International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014.

Location Based Service Protocol with Improved Privacy Using Lebesgue Curve

R.Arulprabu[#1], K.Rajakumari[*2]
#PG student, Department of Information Technology,
SNS College of Technology, Coimbatore, Tamil Nadu, India
[1]arulprabu04@gmail.com
[*]*Professor, Department of Information Technology,*
SNS College of Technology, Coimbatore, Tamil Nadu, India.
[2]rajilanju@yahoo.com

***Abstract*— The pervasiveness of mobile devices equipped with positioning capabilities has led to the emergence of numerous location-based applications and services. Using mobile network infrastructures, mobile users can rapidly gain access to a wealth of information by connecting to a variety of services. This includes queries for nearby medical services, specialized stores, social activities and groups, and others. In general, location-based service operators are assumed to be trusted parties that preserve the user's privacy. However, due to the sensitive nature of the information accessed by these parties and repeated information leakages that have been recorded, the privacy of users that access location-based services is at risk.**

***Keywords*— Location Based service,Global Positioning System, homomorphic encryption,Trusted third party,k-Nearest Neighbor**

I. INTRODUCTION

New promising business models is guaranteed by emergence of a set of new products and internet services that are the results on growth of smart phones and mobile devices in both software and hardware capabilities. Location- Based Services (LBSs) have attracted the utmost importance in this regard. Global Positioning System (GPS) or Network-Based Positioning used to determine the current position of a user, in order to define his/her location relatively to a business or a service . User can enquire about that information by communicating wirelessly with an LBS server.

LBSs suffer from a major security pitfall in terms of violating users' privacy. the LBS server gains knowledge of the users' coordinates, this information can be manipulated by the server itself or by any malicious party to trace the movements of the users.

This problematic urged without disclosing users' private information the research community to find a secure way to use LBSs. Strong protection for users' information can be attained by the server retrieving location-related information without being aware of the user's position or the point of interests he/she is requesting. It is challenging to achieve the latter target as the server needs to at least know this search criterion to retrieve the requested information.

For the localization component, It show that it is impossible to hide user locations from radio sensors, if radio-based localization is used. Then present an alternative localization technique based on directed signals, which protects users' location privacy against the localization service provider. For the communications component, design an anonymous communication protocol that prevents the communication service provider from linking a user's location information with her identity in a commercial setting.

Although such trusted servers allow the implementation of flexible access control policies, they are undesirable for many reasons. First, with the trust comes the liability. Many providers are reluctant to bear the liability that follows. Second, many users are uncomfortable with trusting a third party. Thus a requirement for a trusted server may deter the adoption of many location-based services. Third, a single trusted party may become a single point of attack. Thus, if the trusted party is compromised, many users' privacy is compromised.

To preserve the privacy of the user while interacting with the LBS server, It present in this section a novel approach based on homomorphic encryption scheme to preserve the privacy of the user while interacting with the LBS server. Homomorphic encryption schemes allow performing arithmetic operations (additions and multiplications) over encrypted data, meaning that the result of an arithmetic operation would be the same whether applied over plain bits or encrypted bits. Our work uses a symmetric encryption scheme as a basis to request LBS services anonymously and guarantee retrieving only suitable data.

Processing a user's request goes through the following four main steps:

1) Localizing category;
2) Localizing services;

3) Filtering services;
4) Generating results.

Demonstrate how these steps work by the follow-ing example. Assuming that the user needs to enquire about the nearby hospitals, he/she sends an encrypted request that represent both his/her current location (x,y) and the enquired category (hospital in this case). Once the server receives the request, it uses the user's position to calculate distances and localize nearby services. There- after, it selects only the objects enquired about, and sends them back to the user in encrypted form. Note that encryption scheme, described, allows performing operations between plain and encrypted bits and the resulting record becomes encrypted.

Mobility is key to personal freedom. With the increasing availability of mobile devices, many providers begin to offer location-based services. Although these services greatly enrich our mobility experiences, with them also comes the privacy concerns, as a location-based service provider now can continuously track the location of a user. This tracking may allow unauthorized access and cause serious consequences. Although a few solutions have been proposed to address the privacy concerns in various aspects, there has not been any comprehensive study of the problem; furthermore, most of the existing solutions require that a user trust a third party such as a location server as shown in fig 1.

