ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

EPLQ: Efficient Privacy Preserving Location based Query Over Outsourced Encrypted Data

Fasna kp

PG Scholar, Department of Computer Science and Engineering, CCET Engineering College, Kerala, India

ABSTRACT: Location-based service (LBS) is booming up in recent years with the rapid growth of mobile devices and the emerging of cloud computing paradigm. Along with the challenges to establish LBS and the user privacy issue becomes the most important concern. So successful privacy-preserving LBS must be secure and provide accurate query results. In this paper we present a solution to one of the location-based query problems that provide privacy for the user's location . This mainly focused spatial range query,. In this paper, aiming at spatial range LBS is giving the data about the interested area within a given boundary, here i present an efficient and privacy-preserving location based query solution (EPLQ) . This mainly look to provide privacy preserving spatial range query, it use the predicate only encryption scheme for inner product range, that can find out whether a position is within a given circular area in a privacy-preserving way or not. This use tree model structure(ss^tree) for minimize searching time.

KEYWORDS: Location-based Services, security-providing methods, Spatial Range Query, Outsourced Encrypted Data

I. INTRODUCTION

Protecting location information of mobile users in Location Based Services is a very important but quite difficult and still largely unsolved problem. Location information has to be protected against unauthorized access not only from users but also from service providers storing and processing the location data, without restricting the functionality of the system. In the old days LBS is used only for the military application but today used for many areas , it create many issues like the criminals may follow any person to use the information to follow their locations . It also used for som industrial purpose that thy have some valuable information about the firm that contain location trade secret . So protecting the location of users is most important one .This paper mainly discusses to the spatial range query.it faces many challenges like how to encrypt querying LBS information and how to get privacy etc. There are already some methods for spatial range query[1].

II. RELATED WORK

In [2] .authors used an approach based on coordinate transformations. It look to how location information can be rendered illegible in such a way that it is still possible to perform processing operations required by LBS.in this approach all users share one single transformation function, it is thus only suitable for closed user groups in which all members trust each .it is basically possible to solve the major privacy problem of LBS and to protect the location data of mobile users even against malicious location and event service providers. it give a relatively ‘weak’ protection; it not a better solution and it cannot offer a perfect solution . in [3] Authors focuses on the outsourcing of spatial datasets. Aim is to enforce the user authorization defined by the data owner, even when the service provider cannot be trusted. The method that protect location information from unauthorizers,provide authorized users to search spatial queries that are querying by the service provider. Given a set Q of data points, the data owner maps Q to another point set Q0 using a transformation with a secret key. The data owner uploads Q0 to the service provider and sends the key to authorized users through a secure channel. Since the service provider does not know the key. At query time, an authorized user maps a query X to another query X0 by using the key and then submits X0 to the service provider. Then service provider executes X0 against Q0 and returns the result R0 P0 to U, who uses the key to decode R0 and obtain the actual result R P. used an optimization function which considers nature of the packet, size of the packet and

