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

M.Vani
G. Pulla Reddy Engineering college, kurnool, India
Corresponding author: M.Vani
G. Pulla Reddy Engineering college, kurnool, India

Abstract: - With the inescapability of PDAs, location-based administrations (LBS) have gotten extensive consideration and turn out to be progressively prevalent and indispensable as of late. Be that as it may, the utilization of LBS like-wise represents a potential danger to client's area security. In this paper, going for spatial range inquiry, a mainstream LBS giving data about POIs (Points Of Interest) inside a given separation, we present a productive and protection safeguarding area based inquiry arrangement, called EPLQ. Area based administration (LBS) is blasting up lately with the quick development of cell phones furthermore, the rising of distributed computing worldview. Alongside the difficulties to build up LBS and the client protection issue turns into the most vital concern. So fruitful protection saving LBS must be secure and give precise inquiry results. In particular, to accomplish privacy-preserving spatial range inquiry, we propose the first predicate only encryption plot for internal item extend, which can be used to recognize whether a position is inside a given round zone in a security safeguarding way. To lessen question inactivity, we further plan a security safeguarding tree file structure in EPLQ. Point by point security examination affirms the security properties of EPLQ. Likewise, broad tests are led, and the outcomes exhibit that EPLQ is exceptionally productive in privacy-preserving spatial range inquiry over re-appropriated encoded information. Specifically, for a portable LBS client utilizing an Android telephone, around 0.9 second is expected to create an inquiry; and it likewise as it were requires a product workstation, which assumes the job of the cloud in our tests, a couple of moments to look POIs.

INTRODUCTION:- A few decades back, territory based organizations (LBS) were used in military figuratively speaking. Today, by virtue of advances in information and correspondence advancements, more sorts of LBS have showed up, and they are especially useful for not simply affiliations yet furthermore individuals. We should take the spatial range request, one kind of LBS that we will focus on in this paper, for example. Spatial range question is a by and large used LBS, which empowers a customer to find POIs (Point Of Interests) inside an offered division to his/her region, i.e., the inquiry point. As delineated in Fig. 1, with this kind of LBS, a customer could procure the records of all restaurants inside walking division .By then the customer can encounter these records to find a charming diner considering cost and reviews. While zone based organizations are unmistakable and urgent, most of these organizations today including spatial range request require customers to show their territories, which raises veritable concerns about the spilling and mishandling of customer territory data. For point of reference, hooligans may utilize the data to pursue potential abused individuals and anticipate their zones. For another model, a couple sensitive region data of affiliation customers may incorporate trade riddle or national security. Guaranteeing the security of customer zone in LBS has pulled in broad interest. In any case gigantic challenges still remain in the structure of privacy-preserving LBS, and new troubles rise particularly due to data redistributing.

Starting late, there is a creating example of redistributing data including LBS data because of its budgetary in addition, operational points of interest. Lying at the intersection purpose of adaptable preparing and dispersed figuring, arranging security shielding re-appropriated spatial range question faces. Anchoring region information of versatile customers in Location Based Services is a basic anyway extremely troublesome and still, as it were, unsolved issue. Region information must be protected against unapproved get to not simply from customers yet also from authority associations securing and taking care of the region data, without restricting the value of the structure. In the times of yore LBS is used only for the military application yet today used for a few districts , it make various issues like the guilty parties may seek after any person to use the information to seek after their regions . It in like manner used for some mechanical reason that thy have some huge information about the firm that contain region focused advancement.

Fig. 1: An example of spatial range query

1) **Challenge on querying encrypted LBS data:-**

The LBS provider isn't willing to reveal its critical LBS data to the cloud. As laid out in the LBS provider scrambles and re-appropriates private LBS data to the cloud, additionally, LBS customers question the mixed data in the cloud. As a result, addressing mixed LBS data without security break is a noteworthy test, and we need to guarantee not simply the customer zones from the LBS provider and cloud, however what's more LBS data from the cloud.