These applications greatly enrich our lives and drive the demands for mobile and wireless communications services. However, they also raise serious privacy concerns as they enable the continuous tracking of involved users' locations. This tracking may allow improper disclosure or access to the location of a user by a stalker and thus may place a person in physical danger. Given the increasing concerns about location privacy, many governments and organizations are initiating studies on location privacy.

II. RELATED WORK

Popularity of mobile network and the soaring trends of cloud computing, people can enjoy the convenient life experiences offered by the mobile devices and remote servers. One of the popular services is LBS (e.g., Google Latitude), in which users can utilize the geographical information for gaining entertainment services. In general, the kernel of LBS relies on a -nearest neighbor (k-NN) search mechanism.

However, this action will disclose the user's current location which might harm the privacy of the user. In order to resolve the problem, a privacy-preserving LBS is needed. For building a privacy-preserving LB, security and accuracy are the two major challenges (in k-NN search). There are two major types of research works dealing with the predescribed challenges in the -NN search of LBS which can be classified into 3-tier and 2-tier LBS architectures. The 3-tier architecture hides user's location with the aid of a trusted third party (TTP). There are some drawbacks when it rely the privacy-preserving LBS upon a TTP. First, in these approaches, a TTP is a must for hiding the location of user.

The TTP knows about the user's too much sensitive information and becomes a single point to be attacked. Second, the anonymized status or space transformed status of a user is breakable by applying the Background Knowledge Attack or the Correlation Attack. Let's take the cloaking technique as an example to illustrate the situation of being attacks. In a cloaking technique, the querying user is anonymized in the cloak region with the security level of – anonymity benefits of the proposed protocol are listed in the following:

1) Resistance to Correlation Attack and Background Knowledge Attack. Before each query secret circular shift is performed and the amount of shift is determined only by the querying user, which can be regarded as an one-time pad encryption scheme, and therefore, providing high security. Servers cannot infer any knowledge about the user's location from the query history and the user's profiles, since the amount of shift has been scrambled by user and the POI information has also been encrypted. Under such circumstance, the Correlation Attack and Background Knowledge Attack made by the server cannot succeed.

2) Supporting multiuser scenario. The public-key characteristics of Paillier cryptosystem, one of the key components of our protocol, can easily adapt to the multiuser environment.

The proposed protocol only requires users to keep their private keys on the client side and send the corresponding public keys to the server side, which decouples the relation among users. The key management issue of newly joined user can be intuitively solved by the properties of the adopted public-key cryptosystem.

3) Providing high accuracy -NN search results. In general, the security challenge and accuracy challenge cannot be jointly addressed. There are lots of works which can obtain accurate K-NN results but are vulnerable to the Correlation Attack

III. PROBLEM DEFINITION

The e The number of smart phones or mobile devices is rapidly increasing nowadays. Because of the popularity of mobile network and the soaring trends of cloud computing, people can enjoy the convenient life experiences offered by the mobile devices and remote servers. One of the popular services is LBS (e.g., Google Latitude), in which users can utilize the geographical information for gaining entertainment services. This action will disclose the user's current location which might harm the privacy of the user. A performance

disadvantage of the Paillier cryptosystem is that one needs to compute rn mod n2. The distribution of their keys is not the same as that of the original one. The reduced number-theoretic problems are different from the original scheme. However, they did not prove the one-wayness/semantic security for the distribution.

IV. SYSTEMDESIGN & IMPLEMENTATION

A. *Design Network model*

In that module using java create and connect the two file named as Client and database server. If user request to register or send query to server through the client window send the process

B. *H-index generation*

H-Index versus H-Value: Observing the Hilbert curve one can find that the starting and the ending cells do not neighbor to each other. In this case, if the query position is near to the starting or ending cell of the curve, then the searching directions will be reduced from two to one, which is opposite to the starting or ending cell. Besides, one can also find that those H-values in DB are only used to string all the POIs together in a locality-preserving order and behave as a tool for addressing all POIs in DB. As long as those H-values retain their numerical order, altering those H-values won't affect the result of query because only the order of H-values is of concern in retrieving k-NN search results.

