Encrypt Solitude Preserving Position Based Service Over Cloud Data

Mr.S.Gokulakrishnan
Assistant Professor, Department of Computer Science,
SrimathSivagnanaBalayaSwamigal Tamil Arts and Science College
Mailam, Tindivanam, Villupuram– India

J.Jayalakshmi,
PG-M.Sc(cs),
S.S.B.S.Tamil, Arts & Science College, Tamilnadu, India

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.

Keyword: Privacy, Location Based Services, Encrypt, Point of interest (POIs), inner product range (IPRE)

1.INTRODUCTION

Around afew 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 us take the spatial range query, one kind of LBS that we will focus in this paper, as an example. 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, i.e., the query point. As illustrated in 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. While LBS are popular 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. 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 below.

2. LITERATURE REVIEW

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.

3. PROBLEM OF STATEMENT

- 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.

4. ALGORITHMS USED IN DATA MINING DOMAIN

Attack Models

Similar to most previous works on outsourced data query,the cloud is assumed honest but curious and considered as thepotential attacker in this work. That is, the cloud would honestly

Store and search data as requested; however, the cloud wouldalso have financial incentives to learn those stored LBS dataand user location data in query. Because both LBS data anduser location data are valuable, they should be protected andhidden from the cloud. In general, in the outsourced LBS setting,the cloud can observe both queries from LBS users andencrypted LBS data from the LBS provider, which could be anadvantage to learn user locations. Therefore, assuming differentabilities of the attacker, there are mainly four attack models inoutsourced LBS setting.

Setup Algorithm

The setup algorithm is a probabilistic algorithm, which takesa security parameter λ, the attribute/predicate vector length t,and an inner product range [τ1, τ2] as input. The algorithm Outputs an attribute encryption key AK = (α, β, d,M), a predicateencryption key PK = (d,M), and a public parameter PP =((G1,G2, g, p, e), (Ωk)τ2k=τ1).α, β ∈Fpare two random numbers for encoding functions.dis a positive integer, and its value depends on the securityparameter. The scheme is more secure if d is bigger. dcouldbe 2, or d is an integer satisfying GCD(d, p − 1) = 1. If d =2, α, β must be chosen to make sure that the intersection ofthe set {z : z = −z1 − 2β/α mod p, τ1 ≤ z1 ≤ τ2} and the setS − [τ1, τ2] is empty. Here, S be the set of all possible values of Inner products.M is an n × n random invertible matrix over thefield Fp. n is the length of encoded attribute/predicate vectors.(G1, G2, g, p, e) is the pairing parameter generated by runningGen (λ), and Ωk= Hash (e(g, g)(α×perm(k)+β)d). Here,Hash() is a hash function and perm() is a random bijectionmapping from [τ1, τ2] to [τ1, τ2], i.e., a random permutationfunction. Let |Hash()| be the range size of Hash(). Hash() ischosen to make p |Hash()| τ2 − τ1.

Enc Algorithm

The algorithm of encrypting attribute vectors is a probabilistic algorithm, which takes an attribute vector−→**Vj**=(vj,1, vj,2, . . . , vj,t) and a random number sj∈Fpas input, andoutputs Cj= (cj,1, cj,2, . . . , cj,n+1) = ((gv__j,k)nk=1, e(g, g)sj).Here, (v__j,1, v__j,2, . . . , v__j,n)T = M−1(EncodeV (−→**Vj**, sj))T modp. T is the matrix transpose operator.

USER LEVEL ATTRIBUTE

A system model is the conceptual model as a result of system modeling 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.

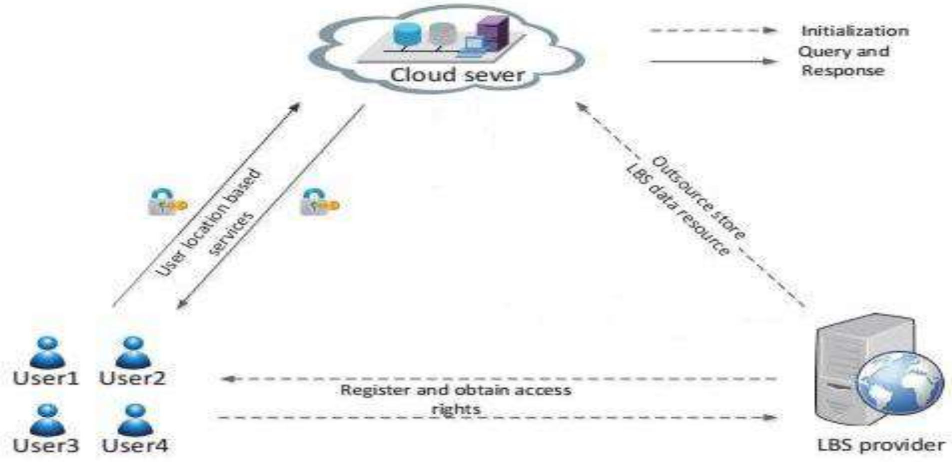

Fig 1.0

Fig1.0: 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.