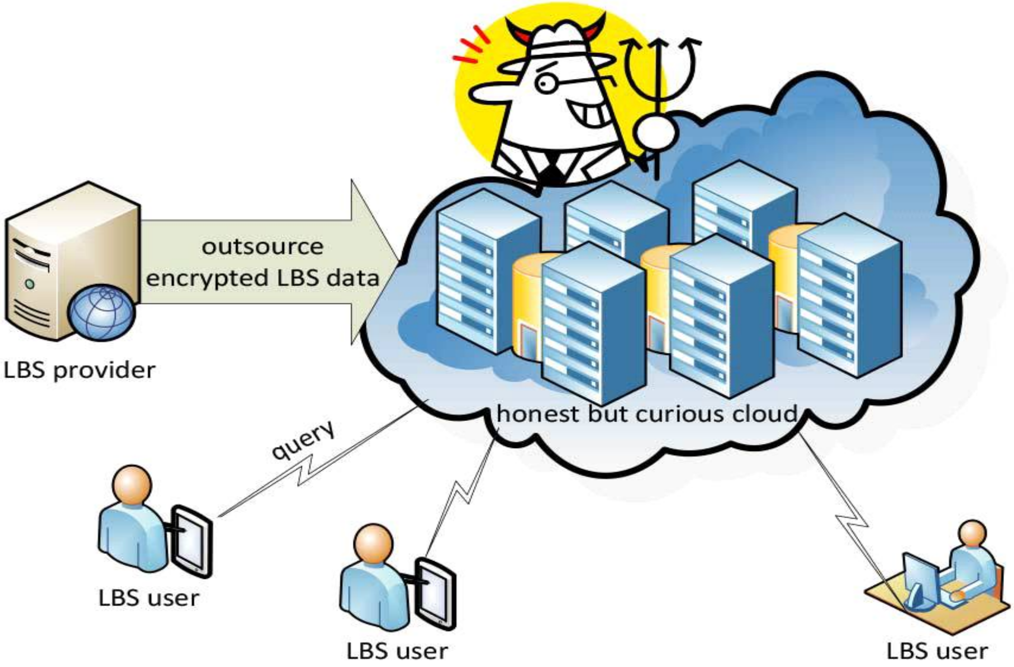
DOI: 10.15680/IJIRCCE.2017. 0503353

distance between the nodes, number of hops and transmission time are also considered for optimization. In [4]Author look to anonymous communication technique to protect the location privacy of people using LBSs. In our proposed technique, a user sends true position data with several false position data ('dummies') to a service provider, who creates a reply message for each received position data. The user simply extracts the necessary information from the reply message. In this manner, even if the service provider stores the set of position data, it cannot distinguish the true position data from the set of position data. To apply our anonymous communication technique in LBSs, the two important issues are; Realistic dummy movements , Reduction of communication cost. In[5]The author present Casper is new method in which mobile and stationary users can entertain location based services without revealing their location information. Casper consists of two main components, the location anonymizer and the privacy-aware query processor. The location anonymizer blurs the users' exact location information into cloaked spatial regions based on user specified privacy requirements. The privacy-aware query processor is embedded inside the location-based database server in order to deal with the cloaked spatial areas rather than the exact location information. Experimental results show that Casper achieves high quality location-based services while providing anonymity for both data and queries.. In [6] Authors introduce new method basing on coordinate transformations. it shows how location information can be rendered illegible in such a way that it is still possible to perform processing operations required by LBS.

III. PROPOSED ALGORITHM

- *Design Consideration*

    - System model: it consist of three models ;LBS provider ,LBS users and cloud



..

    - Attack model
    - design aim: energy, certainty, freedom

- *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to privacy preserving spatial range query. Here use inner product encryption scheme and for indexing spatial data we use ss^tree .

inner product encryption scheme contain four algorithms

1 Setup algorithm
2 Enc algorithm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

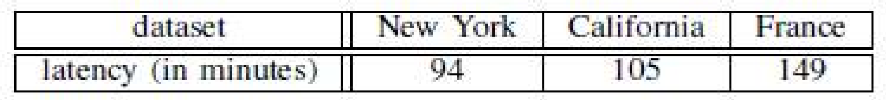
3 Gen token algorithm
4 Check algorithm

Setup algorithm is used for generate a public parameter key ,attribute encryption scheme and predicate encryption scheme. Enc for encrypting attribute vectors to ciphertexts; GenToken for encrypting predicate vectors to tokens; Check for checking if a ciphertext's attribute satisfies a token's predicate. The solution of propose method contain of two algorithms: system setup and spatial range search. In the former one the LBS provider initializes the system through many steps.

