EPLQ: Efficient Privacy-Preserving Location-based Query over Outsourced Encrypted Data

M. Vani, Dr. Y. Rama Mohan

Abstract— With the unavoidability of PDAs, location-based services (LBS) have received great attention and turn out increasingly dominant and indispensable delayed. In any case, the use of LBS also poses a potential threat to the security of the customer area. In this paper, which refers to a request for spatial classification, the standard LBS system, which provides information on the individual POIs (Points of Interest), we offer a game plan based on the creation range and the protected area security called EPLQ. Location-based Service (LBS) has recently had an impact on the rapid improvement of mobile phones, as well as the bottom-up perspective of distributed processing. Closed due to LBS development issues, and customer insurance is becoming a significant issue. Therefore, productive LBS economies must be safe and deliver accurate results. To guarantee the protection of the request for spatial range request, we propose in particular the main encryption structure of the main internal extension base, which can be used to find out whether the position is in a specific circular zone in the form of security. To minimize inactivity, we organize the EPLQ Security Tree structure. Point security checks confirm EPLQ security features. The in-depth tests are carried out in the same way, and the results show that EPLQ is extremely productive for the protection of spatial activity, for which coded information on allocation is required. Especially for a small LBS client using an Android phone, the question arises for 0.9 seconds. That's why a product workstation is necessary, and our cloud activity will take two to three minutes to understand POIs in our investigations.

Keywords: Location-based Service (LBS), Personal Digital Assistant (PDAs), Point of Interest (POI)

1. INTRODUCTION

Since from few decades LBS were used in military areas several new types of LBS systems have emerged, which are especially useful not only for communications but also for persons. We need to include the demand for space organization, the type of LBS system are going to address, for example. The issue of spatial range requests the LBS system, which is commonly used to allow the client to search for points of interest in the proposed part for their region, i.e., the reference point. As described in Figure 1. A customer with this type of geolocation system can retrieve the entire walkthrough restaurant archive. During this time, the customer can find this information to find a charming restaurant, taking into account costs and corrections. Although zone-based areas are undeniable and urgent, most of these organizations, including spatial rankings, require customers to display their domain as a real problem with distribution and misuse.

Data from the client's territory. Referring to this, hooligans can use this data to address abuse and to target their territories. For another model, a pair of sensitive data for the associated regions may include commercial secrecy or national security. Securing the safety of the LBS client area has caused great intrigues. Regardless of the enormous problems that remain in the LBS security structure, new issues arise, in particular by redistributing information. If we start too late, there is a case where information, including LBS information, is reallocated from your budget and operational contact points. Intelligent design security, at the crossroads of multifaceted preparation and scattered characters, protect faces from recurring spatial issues. Regional information where multifunctional customers are embedded in location services is a significant issue, at least very problematic and, of course, unresolved. Local data must be protected against unauthorized purchases, not only for customers but also for energy links that check and process area information, without prejudice to the assessment of the structure. In the old days, LBS is only used for military applications that are used today in many areas that cause various problems, such as guilty meetings found when people use data Look for your districts. It is used in the same way, for mechanical reasons, because it contains essential information about the community and contains regional-oriented events.

Figure 1. Illustration of Spatial range Query

Revised Manuscript Received on March 10, 2019.

M. Vani, M. Tech Student, G.Pulla Reddy Engineering College, Kurnool, AP, India.(E-mail: vani.chari473@gmail.com)

Dr. Y. Rama Mohan, Associate professor, Department of CSE, G.Pulla Reddy Engineering College, Kurnool, India.(E-mail: yrmgprec@gmail.com)

2. CHALLENGES

2.1 Challenge on querying encrypted LBS data

The LBS provider does not want to disclose your LBS critical data to the cloud. As defined by the LBS provider, private LBS data is encrypted and assigned to the cloud. Also, LBS customers need mixed data in the cloud. As a result, mixed LBS data processing without stopping security is a significant test. Not only do we need to protect the LBS provider and cloud client areas, but we also need to get more LBS data from the cloud.

2.2 Challenge on resource consumption in mobile devices

Various LBS customers are versatile customers, and their terminals are propelled cells with uncommonly compelled resources. In any case, the cryptographic or security enhancement frameworks used to recognize the security issue usually result in high computational costs or conceivably accumulating charges on the customer side.

