Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-4, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Effectively Preserving Location for Achieving Confidentiality

Ashwini Dasharth Gangurde [1], Shubhangi Subhash Deore [2] , Komal Kishor Nadage [3], Vrushali Rajendra Bathe[4.]
[1,2,3,4] B.E Student, Dept. of Computer engg, LoGMIEER, Nashik, Maharashtra, India

Abstract: *The aim of safe tourister application to outsource the location based service (LBS) data from the LBS provider to the cloud and from the cloud to the LBS provider which protects the privacy related issues of the LBS data. Initially LBS user query for a place to the LBS provider, LBS provider in turn upload the details to the cloud but in the form of encrypted text to prevent the cloud from stealing the data. LBS users in turn decrypt the details by the personal password send by the LBS provider to the LBS user. When the query of the LBS user matches the details in the cloud the LBS user will retrieve the details and make use of it. In this application it is shown with the demo of a tourist requesting for tourist places tourist is the LBS user and admin is the LBS provider .With the pervasiveness of smart phones, location based services have received considerable attention and become more popular and vital recently. However, the use of LBS also has a potential threat to user's location privacy. In this paper, aiming at spatial range query, popular LBS providing information About Points of Interest, we present an effective and privacy-preserving LBS solution, called EPLQ. To reduce query latency, we further design a privacy-preserving tree index structure in EPLQ. Detailed security analysis confirms the security properties of EPLQ. In additional, extensive experiments are conducted, and the results demonstrate that EPLQ is very effective in privacy preserving spatial range query over outsourced.*

Encrypted data. In particular, for a mobile LBS user using an Android phone device, around 1 second is needed to generate a query; and it also only requires a workstation, which plays the role of the cloud in our experiments, a few seconds to search POIs.

Keyword*: Location-based services (LBS), spatial range query, outsourced encrypted data, privacy-enhancing technology, Query Point, Effective and Privacy Preserving Location-Based query (EPLQ).*

1. Introduction

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 Loop, 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. Diverse applications include fleet tracking, emergency dispatch, roadside assistance, navigation, and more.
With overall view, the LBS applications can be categorized as:

- Navigation applications such as Route description, Turn-by-turn navigation.

- Safety and emergency applications like nearest medic center, Emergency calls, Warning about unsafe areas.

- Tracking applications such as Find a friend, Asset tracking etc.

- Information service applications like Traffic information, City Guide, Parking, Maps etc.

- Operator & Tariff applications likeTraffic measurements, Network planning.

2. System Model

a)The LBS Provider has abundant of LBS data, which are POI records. The LBS provider allows

authorized users (i.e., LBS users) to utilize its data through outsourcing, the LBS provider offers the query services via the cloud.

b) The Cloud has rich storage and computing resources. 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.

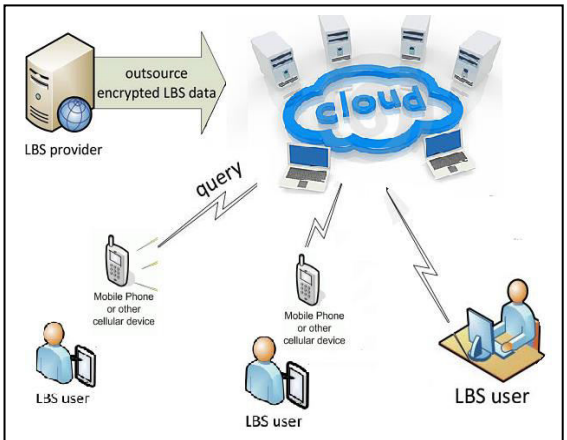

Figure 1.Proposed System Model

3) 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.

3)Design Model

Under the outsourced LBS system model, our design goal is to develop an efficient, accurate, and secure solution for privacy-preserving spatial range query. Specifically, the following three objectives should be achieved.

a) ***Efficiency***:-A good solution should not consume many resources of mobile LBS users, and the POI search latency should be acceptable for online query.

b) ***Accuracy*****:** It is desirable that a query result contains the exact records matching the query. False negatives would hurt user experience, while false positives would increase communication cost. Additional computational cost is also required at the user side to filter out false positives.

c) ***Security***: 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.