IV. **PERFORMANCE EVALUATION**

The result of the proposed EPLQ solution in terms of communication cost, computational cost, storage cost and accuracy. *Computational Cost at mainly in three side ,User Side ,cloud and lbs provider side. In user side they require two predicate vector tht needs* 2*n* modular exponentiations, about 2*n*2 multiplications and about 2*n*2 additions. *n* is the length of encoded vectors. the Android phone in test generate 1000 queries, and the average latency per query generation is about 0.9 second. In *LBS Provider's Computational Cost* in the time of system setup, they want to encrypt POI records, setup IPRE and build the ˆ *ss*-tree. computational cost mainly based on IPRE and ˆ *ss*tree . The cost is evaluated by system setup latency, that is the time used to setup IPRE and build the ˆ *ss*tree.

Communication Cost and Storage Cost of this eplq for creating query , LBS user create two tokens to the cloud andLBS provider sends the cloud the public parameter and the tree only once. So the communication cost is acceptable.The public parameter and ˆ *ss*-tree can use in the memory of even one single server. so, the storage cost is acceptable. The EPLQ provide *Accuracy* by using hash function in IPRE scheme and it reduces the size of public parameter, reduce false positives. cost of Table 1 show, the latencies for the three datasets are between 1 and 3 hours. Considering that system setup is conducted only once.



dataset	New York	California	France
latency (in minutes)	94	105	149

Table 1:System Setup Latency

Cloud's Computational Cost is acceptable based on experiment In the experiments, a workstation plays the role of cloud, and only four CPU cores can be utilized to do the computing. A real cloud has much more computing resources, and the query latency at a real cloud should be much lower. Figure1 show the experiment result.

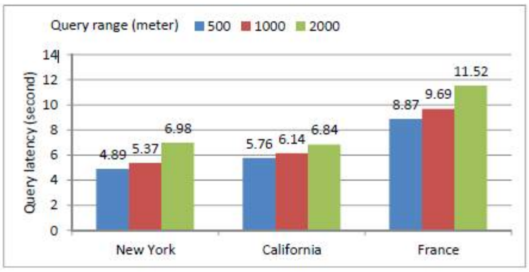


Fig:1 POI query latency at cloud side. Note that the latency should be much lower once deployed at a real cloud.

V. **CONCLUSION AND FUTURE WORK**

This paper introduces ; inner product range encryption scheme and sstree data structure which mobile users can entertain location-based services without the need to disclose their private location information and it provide security.

REFERENCES

[1] Lichun Li, Rongxing Lu, Senior Member, IEEE, and Cheng Huang, “EPLQ: Efficient Privacy-Preserving Location-BasedQuery Over Outsourced Encrypted Data”, IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 2, APRIL 2016.
[2] A. Gutscher, “Coordinate transformation - a solution for the privacy problem of location base services?” in 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), Proceedings, 25-29 April 2006, Rhodes Island, Greece, 2006. [Online].
[3] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new casper: query processing for location services without compromising privacy,” in VLDB, 2006, pp. 763
[4] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati, “Location privacy protection through obfuscation-based techniques,” in Data and Applications Security XXI. Springer, 2007
[5] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proceedings of the 1st international conference on Mobile systems, applications and services. ACM,2003.
[6]C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Di Vimercati, and P. Samarati, “Location privacy protection through obfuscation-based techniques,” in Data and Applications Security XXI. Spinger, 2007, pp. 47–60.
[7]Gabriel Ghinita1, Panos Kalnis1, Ali Khoshgozaran2, Cyrus Shahabi2, Kian-Lee Tan1 "Private Queries in Location Based Services Anonymizers are not Necessary".
[8]H. Kido, Y. Yanagisawa, and T. Satoh, “An anonymous communication technique using dummies for location-based services,” in ICPS. IEEE, 2005, pp. 88–97.
[9]A. R. Beresford and F. Stajano."Location privacy in pervasive computing" In IEEE Pervasive Computing, pages 46–55, 2003.
[10]G. Aggarwal. et al. Vision Paper: Enabling Privacy for the Paranoids. In VLDB, 2004