ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Privacy Preserving on Location Based Queries Using Symmetric Key

S.Purni[1], K.K.Shalini[2], R.Susila[3], Mrs.J.Preetha[4]

UG students, Department of Computer Science and Engineering, Muthayammal Engineering College, Rasipuram, Tamil Nadu, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Muthayammal Engineering College, Rasipuram, Tamil Nadu, India[4]

ABSTRACT: Location based system are used for finding out Point Of Interests (POI) from a specific location. Usually a GPS latitude and longitude is sent as an input to the location servers and based on the GPS coordinate the point of interests can be served back to the client from the location server. To solve problems associated with the location data. The user does not want to send his location data (GPS coordinate) to the server directly, since doing so the server can find the user's location preferences and use that data for advertising the user's privacy is lost. The second part is like the server wants to protect its data from the user query. The server want to return back only relevant data to the user .The server cannot sent back other sensitive data to the user. A major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Symmetric key Transfer and the second step is based on Private Information based on Symmetric key Retrieval, to achieve a secure solution for both parties. The solution is efficient and practical in many scenarios. Implement the solution using a real cloud location server and android mobile application.

KEYWORDS: Location based query, private information query, Advanced symmetric key, Private information Retrieval

I. INTRODUCTION

Location based service (LBS) is an information, entertainment and utility service generally accessible by mobile devices such as, mobile phones, GPS devices, pocket PCs, and operating through a mobile network. LBS can offer many services to the users based on the geographical position of their mobile device. The services provided by LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station. The user will search for information asking for the Point of interest say a shopping mall nearby or any route from source to destination The location provider will return the point of interest to the user queries by displaying nearby attraction for given query. The server will return the data based on search with its GPS coordinates. Location of the data will be identified in private grid which is generated internally by the application there by client will sent his/him location to be determined in public grid which is on the server side The client will send a request using the server's cell information asking for the Point of interest say a shopping mall nearby, then the server will return an encrypted data of the point of interest to the client.

II. EXISTING SYSTEMS

Mobile smart phone users frequently need to search for nearby points of interest from a location based service, but in a way that pre- serves the privacy of the users' locations. The algorithm makes use of a variable- sized cloaking region [2] that increases the location privacy of the user at the cost of additional computation, but maintains the same traffic cost. Users of mobile devices tend to frequently have a need to find Points Of Interest (POIs), such as restaurants, hotels, or gas stations, in close proximity to their current locations. Collections of these POIs are typically stored in databases ad-

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

ministered by Location Based Service (LBS) providers such as Google, Yahoo!, and Microsoft, and are accessed by the company's own mobile client applications or are licensed to third party independent software vendors. Mobile devices with global positioning capabilities allow users to retrieve Points Of Interest (POI) in their proximity. To protect user privacy, it is important not to disclose exact user coordinates to un-trusted entities that provide location-based services. There are two main approaches [3] to protect the location privacy of users: hiding locations inside Cloaking Regions (CRs) and encrypting location data using Private Information Retrieval (PIR) protocols. Previous paper focused on finding good trade-offs between privacy and performance of user. Next it is MobiMix[4], a road network based mix-zone framework to protect location privacy of mobile users travelling on road networks. In contrast to spatial cloaking based location privacy protection, the approach in MobiMix is to break the continuity of location exposure by using mix-zones, where no applications can trace user movement. This paper makes two original contributions. First, it provide the formal analysis on the vulnerabilities of directly applying theoretical rectangle mix-zones to road networks in terms of anonymization effectiveness and attack resilience. It argue that effective mix-zones should be constructed and placed by carefully taking into consideration of multiple factors, such as the geometry of the zones, the statistical behaviour of the user population, the spatial constraints on movement patterns of the users, and the temporal and spatial resolution of the location exposure. Second, it develop a suite of road network mix-zone construction methods that provide higher level of attack resilience and yield a specified lower-bound on the level of anonymity. Then it evaluate the MobiMix approach through extensive experiments conducted on traces produced by GTMobiSim on different scales of geographic maps.

III. PROPOSED SYSTEMS

The proposed system consists of six phases namely user mobile, private grid, then third phase is encrypted data and decrypted data, fourth phase is location query web service, public grid and location server to the client.