ALGORITHM

Check Algorithm

The check algorithm takes a ciphertextCj= (cj,1, cj,2, . . . ,cj,n+1) of an attribute vector−→**Vj**and a token Ki =(qi,1, qi,2, . . . , qi,n+1) associated with a predicate vector−→**Ui**as input. The algorithm computes Ψ = _nk=1 e(cj,k,qi,k)cj,n+1×sj,n+1. IfHash(Ψ) is in the set {Ωk: τ1 ≤ k ≤ τ2}, the algorithm outputs1. Otherwise, it outputs 0.Remark 1: If two inner products are equal, their Ψ are thesame. This is not desirable for some applications. This problemcan be circumvented by adding randomness in the generation ofpredicate/attribute vectors. For a pair of fixed predicate vectorand attribute vector, the value Ψ is still fixed. However, givena pair of predicate and attribute, their vectors and their vectors’inner product all have multiple possible values. We willdemonstrate it in our EPLQ solution in Section V.Correctness proof . First, we prove Hash(Ψ) ∈ {Ωk:τ1 ≤ k ≤ τ2} if τ1 ≤ _−→**Ui**,−→**Vj**_ ≤ τ2. Recall that Ωk=Hash(e(g, g)(α×perm(k)+β)d). From the following equation,it is easy to find out that Hash(Ψ) ∈ {Ωk: τ1 ≤ k ≤ τ2} ifτ2 ≥ _−→**Ui**,−→**Vj**_ ≥ τ1:Ψ =_nk=1 e(cj,k, qi,k)cj,n+1 × sj,n+1=_nk=1 e(gu__i,k, gv__j,k)e(g, g)hi × e(g, g)sj=e(g, g)_nk=1 u__i,k×v__j,ke(g, g)hi+sj= e(g, g)EncodeU(−→**Ui**,hi)MM−1(EncodeV(−→**Vj**,sj))Te(g, g)hi+sj=e(g, g)_EncodeU (−→**Ui**,hi),EncodeV(−→**Vj**,sj)_e(g, g)hi+sj=e(g, g)(α×_−→**Ui**,−→**Vj**_+β)d+hi+sj e(g, g)hi+sj= e(g, g)(α×_−→**Ui**,−→**Vj**_+β)d.Second, we prove Hash(Ψ) /∈ {Ωk: τ1 ≤ k ≤ τ2} withoverwhelming probability if _−→**Ui**,−→**Vj**_ /∈[τ1, τ2].

Lemma 1: ∀a ∈Fp, a has at most one dth root ifGCD(d, p − 1) = 1 and p is a prime.

Proof: Clearly, if a = 0, it has only one dth root 0. Ifa _= 0, we prove the lemma by contradiction. If a had twoor more distinct dth roots, let χ1, χ2 ∈Fpbe two of them.

Since χd1= χd2= a, we have (χ1/χ2)d= 1. Noticing that Z∗pis a cyclic group of order p − 1, we have order(χ1/χ2)|d andorder(χ1/χ2)|(p − 1). So, order(χ1/χ2) is a common divisorof d and p − 1. Since χ1 and χ2 are distinct, we haveorder(χ1/χ2) _= 1. This contradicts with GCD(d, p − 1) = 1.Therefore, the assumption of a having two or more distinctsquare roots must be false.

Lemma 2: ∀a ∈Fp, a has at most two square roots if p is aprime.

Proof: Clearly, if a = 0, it has only one square root 0.

If a _= 0, we prove the lemma by contradiction.

5. PROPOSED METHODOLOGY

- 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.

ADVANTAGE 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.
- 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.

6. EXPRIMENTAL SETUP

.NET technology is both a programming language and a platform.