2.3 Challenge on the efficiency of POI searching

The spatial extension request is an online organization, and LBS customers are sensitive to address dormancy. To give customers exceptional experience, the POI's interest in cloud computing needs to be implemented quickly. Again, techniques for recognizing security techniques require increased attention in delays. So far it is possible to carry out the necessary preparation tasks for LBS. In this approach, all customers have a common responsibility. In this respect, it is suitable for close customer groups where everyone has confidence. Possible level to solve outstanding LBS security problem and guarantee customizable client territory data, even against cruel authors' associations in events and territories. Provides a small "weak" explanation; It is not an unprecedented game plan and cannot offer perfect action. The authors turn around for reuse of spatial data sets. This is to maintain customer support represented by the data owner, even if the authorization association cannot be trusted. A system that protects the region against unauthorized people offers experienced customers the opportunity to look for spatial issues addressed by the professional community. For the data set Q, the data owner Q assigns a set of other Q0 points with a secret key. The owner of Q0 data exchange sends the best access to approved customers through a secure channel from an expert association. Since the main center does not know the key.

3. SYSTEM STUDY

3.1 Proposed System

A novel predicate-just encryption plot designed for internal thing run named IPRE, which states that the interior result of two vectors is within a certain range without revealing vectors. Predictive encryption key to the predicate, f, can decrypt the content of the image, if and only if the image content x matches typically the predicate, for example, f (x) = 1 predicate - encryption is just an unusual predicate encryption method for encrypting/decrypting messages. Or, on the other hand, perhaps discover whether f (x) = 1 or not. It was suggested that conventional predicate coding structures that support unique types of predicates [7] [8] require security savings in re-allocated information. To better understand, no agreement/predicate supports internal implementation. Regardless of how our scheme is used for the space-saving security claimed in this paper, it can also be associated with a variety of applications. EPLQ, the expert's answer to maintaining the security of the space range, asks. Specifically, we show that if a POI organizes a spatial order or cannot try it by observing the internal nature of two vectors, it is within a certain range. Both vectors contain data from the POI area and the demand freely. Based on this information and our IPRE plot, it is possible to create the required spatial range without spilling surface. To deny the isolation of all Points of Interest (POIs) to stimulate Points of Interest (POIs), we try to create a new registration structure called ssˆ - tree that covers sensitive area data with our IPRE plan. Our basics of implementation show that our response is exceptionally fruitful. Likewise, the security test shows that EPLQ is safe by referring to point-to-point attacks and content to talk about ambushes. Our methods may use multiple types of security registration requests for re-registered information. In the spatial field required by this article, we are thinking of the Euclidean schedule, which is widely used in spatial databases. Our IPRE Imagine, and s-tree can also be used to help recordings in a specific weighted Euclidean separation or emergency buoy. The weighted empty Euclidean serves to test the qualification in various forms of information, while the circle releases a unit of two symbols outside the circle. Exact is the excellent separation of the exception, rather than the termination of the Euclidean into long segments outside the Earth. By supporting these two types of separation, approval that guarantees proximity and spatial demand with a wide range can be understood in the same way.

3.2 Models and Design Goal

Protection safeguarding The POI issue was tested in two LBS configurations: open LBS and redistributed LBS. In this paper, we based on the last setting. In the above configuration, there is a LBS provider that has a spatial database of IP records in plain text, and LBS clients ask for the site of the POI provider. In the corresponding LBS as shown in Figure 2, the system includes three types of substances: LBS provider, LBS clients and cloud. The LBS Provider does not have a LBS information restriction, it is a list of places of interest. LBS service provider pieces include customers who use their information through a domain request. Due to the good operating conditions and resources arising from the redistribution of information, the LBS provider offers application administration via the cloud. In any case, the LBS provider does not want to find the LBS information available in the cloud. In this way, the LBS provider encrypts LBS information and redistributes it to the cloud.

LBS-Consideration

Cloud is a precious resource and management resource. It stores the encrypted LBS data from the LBS provider and also provides a list of LBS customers. Therefore, the cloud needs to check IP registration in a neighboring group to find

those who organize the interests of LBS customers. LBS customers have information from their districts as well as encrypted records of the points of interest in the cloud. Cryptography or reactivation of security frames is usually used to cover information about the area that is sent to the cloud. To convert encrypted records from the cloud, LBS clients must first receive the decryption key from the LBS provider.