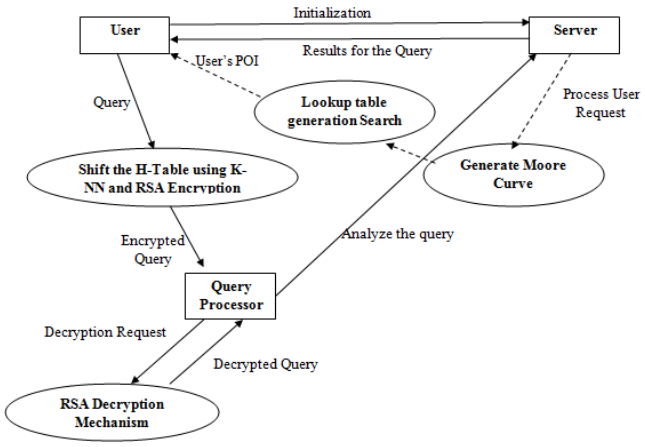

Figure 1 System Architecture

C. *Paillier Cryptosystem*

The public-key characteristics of Paillier cryptosystem, one of the key components of our protocol, can easily adapt to the multiuser environment. The protocol only requires users to keep their private keys on the client side and send the corresponding public keys to the server side, which decouples the relation among users. The key management issue of newly joined user can be intuitively solved by the properties of the adopted public-key cryptosystem.

Public-key cryptography based on the decisional composite residuosity problem to guarantee its security. Use Er(m) to denote the encryption of a message and D(Er(m)) to denote the corresponding decryption, where r a random number is belongs to and is a product of two large primes. The inherent random number r in the Paillier cryptosystem will prevent from generating the same ciphertext of the same plaintext message m, that is, the ciphertext Er1(m) will be totally different to the ciphertext Er2(m).

In the field of secure computation, Paillier cryptosystem is famous for its Additive Homomorphism. That means, for a given public-key kp and the ciphertexts Er1(m1) and Er2(m2), one can directly compute the addition of plaintexts m1+m2 in the encryption domain as:

D(Er1(m1)* Er2(m2) mod n2) = m1+m2

Paillier also supports Homomorphic Multiplication of one cyphertext and one plaintext, that is, for the given kp , Er1(m1) and m2, one can directly compute the multiplication of in the encryption domain by:

D((Er1(m1))m2 mod n2) = m1*m2

D. *Secret circular shift*

Due to the characteristics of Moore curve, the POIs stored in H-table's first and last rows are very close to each other, geographically. That is, despite whatever the H-index distance between the first and the last row would be, the two POIs neighbor to each other in the 2-D space. Following the same inference, the first and the last rows of H-table could be thought of as linking together just like an edge had been added to connect the two ending points of the corresponding Moore curve.

Let's define an entry (or a row) of H-table as the basic accessible unit; obviously, every entry (including both the first and the last one) has a neighboring relationship between its two adjacent entries. Now, if circularly shift the POI-info column of H-table two units downward but keep the H-index column intact and then make a k-NN query at Q. In general, if want to get the same k-NN query results after shifting the POI-info column units downward circularly, just need to change our querying H-index, H-index (Q), to shifted querying H-index, shifted-H-index (Q), as shifted-H-index (Q) = H-index (Q) + (d * t) and then send shifted-H-index (Q) to server as the new querying index. Notice that, upward shifting

the POI-info column is equivalent to set a negative integer to t.

E. K-NN Search Algorithms in PCQP

k-Adaptive Search Window: In a k-NN problem, the ground truth with respect to a query location Q is distributed on the map and could be covered by a sufficiently large 2-D search window. In order to find the exact k-NN result, define a –adaptive search window of size (2*D+1)2, where is the distance between the querying (or center) cell and the nearest cell on the borders of the search window. Thus, for applying PCQP to k-NN search, is chosen to be the minimum positive integer satisfying (2*D+1)2 ≥ k to guarantee that there are more than or equal to k POIs close to the query location in the search window, under the condition that (POI)/(cell) . If the full coverage of the predescribed k-adaptive search window could be searched, one would get the exact k-NN result since the coverage of -adaptive search window centered at includes more than or equal to k POIs.

Connected-Path Based k-NN Search Algorithm: Within a k-adaptive search window, the Moore curve can be divided into many disjoint connected paths. And based on the basic search process, the returned POIs from a k-NN search consist a connected path on the Moore curve. For finding the best neighbors which are covered by a k-adaptive search window, issue k-NN queries at each connected path to achieve the full coverage.

F. Modified Paillier cryptosystem

The main differences of the M-Paillier cryptosystem from the original one are the choice of the key g and the decryption algorithm. The public key g is chosen from the set.

GM-Paillier = {g

The set GM-Paillier is a subset of all public keys g of the original Paillier cryptosystem ,i.e., GM-Paillier Paillier. Then the computation L(gλ mod n2) in the Paillier decryption is equal to 1, due to gλ mod n2 = 1+n.