4)Algorithm

a)Message-Digest5 Algorithm:

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. According to RFC 1321, "MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input …The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA."

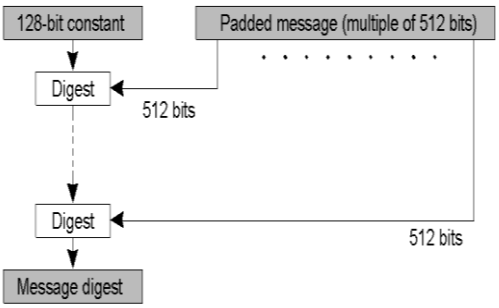

Figure 2.2 MD-5 Structure

Algorithmic Steps:

Step1: Append padding bits.
The input message is "padded" (extended) so that its length (in bits) equals to 448 mod 512. Padding is always performed, even if the length of the message is already 448 mod 512.

Step2. Append length
A 64-bit representation of the length of the message is appended to the result of step1. If the length of the message is greater than 2^64, only the low-order 64 bits will be used.

Step3. Initialize MD buffer
A four-word buffer (A, B, C, D) is used to compute the message digest. Each of A, B, C, D is a 32-bit register. These registers are initialized to the

following values in hexadecimal, low-order bytes first):
word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step4. Process message in 16-word blocks
Four functions will be defined such that each function takes an input of three 32-bit words and produces a 32-bit word output.

2) Shamir's Secret Sharing Algorithm:

Step 1: Suppose we want to use (k,n) threshold scheme to share our secret S where k _ n:

Step 2: Choose at random (k-1) coefficients a1, a2, a3,....,ak-1, and let S be the a0.

Step 3: Construct n points (i,f(i)) where i=1,2..n

Step 4: Given any subset of k of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a 0=S, which is the secret.

Conclusion:-

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. 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.

References:-

[1] lichun li, rongxinglu, *senior member, ieee*, and chenghuang "EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data." IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 2, APRIL 2016.

[2] T. K. Dang, j. Küng, and r. Wagner, "the sh-tree: a super hybrid indexStructure for multidimensional data," in proc. 12th int. Conf. DatabaseExpert syst. Appl. (dexa' 01), munich, germany, sep. 3–5, 2001,Pp. 340–349.

[3] A. Gutscher, "coordinate transformation a solution for the privacyProblem of location based services?" In *proc. 20th int. Parallel distrib.Process.Symp. (ipdps'06)*, rhodes island, greece, apr. 25–29, 2006,P. 424.

[4] A. Khoshgozaran and c. Shahabi, "blind evaluation of nearest neighbor Queries using space ransformation to preserve location privacy," in *Advances in spatial and temporal databases*. New york, ny, usa: Springer, 2007, pp. 239–257.

[5] G. Ghinita, p. Kalnis, a. Khoshgozaran, c. Shahabi, and k.-l. Tan,"private queries in location based services: anonymizers are not necessary,"In *proc. Sigmod*, 2008, pp. 121–132.

[6] W. K. Wong, d. W.-l. Cheung, b. Kao, and n. Mamoulis, "secureKnn computation on encrypted databases," in *proc. Sigmod*, 2009,Pp. 139–152.

[7] M. L. Yiu, g. Ghinita, c. S. Jensen, and p. Kalnis, "enabling searchServices on outsourced private spatial data," *vldb*j., vol. 19, no. 3,Pp. 363–384, 2010.

[8] B. Yao, f. Li, and x. Xiao, "secure nearest neighbor revisited," in *proc.Ieee 29th int. Conf. Data eng. (icde'13)*, 2013, pp. 733–744.

[9] X. Yi, r. Paulet, e. Bertino, and v. Varadharajan, "practical *k* nearest Neighbor queries with location privacy," in *proc. 30th int. Conf. DataEng. (icde)*, 2014, pp. 640–651.

[10] J. Shao, r. Lu, and x. Lin, "fine: a fine-grained privacy-preservingLocation-based service framework for mobile devices," in *proc. IeeeInfocom*, 2014, pp. 244–252.