2) **Challenge on the 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 enhancing frameworks used to recognize security protecting inquiry ordinarily result in high computational cost or conceivably accumulating cost at customer side.

3) **Challenge on the efficiency of POI searching:-**

Spatial expand request is an online organization, and LBS customers are sensitive to address dormancy. To give extraordinary customer experiences, the POI look for performing at the cloud side must be done in a brief time period Afresh, the techniques used to recognize security ensuring request regularly augment the interest latency.It look to how territory information can be rendered muddled so it is up 'til now possible to perform getting ready exercises required by LBS.in this approach all customers share one single change work, it is along these lines suitable for close customer clusters in which all people trust each .it is on a very basic level possible to deal with the noteworthy security issue of LBS and to guarantee the territory data of adaptable customers even against vindictive territory and event authority associations. it give a modestly 'weak' affirmation; it not an unrivaled game plan and it can't offer a perfect course of action . Authors revolves around the re-appropriating of spatial datasets. Point is to maintain the customer endorsement portrayed by the data

proprietor, despite when the authority association can't be trusted. The system that shield region information from un-authorizers, provide affirmed customers to look spatial inquiries that are addressing by the pro community. Given a set Q of data centers, the data proprietor maps Q to another point set Q0 using a change with a secret key. The data proprietor exchanges Q0 to the expert association and sends the best approach to affirmed customers through an ensured channel. Since the master center does not know the key.

PROPOSED SYSTEM: - a novel predicate-just encryption plot for internal thing run named IPRE, which grants testing whether the internal consequence of two vectors is inside a given range without divulging the vectors. In predicate encryption, the key identifying with a predicate, f, can unscramble a cipher text if and just if the characteristic of the cipher text, x, satisfies the predicate, i.e. f(x) = 1. Predicate-just encryption is an exceptional kind of predicate encryption not planned for encoding/unscrambling messages. Or maybe, it reveals that whether f(x) = 1 or not. Predicate-just encryption designs supporting one of a kind sorts of predicates [7], [8] have been proposed for insurance sparing request on re-appropriated data. To the best our understanding, there does not exist predicate/predicate only plan supporting interior thing run. In spite of the way that our plan is used for security sparing spatial range request in this paper, it may be associated in various applications as well. EPLQ, a capable response for security sparing spatial range request.

In particular, we

exhibit that whether a POI organizes a spatial range request or not can be attempted by taking a gander at whether the interior thing of two vectors is in a given range. The two vectors contain the territory information of the POI and the request independently. In light of this disclosure and our IPRE plot, spatial range request without spilling territory information can be cultivated. To refuse separating all POIs to find facilitated POIs, we further undertaking a novel document structure named ssˆ - tree, which covers delicate territory information with our IPRE plan. Preliminaries on our execution demonstrate that our answer is extraordinarily successful. Also, security examination shows that EPLQ is secure under referred to precedent attacks and cipher text-so to speak ambushes. our techniques can be used for more sorts of security sparing inquiries over redistributed data. In the spatial range request analyzed in this work, we consider Euclidean partition, which is comprehensively used in spatial databases. Our IPRE contrive and ssˆ - tree may be used for glimpsing records inside a given weighted Euclidean detachment or unprecedented float expel moreover. Weighted Euclidean evacuate is used to check the distinction in various sorts of data, while mind boggling circle evacuate is the detachment of two on the surface of a circle. Using unprecedented circle separate as opposed to Euclidean detachment for long partitions on the surface of earth is logically exact. By supporting these two sorts of detachments, assurance defending closeness request and long spatial range question can in like manner be made sense of it.