G. Algorithm

Algorithms used for Privacy Preserving Location-Based Service Protocol with Secret Circular Shift are as follows

- Heuristic Cross-Like -NN Search Algorithm
- Modified Paillier cryptosystem

Algorithm 1: Heuristic Cross-Like -NN Search Algorithm

Step 1: k-Adaptive Search Window: define a –adaptive search window of size (2*D+1)2, where is the distance between the querying (or center) cell and the nearest cell on the borders of the search window. Thus, for applying PCQP to k-NN search, is chosen to be the minimum positive integer satisfying:

(2*D+1)2 ≥ k

Step 2: Connected-Path Based k-NN Search: Within a k-adaptive search window, the Moore curve is divided into many disjoint connected paths. And based on the basic search process, the returned POIs from a k-NN search consist a connected path on the Moore curve.

Step 3: For finding the best neighbors which are covered by a k-adaptive search window, issue k-NN queries at each connected path to achieve the full coverage.

Algorithm 2: Modified Paillier cryptosystem

Step 1: Key Generation: The key is generated using the following RSA modulus.

- n = pq, the RSA modulus
- λ = lcm (p − 1, q − 1)
- g∈Z/(n^2 Z)×s.t g^λ=1+n mod n^2
- Public-key: (n, g), Secret key: λ

Step 2: Encryption: The message is encrypted using the following steps.

- m ∈ {0, 1, ..., n − 1}, a message
- h ∈Z/nZ
- c = gmhn mod n2, a ciphertext.

Step 3: Decryption: The message is decrypted using the following step.

m = L(cλ mod n2)

V. EXPERIMENTAL EVALVATION

The proposed PCQP is implemented by Java. The performance evaluation of client side is simulated on a PC equipped with Win7 OS, Intel i5-2400 3.1 GHz processor and 8 GB RAM. The LBS is conducted on a server with Debian 64bit OS, 2 Intel Xeon E5420 processor (8 cores in total) and 32 GB RAM.

In the experiments, the value of is gradually increased and the size of -adaptive search window, i.e., (2D+1)2 , is progressively increased according to , so that there is a little variation in accuracy performance when the window size is changed. This phenomenon is particularly obvious when the number of additional queries is one since the full coverage of the window cannot be reached well, in this case. The accuracy of the various methods are plotted in a graph as shown in Figure 2.

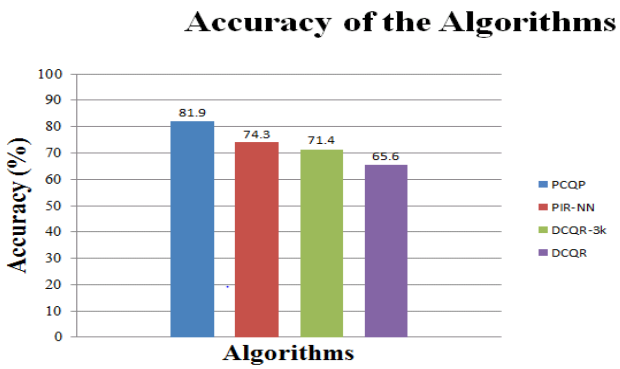

Figure 2 Accuracy graph

The various algorithms such as PCQP, PIR-NN, DCQR and DCQR-3 k are compared. It can be seen that the PCQP mechanism shows a higher accuracy rate than any of the algorithms used. The PIR-NN algorithm is almost accurate as the proposed but still it lags behind some considerable amount. Hence the proposed algorithm out performs all the algorithms.

VI. CONCLUSIONS

In this work, a Private Circular Query Protocol with cross like search mechanism is proposed to simultaneously accomplish the location-based k-NN query and the location privacy preservation, in a novel way. To the best of our knowledge, this is the first work to apply Moore curves to location-based query problem. The proposed circular structure seamlessly integrates the robustness of specific public-key cryptosystems and the clustering property of space-filling curves. In other words, it has achieved a novel computing scheme for conducting secret computation with well-clustering property. Expect the proposed framework not only can address the challenges of privacy preserving LBS, but also inspire the research of secret computation with desired property to achieve privacy preserving information processing. It address the problem of preserving the location privacy and user anonymity when receiving authenticated location-based services. Develop a privacy-preserving communication protocol used M-paillier cryptosystem that allows users to place queries to a location based server without revealing their identity, or current location beyond a certain accuracy.

