Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 114 - 118. Submitted 06/11/2017. Published 17/12/2017

EFFICIENT PRIVACY-PRESERVING LOCATION-BASED QUERY OVER OUTSOURCED ENCRYPTED DATA

[1]A.Kanmani, M.Phil Scholar, Bharathiyar Arts And Science College For Women, Deviyakurichi, Thalaivasal, Salem.

[2]R. Vasugi, Asst. Professor, Bharathiyar Arts And Science College For Women, Deviyakurichi, Thalaivasal, Salem.

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.

1. 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. Around ten years ago, location-based services (LBS) were used in military only. Today, thanks to advance in communication technologies and information technologies, more kinds of location based services have appeared, and they are useful for not only organizations but also individuals. Mobile LBS are services enhanced with positional data, which are provided by mobile apps using GPS, Dmaps, and other techniques. Many mobile apps provide interesting and convenient lbs and functions. The mobile app Yelp recommends nearby shops, restaurants, etc. In the social network mobile app Loopt, the users receive notifications Whenever their friends are nearby. The mobile app Waze reports nearby traffic jams, gas stations and friends. Users can access these services via the desktop, mobile phone, Personal Digital Assistant pager, Web browser , or other devices. When user send Query to the LBS Provider at that time

secret sharing algorithm to be used in order to provide encrypted location based query. Thus, user can achieve more confidentiality using this algorithm. 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. To decrypt the encrypted records received from the cloud, LBS users need to obtain the decryption key from the LBS provider in advance.

2. RELATED WORK

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 . 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.

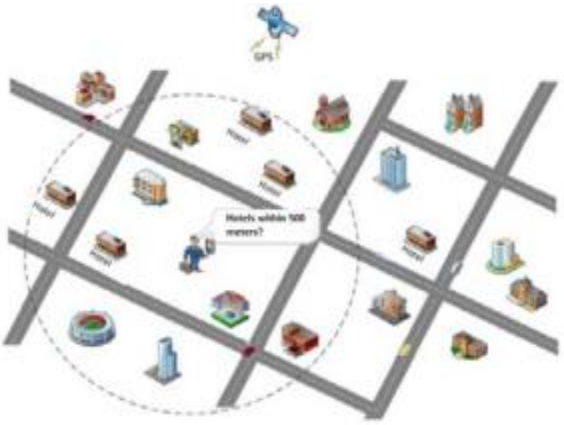

Fig.1.General Structure

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 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 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.

3. PROPOSED SYSTEM

The result of the proposed EPLQ solution in terms of communication cost, computational cost, storage cost and accuracy.

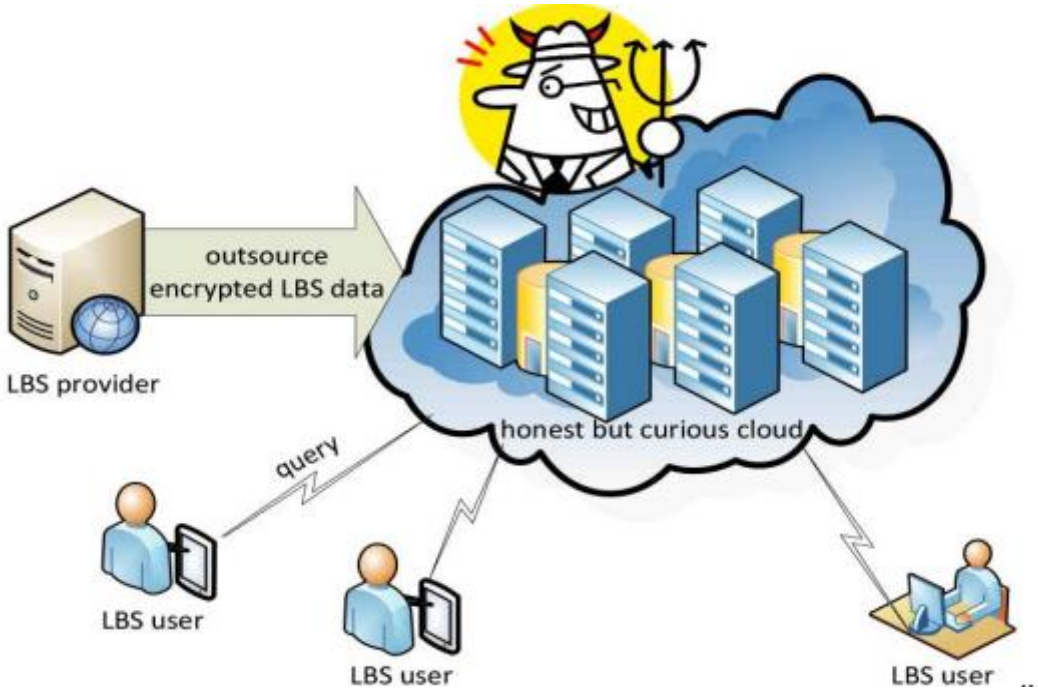

Fig.2.Proposed System

Computational Cost at mainly in three side ,User Side ,cloud and lbs provider side. In user side they require two predicate vector tht needs 2n modular exponentiations, about 2n2 multiplications and about 2n2 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 sstree . The cost is evaluated by system setup latency, that is the time used to setup IPRE and build the ˆ sstree. 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. 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. Spatial range query has extreme performance requirements. A good solution should not consume many resources of mobile LBS users, and the Point Of Interest search latency should be acceptable for online query. The proposed solution should be resilient to cipher text-only attacks and known-sample attacks. An accurate and efficient solution for spatial range query already exists, which is resilient to cipher text-only attacks but not to known-sample attacks and more powerful attacks. The proposed solution should be more secure than available solution.

4. ANALYSIS

The focus of this survey paper is to implement mobile application in which we explained the EPLQ technique that is the LBS user querying the POI to the LBS provider. The LBS provider in turn issue the result to the cloud but the provider don't want to share the raw information so he encrypt the information and share it to the cloud in turn the LBS user query when matches the information the cloud will issue the result to the user. The cloud has rich storage and computing resources.

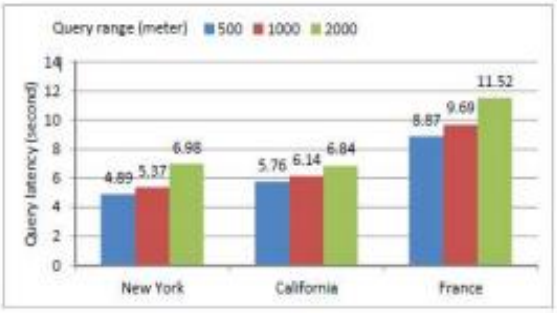

Fig.3.Analysis

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. The user will decrypt the data by the private key shared by the admin. 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.

CONCLUSION

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".