MODELS AND DESIGN GOAL:- Protection safeguarding POI inquiry has been examined in two settings of LBS: open LBS and re-appropriated LBS. In this paper, we center around the last setting. In the previous setting, there is a LBS supplier holding a spatial database of POI records in

plaintext, and LBS clients question POIs at the supplier's site. In re-appropriated LBS, as appeared in Fig. 2, the framework comprises of three sorts of substances: LBS supplier, LBS clients and cloud. The LBS supplier has bottomless of LBS information, which are POI records. The LBS supplier permits approved clients to use its information through area based inquiries. As a result of the money related and operational advantages of information redistributing, the LBS supplier offers the question administrations through the cloud. Notwithstanding, the LBS supplier isn't willing to uncover the profitable LBS information to the cloud. Therefore, the LBS supplier encodes the LBS information, and redistributes the encoded information to the cloud.

LBS-Consideration -

The cloud has rich accumulating and handling resources. It stores the encoded LBS data from the LBS provider, in addition, gives question organizations to LBS customers. So the cloud requirements to glance through the encoded POI records in neighborhood amassing

to find the ones organizing the request from LBS customers. LBS customers have the information of their own regions, additionally, question the encoded records of near to POIs in the cloud. Cryptographic or security updating frameworks are typically used to disguise the territory information in the request sent to the cloud. To interpret the encoded records gotten from the cloud, LBS customers need to get the unscrambling key from the LBS provider early.

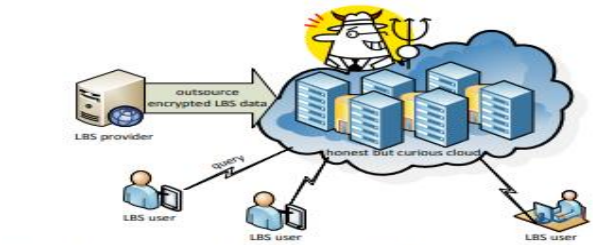


Fig. 2: System model of outsourced LBS under consideration

Attack Models:-Similar as most past wears down re-appropriated data question, the cloud is normal certifiable anyway curious and considered as the potential aggressor in this work. That is, the cloud would genuinely store and chase data as requested, in any case the cloud would in like manner have fiscal helpers to take in those set away LBS data and customer region data in request. Since the two LBS data additionally, customer region data are noteworthy, they should be anchored additionally, kept away from the cloud. All things considered, in the re-appropriated LBS setting, the cloud can watch the two request from LBS customers also, encoded LBS data from the LBS provider, which could be great position to learn customer territories. Thus, tolerating various limits of the attacker, there are generally four ambush models in outsourced LBS setting.

• Cipher text-simply ambush. In this model, the aggressor is skilled to watch the cipher texts of POIs' zones and questions, regardless, does not know the plaintexts. Obviously, every cloud has this limit. This is a weak ambush illustrate.

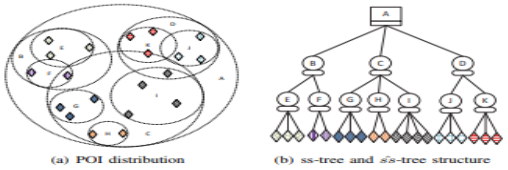
• Known-model ambush. In this model, the attacker knows the plaintexts of a couple of POIs' territories and furthermore request. The aggressor furthermore understands that their relating cipher texts must exist in all the cipher texts seen by the aggressor. Regardless, the assailant does not know which cipher text is identifying with a

known plaintext. Utilizing such information, the attacker may have the ability to reveal the plaintext identified with any given cipher text. Such information isn't hard to get if the aggressor has the establishment discovering that the LBS database must contain the POIs of explicit sort in an explicit domain.

Overview :-The proposed IPRE conspire permits processing inward items and contrasting their qualities and a predefined go in a security protecting way. Supposedly, our plan is the principal predicate/predicate-just encryption plot for internal item go. In IPRE, the two characteristics and predicates are vectors. So we use trait vectors and predicate vectors to allude to the traits and predicates in IPRE. Let Λ ⊆ Z t p be the characteristic set and z ⊆Z t p be the class of predicates in IPRE. p is a major prime here. IPRE permits testing if the inward result of a vector from Λ and a vector from z is in a predefined extend without revealing the vectors. IPRE conspire is a symmetric predicate-just encryption plan, and it comprises of four calculations: Setup calculation for creating an open parameter P, a property encryption key AK and a predicate encryption key PK; Enc calculation for scrambling credit vectors to cipher texts; GenToken calculation for scrambling predicate vectors to tokens; Check calculation for checking if a cipher text's property fulfills a token's predicate.