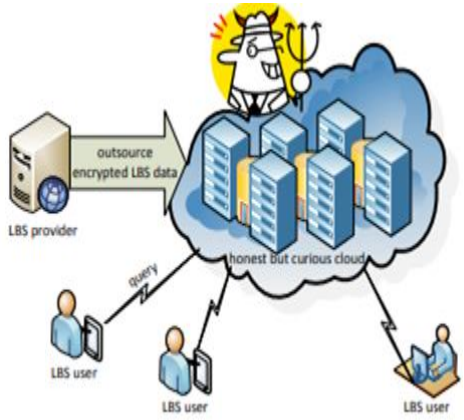


Figure 2. System Model of Outsources LBS under Consideration

Attack Models

As with most of the previous data, the demand for data is visible, the cloud is, in any case, verifiable, yet curious and considered a potential aggressor for this work. In other words, the cloud stores and retrieves the requested information, regardless of whether it has or has no money to receive client LBS information and area information upon request. Since data from both LBS networks is also essential, the data in the client section is essential. They must be related to avoiding the cloud. In the revised LBS configuration, everything that was taken into account can satisfy both the LBS client requirements and the LBS coded LBS information, which could be an emergency to find out the regions of clients. In this line, which supports different fracture points for the attacker, the transmitted LBS configuration usually has four fall patterns.

• Essentially cheat code content. In this model, the attacker is equipped to take account of area numbers and POI issues, at least not knowing the weaknesses. It is clear that every cloud has a farthest point. It's a fragile trap show.

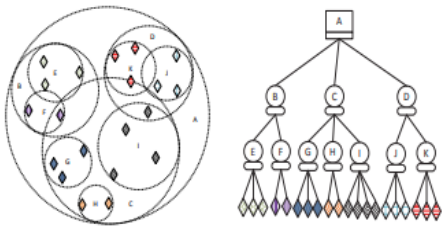
• Demonstration of a known box. In this model, the malicious person knows two or three POIs' domain errors and asks questions. The assailant also understands that his related character writings must have all the characters the attacker has seen. In any case, an attacker is unaware of the image content associated with a known raw text. Using such data, an attacker can find simple version related to image content. It is not difficult to obtain such data if the attacker assumes that the LBS database must identify the POIs in a specific room.

Overview

The IPRE conspire allows you to process the internal elements and the contrast of their properties and offers pre-defined protection. As far as we know, our table is an essential coding element for an internal object only. In the case of IPRE, both properties and predicates are vectors. That's why we use attribute and predicate vectors to incorporate features and predicates into the IEEE. Let $\Lambda \subseteq Z$ t p is the series of registered characters and z $\subseteq Z$ t p is the prediction class of IPRE. p is a significant bonus here. IPRE licenses verify that the vector's internal effects and vector z are in a predefined extension without revealing vectors. IPRE conversion is just a symmetric predicate encryption scheme and contains four accounts: configuration estimation to create an open parameter P, AK property encryption key and PK prediction encryption key; Calculation of calculations to mix credit vectors for writing; GenToken rating for mixing predictive vectors in tokens; Check the rating to see if the image content property matches the predicate of the marker.

Table 1. Notations used in IPRE and EPLQ

Notation	Description
$\langle , \rangle$	inner product operator
α, β	two secret numbers in $\mathbb{F}_p$
$[\tau_1, \tau_2]$	an inner product range
AK	the key to encrypt attribute vectors
C_j	the ciphertext of the j-th attribute vector
d	a positive integer
$e(.,.)$	a non-degradable bilinear mapping
g	a generator of $\mathbb{G}_1$
$\mathbb{G}_1$	a cyclic group of order p
$\mathbb{G}_2$	a cyclic group of order p
K_i	the i-th token
n	the length of encoded vectors
M	a secret $n \times n$ invertible matrix over the Field $\mathbb{F}_p$.
N	the number of POIs in the LBS database
p	a big prime
PK	the key to encrypt predicate vectors (i.e. the key to generate tokens)
PP	the public parameter of IPRE
R	the number of matched POIs
r_i	the radius of the i-th query area
S	the set of all inner products' values
t	the length of attribute/predicate vector
T	matrix transpose operator
$\overrightarrow{U_i}$	the i-th predicate vector $\overrightarrow{U_i} = (u_{i,1}, u_{i,2}, ..., u_{i,t})$
$\overrightarrow{V_j}$	the j-the attribute vector $\overrightarrow{V_j} = (v_{j,1}, v_{j,2}, ..., v_{j,t})$
(x_i, y_i)	the coordinates of the i-th query area's centroid



