.

[7] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Proc. 27th Ann. Int. Conf. Theory Appl. Cryptograph. Tech. Adv. Cryptol. (EUROCRYPT '08)*, Istanbul, Turkey, Apr. 13–17, 2008, pp. 146–162.

[8] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory Cryptograph. Conf. (TCC'07)*, Amsterdam, The Netherlands, Feb. 21–24, 2007, pp. 535–554.

[9] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[10] D. A. White and R. Jain, "Similarity indexing with the ss-tree," in *Proc. 12th Int. Conf. Data Eng. (ICDE)*, 1996, pp. 516–523.