A. FUTURE ENHANCEMENT

In future the Hilbert curve can be replaced by using the Lesbsgue curve to improve the space filling transformation for clustering and optimization algorithms can be used for identifying the user location more accurately.

REFERENCES

[1] I.-Ting Lien, Yu-Hsun Lin,, Jyh-Ren Shieh, and Ja-Ling Wu, “A Novel Privacy Preserving Location-Based Service Protocol With Secret Circular Shift for -NN Search”, IEEE Transactions On Information Forensics And Security, Vol. 8, No. 6, June 2013

[2] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location- based identity inference in anonymous spatial queries,” IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[3] M. Gruteser, D. Grunwalddepartment, and C. Science, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proc. 1st Int. Conf. Mobile Systems, Applications and Services, 2003, pp. 31–42.

[4] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, “Casper*: Query processing for location services without compromising privacy,” ACM Trans. Database Syst., vol. 34, pp. 24:1–24:48, Dec. 2009.

[5] M. Mokbel, “Towards privacy-aware location-based database servers,” in Proc. 22nd Int. Conf. Data Engineering Workshops, 2006, pp. 93–102.

[6] A. Khoshgozaran and C. Shahabi, “Blind evaluation of nearest Neighbor queries using space transformation to preserve location privacy,” in Proc. 10th Int. Conf. Advances in Special and Temporal Databases (SSTD’07), 2007, pp. 239–257.

[7] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location based services: anonymizers are not necessary,” in Proc. 2008 ACM SIGMOD Int. Conf. Management of Data, New York, NY, USA, 2008, pp. 121–132, ser. SIGMOD’08, ACM.

[8] *H. Sagan, Space-Filling Curves. New York, NY, USA: Springer-Verlag, 1994.*

[9] B. Moon, H. Jagadish, C. Faloutsos, and J. Saltz, “Analysis of the clustering properties of the hilbert space-filling curve,” IEEE Trans. Knowl. Data Eng., vol. 13, no. 1, pp. 124–141, Jan./Feb. 2001.

[10] A. Khoshgozaran, C. Shahabi, and H. Shirani-Mehr, Location Privacy: Going Beyond k-Anonymity, Cloaking and Anonymizers. NewYork, NY, USA: Springer-Verlag New York, Inc., Mar. 2011, vol. 26, pp.435–465, no. 3.

[11] S. Papadopoulos, S. Bakiras, and D. Papadias, “Nearest neighbor search with strong location privacy,” in Proc. VLDB Endow., Sep. 2010, vol. 3, no. 1–2, pp. 619–629.

[12] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Advances in Cryptology Eurocrypt 1999*. NewYork,NY, USA: Springer-Verlag, 1999, pp. 223–238.

[13] J. Hoffstein, J. Pipher, and J. H. Silverman, “Ntru: A ring-based public key cryptosystem,” in *ANTS*, ser. Lecture Notes in Computer Science, J. Buhler, Ed. New York, NY, USA: Springer, 1998, vol. 1423, pp. 267–288.

[14] T. Onodera and K. Tanaka, “Shuffle for paillier’s encryption scheme,” IEICE Trans. Fund. Electron., Commun., Computer Sci., vol. E88-A, pp. 1241–1248, 2005

[15] D. Kahn, *The Code Breakers—The Story of Secret Writing*. New York, NY, USA: Macmillan, 1967.

[16] S. A. V. Alfred, J. Menezes, and P. C. van Oorschot, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[17] J.-H. Um, H.-D. Kim, and J.-W. Chang, “An advanced cloaking algorithm using Hilbert curves for anonymous location based service,” in *Proc. 2010 IEEE Second Int. Conf. Social Computing*, 2010, pp. 1093–1098.

[18] A.-A. Hossain, A. Hossain, H.-K. Yoo, and J.-W. Chang, “H-star: Hilbert-order based star network expansion cloaking algorithm in road

networks," in *Proc. IEEE 14th Int. Conf. Computational Science and Engineering (CSE)*, Aug. 2011, pp. 81–88.

[19] H. V. Jagadish, "Linear clustering of objects with multiple attributes," in *Proc. 1990 ACM SIGMOD Int. Conf. Management of Data*, New York, NY, USA, 1990, pp. 332–342, ser. SIGMOD'90, ACM.

[20] E. H. Moore, "On certain crinkly curves," *Trans. Amer. Math. Soc.*,vol. 1, pp. 72–90, Jan. 1900.