I. Active Server Pages.Net (ASP.Net (C#))

ASP.NET is a programming framework built on the common language runtime that can be used on a server to build powerful Web applications. ASP.NET offers several important advantages over previous Web development models:

- **Enhanced Performance.** ASP.NET is compiled common language runtime code running on the server. Unlike its interpreted predecessors, ASP.NET can take advantage of early binding, just-in-time compilation, native optimization, and caching services right out of the box. This amounts to dramatically better performance before you ever write a line of code.
- **World-Class Tool Support.** The ASP.NET framework is complemented by a rich toolbox and designer in the Visual Studio integrated development environment. WYSIWYG editing, drag-and-drop server controls, and automatic deployment are just a few of the features this powerful tool provides.
- **Power and Flexibility.** Because ASP.NET is based on the common language runtime, the power and flexibility of that entire platform is available to Web application developers. The .NET Framework class library, Messaging, and Data Access solutions are all seamlessly accessible from the Web. ASP.NET is also language-independent, so you can choose the language that best applies to your application or partition your application across many languages. Further, common language runtime interoperability guarantees that your existing investment in COM-based development is preserved when migrating to ASP.NET.
- **Simplicity.** ASP.NET makes it easy to perform common tasks, from simple form submission and client authentication to deployment and site configuration. For example, the ASP.NET page framework allows you to build user interfaces that cleanly separate application logic from presentation code and to handle events in a simple, Visual Basic - like forms processing model. Additionally, the common language runtime simplifies development, with managed code services such as automatic reference counting and garbage collection.
- **Manageability.** ASP.NET employs a text-based, hierarchical configuration system, which simplifies applying settings to your server environment and Web applications. Because configuration information is stored as plain text, new settings may be applied without the aid of local administration tools. This "zero local administration" philosophy extends to deploying ASP.NET Framework applications as well. An ASP.NET Framework application is

deployed to a server simply by copying the necessary files to the server. No server restart is required, even to deploy or replace running compiled code.

- **Scalability and Availability.** ASP.NET has been designed with scalability in mind, with features specifically tailored to improve performance in clustered and multiprocessor environments. Further, processes are closely monitored and managed by the ASP.NET runtime, so that if one misbehaves (leaks, deadlocks), a new process can be created in its place, which helps keep your application constantly available to handle requests.
- **Customizability and Extensibility.** ASP.NET delivers a well-factored architecture that allows developers to "plug-in" their code at the appropriate level. In fact, it is possible to extend or replace any subcomponent of the ASP.NET runtime with your own custom-written component. Implementing custom authentication or state services has never been easier.
- **Security.** With built in Windows authentication and per-application configuration, you can be assured that your applications are secure.

LANGUAGE SUPPORT

The Microsoft .NET Platform currently offers built-in support for three languages: C#, Visual Basic, and Java Script.

II)SQL Server:

The OLAP Services feature available in SQL Server version is now called SQL Server 2013 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version is now called Microsoft SQL Server 2013 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services SQL-SERVER database consist of six type of objects,

They are,

1. TABLE
2. QUERY
3. FORM
4. REPORT
5. MACRO

TABLE: A database is a collection of data about a specific topic.

VIEWS OF TABLE: We can work with a table in two types,

1. Design View
2. Datasheet View

Design View

To build or modify the structure of a table we work in the table design view. We can specify what kind of data will be hold.

Datasheet View

To add, edit or analyses the data itself we work in tables datasheet view mode.

QUERY:

A query is a question that has to be asked the data. Access gathers data that answers the question from one or more table. The data that make up the answer is either dynaset (if you edit it) or a snapshot (it cannot be edited).Each time we run query, we get latest information in the dynaset. Access either displays the dynaset or snapshot for us to view or perform an action on it, such as deleting or updating.

TABLE STRUCTURE

Database design is a collection of interactive data store. It is an effective method of defining, storing and retrieving the information in the database. Multiple application and users can use the data contained in the database. It prevents fraudulent and unauthorized users from accessing data and ensures the privacy of data.

The ERD to relational scheme mapping is done in order to make the most efficient use of table space. The relations of the scheme are converted into table and key attributes are converted into primary keys. The various tables that are used in the system are derived from the Entity Relationship Diagram. The tables are maintained are developer table and mining table.

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.

[11] A. Guttman, “R-trees: A dynamic index structure for spatial searching,” in Proc. Annu. Meeting (SIGMOD’84), Boston, MA, USA, Jun. 18–21, 1984, pp. 47–57.

[12] T. K. Dang, J. Küng, and R. Wagner, “The sh-tree: A super hybrid index structure for multidimensional data,” in Proc. 12th Int. Conf. Database Expert Syst. Appl. (DEXA’ 01), Munich, Germany, Sep. 3–5, 2001, pp. 340–349.

[13] B.-Y. Yang and J.-M. Chen, “All in the XL family: Theory and practice,” in Proc. Int. Conf. Inf. Secur. Cryptol, 2004, pp. 67–86.