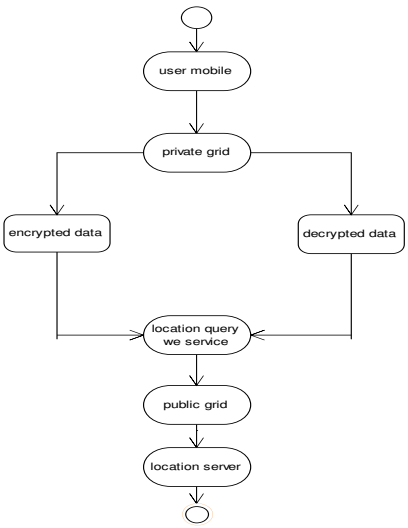

Fig.1Flow of proposed system

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

User Mobile

In this phase the user will use the mobile to search the location based data. The request will be sent from the mobile to the web server.

Private Grid

In this phase the requested data will be stored in the private grid. The grid consists of rows and columns. The latitude and longitude of the user will be stored in the private grid.

Encrypted and decrypted data

In this phase with the help of Advanced symmetric key the data will be encrypted from the private grid so that service provider does not have access. After getting the response from the server the data will be decrypted along with the same key.

Location Query web service

The Location Query is a kind of query which cannot be revealed because it is encrypted. The user or the service provider does not know the encrypted query.

Public Grid

The public Grid will store all the queries that are searched by the user. So that in previous the service providers associate this information along with the phone book or address book to identify the user address. Now the query stored in the public grid will be encrypted so that it cannot reveal user identity.

Location Server

The location server will give response to the client after decrypting with the same symmetric key. The user will get the response for what they searched.

IV. MODULE DESCRIPTION

The main modules in the proposed system are

- Getting User grid cell information
- Finding Server information
- Point of interest
- Symmetric encryption
- Sending information without GPS

Getting user grid cell information

Android Mobile application will send the user grid cell information to the server and the security key to decrypt the data. We will be using symmetric encryption key. *Function*: user will search for information asking for the Point of interest say a shopping mall nearby or any route from source to destination The location provider will return the point of interest to the user queries by displaying nearby attraction for given query. The server will return the data based on search with its GPS coordinates. The client will send a request using the server's cell information asking for the Point of interest say a shopping mall nearby. With the knowledge about which cells are contained in the private grid, and the knowledge of the

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

key that encrypts the data in the cell, the user can initiate a private information retrieval protocol with the location server to acquire the encrypted POI data. Assuming the server has initialized the integer *e*, the user *UI* and *LS* can engage in the following private information retrieval protocol using the *ID*, obtained from the execution of the previous protocol, as input. The *ID* allows the user to choose the associated prime number power πi, which in turn allows the user to query the server.

Finding Server Information

The server will super imposed the user cell information with the server location grid and find the location server's grid cell information. The server's cell Information will be sent back to user.
The server will also send all the information encrypted using the key sent by the client. The communication between client and server will be secure. The client will never send the GPS coordinate but will send an information grid of its location. New privacy metrics have been proposed that captures the users' privacy with respect to LBSs. The authors begin by analyzing the shortcomings of simple k-anonymity in the context of location queries. Next, they propose privacy metrics that enables the users to specify values that better match their query privacy requirements. From these privacy metrics they also propose spatial generalization algorithms that coincide with the user's privacy requirements. Methods have also been proposed to confuse and distort the location data, which include path and position confusion. Path confusion was presented by Hoh and Gruteser. The basic idea is to add uncertainty to the location data of the users at the points the paths of the users cross, making it hard to trace users based on raw location data that was k-anonymised. Position confusion has also been proposed as an approach to provide privacy. The idea is for the trusted anonymiser to group the users according to a cloaking region (CR), thus making it harder for the LS to identify an individual. A common problem with general CR techniques is that there may exist some semantic information about the geography of a location that gives away the user's location. For example, it would not make sense for a user to be on the water without some kind of boat. Also, different people may find certain places sensitive. Damiani *et al.* have presented a framework that consists of a obfuscation engine that takes a users profile, which contains places that the user deems sensitive, and outputs Obfuscated locations based on aggregating algorithms

Point Of Interest

The client will send a request using the server's cell information asking for the Point of interest say a shopping mall nearby. The server will return an encrypted data of the point of interest to the client. The client will plot the information in the graph. *Function:* location of the data will be identified in private grid which is generated internally by the application there by client will sent his/him location to be determined in public grid which is on the server side The client will send a request using the server's cell information asking for the Point of interest say a shopping mall nearby, then the server will return an encrypted data of the point of interest to the client.

Symmetric Encryption

The request sent by the client will use the symmetric encryption key to encrypt all the data. Further the connection between server and client will be secure. The request sent by the client will use the symmetric encryption key to encrypt all the data. Further the connection between server and client will be secure. the privacy of the user is maintained by constantly changing the user's name or pseudonym within some mix-zone. It can be shown that, due to the nature of the data being exchanged between the user and the server, the frequent changing of the user's name provides little protection for the user's privacy. A more recent investigation of the mix-zone approach has been applied to road networks. They investigated the required number of users to satisfy the unlink ability property when there are repeated queries over an interval. This requires careful control of how many users are contained within the mix-zone, which is difficult to achieve in practice. A complementary technique to the mix-zone approach is based on k-anonymity. The concept of k-anonymity was introduced as a method for preserving privacy when releasing sensitive records. This is achieved by generalization and suppression algorithms to ensure that a record could not be distinguished from $(k-1)$ other records. The solutions for LBS use a trusted

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

anonymiser to provide anonymity for the location data, such that the location data of a user cannot be distinguished from *(k − 1)* other users.

Sending Information without GPS

The server will also send all the information encrypted using the key sent by the client. The communication between client and server will be secure. The Client will never send the GPS coordinate but will send an information grid of its location. We analyze the security of the client and the server. While the client does not want to give up the privacy of his/her location, the server does not want to disclose other records to the client. This would not make much business sense in a variety of applications. the information that is most valuable to the user is his/her location. This location is mapped to a cell. In both phases of our protocol, the oblivious transfer based protocol and the private information retrieval based protocol, the server must not be able to distinguish two queries of the client from each other.

V. PROPOSED ADVANCED SYMMETRIC KEY GENERATION STEPS

1. Select or create any private key of Size 256 X 2 bits or 64 characters.
2. Size of selected key will be varying from 128 bits to 512 bits or 16 to 64 characters.
3. We can choose any character from 0 to 255 ASCII code.
4. Use of 64 * 8 key that means 512 bits in length.
5. Divide 64 bytes into 4 blocks of 16 bytes likes Key_Block1, Key_Block2, Key_Block3, and Key_Block4.
6. Apply XOR operation between Block1 and Block3. Results will store in new Key_Block13.
7. Apply XOR operation between Block2 and Block13. Results will store in new Key_Block213.
8. Apply XOR operation between Key_Block213 and Key_Block4. Results will store in new Key_Block4213.
9. Repeat Step 7, 8, 9 till (random number / 4).
10. Exit

VI. EXPERIMENTATION RESULT

Graphical representation for the table 1 and with blue line and orange line for encryption time and decryption time o "**Advanced Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm"** and **"Effect of Security Increment to Symmetric Data Encryption through AES Methodology"**, respectively and green line is for **"Proposed Algorithm"**. According to the graph, there is a tendency that encryption/decryption time for Proposed Algorithm, and compared algorithms increases with file size. But required time for the encryption/decryption

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Table 1: Encryption time comparisons of text files

Plain Text size	DJSA algorithm	Data Encryption through AES Methodology	Proposed algorithm
1.66 mb	0:01:34	0:01:32	0:01:25
56 kb.txt	0:00:37	0:00:35	0:00:28
187 kb.txt	0:00:18	0:00:16	0:00:09
46 kb.txt	0:00:11	0:00:09	0:00:02
16 kb.txt	0:00:10	0:00:08	0:00:01

through Proposed Algorithm is much smaller than encryption/decryption time for compared algorithms. The observations were made using personal computer with specifications of Intel Pentium Dual Core E2200 2.20 Ghz, 1 GB of RAM and Window-XP SP2as the platform.

VII. CONCLUSION

We have presented a location based query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is for a user to privately determine his/her location using Advanced Symmetric key transfer on a public grid. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency. We analyzed the performance of our protocol and found it to be both computationally and communicational more efficient than the solution by Ghinita *et al.*, which is the most recent solution. We implemented a software prototype using a desktop machine and a mobile device. The software prototype demonstrates that our protocol is within practical limits

REFERENCES

[1]R.Paulet,M.GolamKaosar,X.Yi,andE.Bertino,"Privacypreserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53
[2]X. Chen and J. Pang, "Measuring query privacy in location-based services," in *Proc. 2nd ACM CODASPY*, San Antonio, TX, USA, 2012, pp. 49–60.
[3]G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearest neighbour queries with database protection," *GeoInformatica*, vol. 15, no. 14, pp. 1–28, 2010.
[4]B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in *Proc. ICDE*, Hannover, Germany, 2011, pp. 494–505.
[5]G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacy preserving matching of spatial datasets with protection against background knowledge," in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12
[6] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearest neighbour queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010