TABLE I: Notations frequently 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

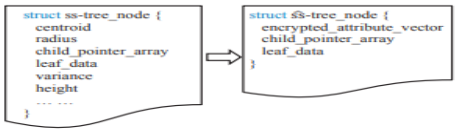


Fig. 4: The data structures of ss-tree node and $\hat{ss}$-tree node

Algorithm:-

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

```
1: \\ nd: the node to be searched
2: \\ 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.
3: \\ ndl: the list to store matched leaf nodes
4:
5: C ← nd.encrypted_attribute_vector
6: if nd is a leaf node then
7:     if Check(Ks[0], C) == 1 then
8:         \\ nd's record matches the q's area
9:         Add nd to node_list ndl.
10:    end if
11: else
12:    if Check(Ks[0], C) == 1 then
13:        \\ nd's area intersects with the q's area
14:        for each child node cld_i of nd do
15:            Search_ŝs-tree(cld_i, Ks, ndl)
16:        end for
17:    end if
18: end if
```

SECURITY ANALYSIS:-

we analyze the security properties of the proposed EPLQ game plan. Specifically, after the security requirements inspected previously, our examination will focus on how the proposed EPLQ game plan can achieve the LBS data arrangement and the customer's territory security. The arrangement of LBS data joins not simply the arrangement of POI records yet moreover the mystery of zone information in

ssˆ - tree. Of course, customer region security incorporates guaranteeing sensitive region information in customer questions and ssˆ - tree. The security of EPLQ course of action depends upon the essential standard encryption plan and IPRE plot. The standard encryption plot is able for shielding the cloud from learning POI records, while our IPRE plot is accountable for anchoring customer zone and POI region from the cloud. The current AES standard can be used as the standard arrangement, and it is secure under ciphertextonly, known-model and known-plaintext attacks. Thusly, we focus on the examination of customer/POI territory affirmation with IPRE plot.

CONCLUSION :- In this paper, we have proposed EPLQ, a profitable privacy preserving spatial range question respond in due order regarding propelled cell phones, which ensures the security of customer region, and achieves security of LBS data. To recognize EPLQ, we have arranged a novel predicate-just encryption plot for inner thing run named IPRE and a novel security ensuring record tree named ssˆ - tree. EPLQ's feasibility has been surveyed with speculative examination and breaks down, and quick and dirty examination exhibits its security against known-precedent attacks and ciphertext-just attacks. Our methodology have potential uses in various sorts of security sparing inquiries. If the inquiry can be performed through standing out internal things from ensured run, the proposed IPRE and ssˆ - tree may be associated with make sense of it security sparing inquiry. Two potential uses are privacy preserving closeness request and long spatial range question. In the future, we will design answers for these circumstances and perceive more employments.

REFERENCES:-

[1] A. Gutscher, "Coordinate transformation - a solution for the privacy problem of location based services?" in 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), Proceedings, 25-29 April 2006, Rhodes Island, Greece, 2006. [Online]. Available: http://dx.doi.org/10.1109/IPDPS.2006.1639681

[2] 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.

[3] 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.

[4] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, "Practical k nearest neighbor queries with location privacy," in ICDE. IEEE, 2014, pp. 640–651.

[5] 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.

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

[7] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner 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.

Proceedings, 2008, pp. 146–162. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-78967-3 9

[8] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings, 2007, pp. 535–554. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-70936-7 29

[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. [Online]. Available: http://dx.doi.org/10.1137/S00975397013985 21

[10] D. A. White and R. Jain, "Similarity indexing with the ss-tree," in ICDE. IEEE, 1996, pp. 516–523.