(a) POI distribution (b) ss-tree and $\hat{ss}$-tree structure

Fig. 3: Index POIs with ss-tree and $\hat{ss}$-tree

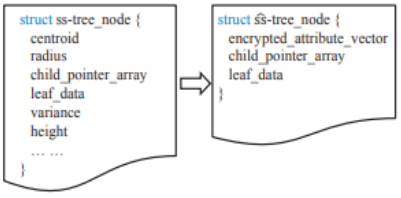


Fig. 4: The data structures of ss-tree node and $\hat{ss}$-tree node

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

4. ALGORITHM USED

Algorithm 1 Search_$\hat{ss}$-tree(node nd, query_tokens Ks, node_list ndl)

```
\\ nd: the node to be searched
\\ Ks: the array of two tokens associated with the query's predicate vectors. Ks[0] is the token for POI matching detection, while Ks[1] is the one for detecting intersection of circular areas.
\\ ndl: the list to store matched leaf nodes

C ← nd.encrypted_attribute_vector
if nd is a leaf node then
    if Check(Ks[0], C) == 1 then
        \\ nd's record matches the q's area
        Add nd to node_list ndl.
    end if
else
    if Check(Ks[0], C) == 1 then
        \\ nd's area intersects with the q's area
        for each child node cld_i of nd do
            Search_ŝs-tree(cld_i, Ks, ndl)
        end for
    end if
end if
```

5. SECURITY ANALYSIS & RESULT

We analyze the security features of the Code of Conduct proposed by EPLQ. In particular, according to the previously assessed security requirements, our assessment will focus on how EPLQ's line of business is in line with the LBS information plan and the security of the customer region. The LBS Information Game Plan complements not only the progress of points of interest but also the confidentiality of area data in the trees. Of course, the security of the client's local configuration is unified to guarantee the area's sensitive data on the client's issues and the ssˆ - tree. EPLQ game plan security is based on standard encryption scheme and IPRE frame. The conventional coding system can protect the cloud against POI records, while our IPRE system is responsible for connecting the client area and the cloud POI. The current AES standard can be used as a standard operation and is secure against known and known untreated and coded text attacks. That's why we focus on Customer's land claim/interest point using the IPRE plot.

6. CONCLUSION

In this paper, we proposed EPLQ, which provides privacy preserving for spatial range request with respect to the customer location and provides security for the location-based information. To realize EPLQ, we have designed an IPRE and a novel privacy-preserving index tree named ssˆ -tree. The availability of EPLQ has been studied with theoretical and different separates and speedy.

The investigation shows privacy against attacks on known landmarks and attacks with coded text only. Our technique can be used for various types of security requests. The low probability that a request can be made using internal elements resulting from guaranteed performance could be attributed to IPRE and the proposed ssˆ - tree by understanding the demand for security savings. Two possible applications are security, proximity protection, and long distance demand. In the future, we will develop responses to these situations and see more services

REFERENCES

1. A. Gutscher, "Facilitate change - an answer for the protection issue of area-based administrations?" in twentieth International Parallel and Distributed Processing Symposium (IPDPS 2006), Proceedings, 25-29 April 2006, Rhodes Island, Greece, 2006. [Online]. Accessible: http://dx.doi.org/10.1109/IPDPS.2006.1639681
2. W. K. Wong, D. W.- l. Cheung, B. Kao, and N. Mamoulis, "Secure knn calculation on scrambled databases," in SIGMOD. ACM, 2009, pp. 139– 152.
3. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.- L. Tan, "Private inquiries in area based administrations: anonymizers are redundant," in SIGMOD. ACM, 2008, pp. 121– 132.
4. X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Functional k closest neighbor questions with area security," in ICDE. IEEE, 2014, pp. 640– 651.
5. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private data recovery," Journal of the ACM (JACM), vol. 45, no. 6, pp. 965– 981, 1998.
6. F. Olumofin and I. Goldberg, "Returning to the computational common sense of private data recovery," in Financial Cryptography and Data Security. Springer, 2012, pp. 158– 172.
7. J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial conditions, and inward products," in Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Procedures, 2008, pp. 146– 162. [Online]. Accessible: http://dx.doi.org/10.1007/978-3-540-78967-3 9
8. D. Boneh and B. Waters, "Conjunctive, subset, and range inquiries on encoded information," in Theory of Cryptography, fourth Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings, 2007, pp. 535– 554. [Online]. Accessible: http://dx.doi.org/10.1007/978-3-540-70936-7 29
9. D. Boneh and M. K. Franklin, "Character based encryption from the weil blending," SIAM J. Comput., vol. 32, no. 3, pp. 586– 615, 2003. [Online]. Accessible: http://dx.doi.org/10.1137/S0097539701398521
10. D. A. White and R. Jain, "Comparability ordering with the ss-tree," in ICDE. IEEE, 1996, pp. 516– 523.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication