EFFICIENTLY PRESERVING THE OUTSOURCED ENCRYPTED DATA USING LBS

[1]G.B.PAVITHASRI [2]A.M.VAISHNAVI [3] K.MAHIMAA VIJAYASARMI [4] G. RAJARAJAN

[1,2,3] B.E (CSE), Anjalai Ammal Mahalingam Engineering College, Kovilvenni.

[4] Assistant Professor, Department of CSE, Anjalai Ammal Mahalingam Engineering College, Kovilvenni.

Email: g.b.pavithasri@gmail.com

Abstract: Now a days, most of the people are has to hide or modify their original location from unauthorized user. This means they want to have their privacy. In the paper we are aiming the query, LBS information about POI's. With this efficiently preserving the outsourced encrypted data using LBS is called EPEL. Majorly, to achieve privacy we focus on spatial range query, with by encrypting with inner product range within that circular port the privacy will act. With respect to the index tree we used to reduce the latency security has be demonstrated in the result of EPEL. With respect to the web application, around 0.9second is needed to generate a query with respect to the workstation. This will takes few seconds to search POI's

Index Terms: Location Based Service, Privacy Preserving Technology, Spatial Range Query, Outsourced Encrypted Data.

I. INTRODUCTION

As Before, Location-based services (LBS) were used in Military, Airlines etc. Now days it was commonly used for safety purpose with each individuals. With respect to the spatial range query we use one kind of LBS. This POI's (Point of Interest) is focused within a given distance to his/her location. As in Fig.1, With that they come know the near important place that is in walking distance. Using this they can also view record and reviews. The LBS was the popular and plays a vital role in Environment .In this, user have to submit their location, but Now, Most of the data's are misused by other user they are considered to be as an unauthorized user . For example, the person A is going Australia and A is plan to various places but a wants to have to private his location for that they use to have LBS, POI and spatial range query with that security want to search the nearest important place. But in the part the major challenge's has to focus. Because, the data are outsourced in the large environment. Therefore, the major challenges are:

- Challenge on query encryption: The LBS provider is not willing to accept the value of LBS data to the cloud. As shown in Fig.2, Thus LBS providers encrypt and outsource private LBS data. By that time, querying encrypted LBS data without privacy breach is the big challenge.
- Challenge on resource capacity: They use computer Laptop, Mobile as a terminates. With that cryptographic or privacy preserving technology to realize the result with high computational and storage cost for user side.
- Challenge on the efficient search POI's: Spatial ranges on queries are online services, the LBS used to proceed with query latency. This POI search performing at the cloud side must have to be in short span of time is

the major challenge to reduce query latency.

- Challenge on security: Security is the major one because LBS is about the POIs in real world. Because, it is most common that the attacker can have some knowledge about original LBS data. This Known sample attack [elaborate later in].

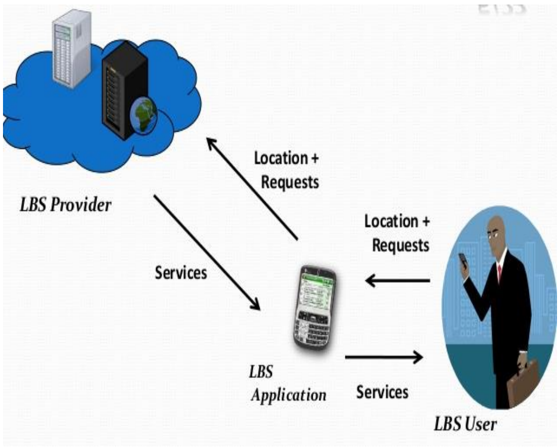
The above challenges that are faced by our existing system. (i.e.). For our proposed system, we have overcome the security, storage. This was the major goal was faced by the EPEL .By this, to improve the performance, the privacy preserving index structure. Encryption can be processed with using inner product range [IPRE]. The major contributions are as follows:

- First, we propose to have predicate only encryption scheme for inner product range [IPRE]. This used to check whether it is within the range. This process is not meaning that for encryption and decryption. Suppose if predicate f decrypt the cipher text x , i.e., f(x)=1. But this type of scheme is used for the outsourced data by supporting IPRE.
- Secondly, we propose EPEL, this EPEL is a efficiently preserving the outsourced encrypted data using LBS. this majorly focuses on the concept of POIs. With respect to the spatial range query the process get started. In that we use encryption technique as IPRE with that we can avoid unauthorized user. This takes a few times to search POIs with their related information.
- Third, the major goal of this paper is to reduce the latency with that spatial range query it has to be defined with respect to both circular and also with the index term. This circular way will take more time to search the POIs. Whereas, this index terms used to search POIs by level by level this use to have the parallel way on process. So this will reduce the latency.

II. MODEL AND DESIGN GOAL

In this section, the coverage are system model, attack model and design goal.

A. SYSTEM MODEL



The major components are LBS user and LBS provider. The LBS user used to outsource their location data and also used to request for their security to encrypt their information. With using LBS provider used to accept their request with respect to their setting it will perform task. But the following functions are commonly accessible by the LBS provider with their application. Their LBS user used to request and response for the performance. The POIs will majorly access in the LBS user side. The database is managed by the LBS provider.

B. ATTACK MODEL:

The attack model work on outsourced data query, in that the data are honest but curios for the potential attacker to work. If the user is searching the data from one place for other person that person accept their request with their permission they can access the original data otherwise they will receive the encrypted data. The list of attack models are.

- Cipher text-only attack: This model used to attacker by fetching the cipher text of POI's
  Locations and queries. So that they don't know there plaintext. So, this is considered to be an weak attack model.
- Known-sample attack: In this the attacker would able to know their plaintext and also know the cipher text but the attacker doesn't known the related matched cipher text for the plaintext. By using the database the certain area will focuses on the place were both plaintext and cipher text is stored.
- Known-plaintext attack: The attacker knows the plaintext but the corresponding ciphertext is unpredictable. By utilizing this plaintext they can have the corresponding ciphertext.
- Access-pattern attack: In this attackers have some knowledge about the pattern of POIs that means if the Pois is most popular one then the attacker can easily identify the known POI. Therefore, this could be more hard to identify.

The above s are most commonly used but the known-sample attack and cipher text only attacks are commonly used by attacker.

C. DESIGN GOAL:

Our outsourced LBS system model has the design goal to improve the efficiency, security, accuracy with that privacy preserving on spatial range query. The three objectives are as follows.

- Efficiency: The users have to be in online for to improve their performance while on registering. The POI search has to reduce latency for acceptable period on time.
- Accuracy: The query should have the exact match with the plain text and cipher text. Their if it have false negative then the values are not acceptable. False positive then it move to the additional computation cost from the user side.
- Security: The proposed system is not focusing on the known sample attack and known cipher text attack. Because attacks are more commonly used in the database. But now our proposed system is focused to proceed with having this out sourced data for processing using the LBS.

III. IPRE: INNER PRODUCT RANGE ENCRYPTION

In this section, we are going to see about the encryption technique named as IPRE this used to give the solution for the EPEL for privacy on spatial range query.

A. OVERVIEW:

In proposed system the IPRE scheme is used to compute the inner product and the values that are in the predefined range in a privacy-preserving way. This can used both predicate/predicate-only encryption scheme for IPRE. In this attribute and predicates are vectors. (i.e.) It is a attribute vector and predicate vector to refer in IPRE. Let Λ ⊆ Zt p be the attribute set and F ⊆ Zt p be the class of predicates. This allow testing if inner product of vector from A and vector from F. This used three common algorithms for process. They are **Setup Algorithm**: For the generate public parameter pp. **Gen token**: For the predicate vector to token. **Enc Algorithm**: Attribute vector to ciphertext.

B. ENCODING ATTRIBUTE VECTOR AND PREDICATE VECTOR:

Before encrypting the paper using IPRE. We used to encode the process with the attribute vector and predicate vectors. This use Encode u() and Encode v() for that separately

C. SETUP ALGORITHM

The setup algorithm is the probabilistic way for the security purpose with the parameter λ length t, inner product range [τ1, τ2]. The attribute encryption key AK= (α, β, d, M), a predicate encryption key PK=(d, M) as public parameter PP= ((G1,G2,g,p,e),(Ωk)τ2 k=τ1).

A. Computational Cost at user side:

D. ENC ALGORITHM:

This is also an probabilistic way to which takes Vj = (vj,1,vj,2,...vj,t) and random number sj ∈ Fp as input.

E. GENTOKEN ALGORITHM:

It is also an probabilistic algorithm, this takes a predicate vector Ui = (ui,1,ui,2,...ui,t) and a random number hi ∈ Fp as input.

IV EPEL: PROPOSED SOLUTION FOR PRIVACY

In this section, this use the major concept of tree data structure name as SS-tree.

A. Preliminary SS-tree:

The SS-tree was already used in our existing system. In that they have used some spatial range on query with by having the point circular are as, rectangular area, single dimension ranges etc., To approve this IPRE scheme we have to focus on SS-tree at the same time. This was naturally applied in IPRE to these data structure for privacy-preserving query.

B. Proposed SS-tree:

The past SS-tree will give the EPEL solution. The each tree will hides the location information using our predicate-only encryption scheme, and removes unnecessary information. Because of encryption, detecting circular area intersection and matched records are also different in matched record on a tree.

To generate a query with respect to the LBS user. With that, the user used to query to the LBS provider there it use to search the POIs within0.9 seconds this performance the latency . so in this paper we are decided to reduce the latency and to extend the storage capacity to process the data.

B. LBS Provider Computational cost :

During this system setup, the LBS provider used to get the information from the LBS user. The information that is stored in the LBS provider side. This information are encrypted and partially store under it. The LBS provider used to manage private database for access to information.

C. Cloud’s Computational Cost:

Generally, cloud is the common term for process. This intermediately acces the information from LBS user to LBS provider. Because, with the web application this will processed. By this time we can also reduce the query latency.

D. Accuracy:

The user query should match the data present in the record. For the security purpose this also have to match the ciphertext to have support from the unauthorized user.

CONCLUSION:

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. 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 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.

REFERENCE:

- W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, “Secure knn computation on encrypted databases,” in SIGMOD. ACM, 2009, pp. 139–152.

- G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location based services: anonymizers are not necessary,” in SIGMOD. ACM, 2008, pp. 121–132.

- B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” Journal of the ACM (JACM), vol. 45, no. 6, pp. 965–981, 1998.

- B. Yao, F. Li, and X. Xiao, “Secure nearest neighbor revisited,” in ICDE. IEEE, 2013, pp. 733–744

- Y. Elmehdwi, B. K. Samanthula, and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments, “in ICDE. IEEE, 2014, pp.664–675