Preserving User Privacy and Preventing Location Server Content in Location Based Service

B. Dwarakanath [1], P. Adorin Rini[2]

[1, 2]Hindustan University, Department of Information Technology,
Chennai, Tamil Nadu, India

Abstract: ***Nowadays, it is very easy for a person to learn his/her location with the help of a Global Positioning System (GPS) enabled device. A location-based service (LBS) is a new and developing technology for mobile users. When this location is provided to a LBS via querying, it is possible to learn location dependent information, such as locations of friends or places, weather or traffic conditions around the location. This problem is defined as follows: (i) a user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users.***

Keywords: Location based query, point of Interest, and private query.

1. Introduction

A location-based service (LBS) is a mobile application that is dependent on the location of a mobile device, like mobile phone "Information services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the mobile device "Open Geospatial Consortium "defined LBS service similarly: "A wireless-IP service that uses geographic information to serve a mobile user, any application service that exploits the position of a mobile terminal." A Location Based Service (LBS) is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of geographical position of the mobile device. Location-based services (LBS) provide the mobile clients personalized services according to their current location. The Location object represents a geographic location which can consist of a latitude, longitude, timestamp, and other information such as bearing, altitude and velocity [4].

In location based services (LBS), users with location were mobile devices can query their surroundings anywhere and at any time. While this ubiquitous computing paradigm brings great convenience for information access, it raises a concern of potential intrusion on user's location privacy, which has hampered the widespread use of LBS [1]. The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all conditions, anywhere on or near the Earth. GPS satellite transmits data that indicates its location and the current time. All GPS satellites synchronize operations so that these repeating signals are transmitted at the same instant. The signals, moving at the speed of light, arrive at a GPS receiver at slightly different times because some satellites are further away than others. The distance to the GPS satellites can be determined by estimating the amount of time it takes for their signals to reach the receiver.

2. Data Mining

Data mining, also known as Knowledge-Discovery in Databases (KDD), is the process of automatically searching large volumes of data for patterns. Data Mining applies many older computational techniques from statistics, machine learning and pattern recognition Extract, transform, and load transaction data onto the data warehouse system. Store and manage the data in a multidimensional database system. Provide data access to business analysts and information technology professionals. Analyze the data using application software.

3. Product Perspective

The Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting Point of Interests (POIs). Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBS have to ensure that LS's data is not accessed by any unauthorized user.

During the process of transmission the users should not be allowed to discover any information for which they have not paid. It is thus crucial that solutions be devised that address the privacy of the users issuing queries, but also prevent users from accessing content to which they do not have authorization.

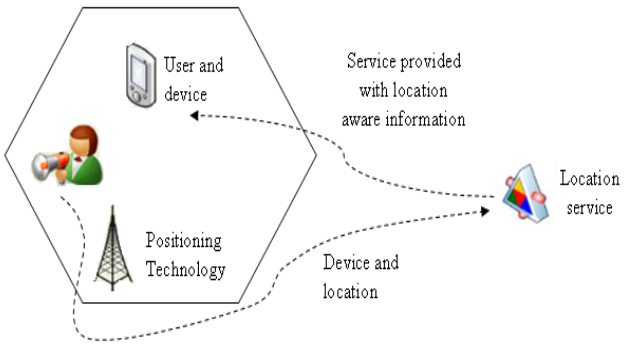

Figure 1: Location infrastructure

4. Existing Approach

In this module, we define the problems in existing approach that doesn't take care of privacy of the user and also failed to protect the location server content. Querying about the location details, the server cannot prevent their details from the user and the user cannot preserve their privacy from server [6].

5. Proposed work

The ultimate goal of our project is to obtain a set (block) of POI records from the LS, which are close to the user's position, without compromising the privacy of the user or the data stored at the server [3]. We propose this by applying a two stage approach

1. Oblivious Transfer (OT)
2. Private Information Retrieval (PIR)

The first stage is based on a two-dimensional oblivious transfer and the second stage is based on a communicational efficient PIR. The oblivious transfer based protocol is used by the user to obtain the cell ID, where the user is located, and the corresponding symmetric key. The knowledge of the cell ID and the symmetric key is then used in the PIR based protocol to obtain and decrypt the location data.

IDQi, j ----- Cell ID
ki,j ----- Symmetric key

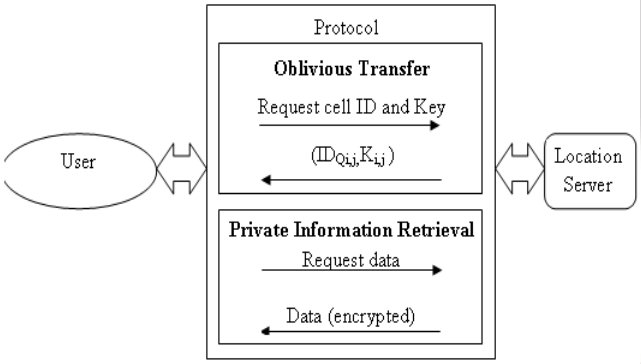

Figure 2: Architecture Diagram

5.1. User Classes and Characteristics

A user u from the set of users U initiates the protocol process by deciding a suitable square cloaking region CR, which contains his/her location. All user queries will be with respect to this cloaking region [8]. The user also decides on the accuracy of this cloaking region by how any cells are contained within it. The server encrypts each record ri within each cell of Q,Qi,j, with an associated symmetric key ki,j [6].

6. Implementation

The encryption keys are stored in a small (virtual) database table that associates each cell in the public grid P, Pi, j, with both a cell in the private grid Qi,j and corresponding symmetric key ki,j The server then processes the encrypted records within each cell Qi, j such that the user can use an efficient PIR , to query the records [9]. Finally, the server uses the Chinese Remainder Theorem to find the smallest integer to find the shortest distance.

6.1 Oblivious Transfer Phase

The purpose of this method is for the user to obtain one and only one record from the cell in the public grid P. This will be achieved by constructing a 2-dimensional oblivious transfer, based on the ElGamal oblivious transfer using adaptive oblivious transfer. The public grid P, known by both parties, has m columns and n rows [10]. In our implementation experiment for the oblivious transfer protocol, we generated a modified ElGamal instance with |p| = 1024 and |q| = 160, where q|(p − 1).We also found a generator a, and set g0 = aq (g has order q).We also set a generator g1, which has order q − 1. We set the public matrix P to be a 25×25 matrix of key and index information. We first measured the time required to generate a matrix of keys. This procedure only needs to be executed once for the lifetime of the data. There is a requirement that each hash value of gg Ri g Cj 1 0 is unique3. We use the SHA-1 to compute the hash H(.), and we assume that there is negligible probability that a number will repeat in the matrix.

6.1.2 Oblivious Transfer Algorithm

1)QueryGeneration1 (Client) (QG1):
Takes as input indices i, j, and the dimensions of the key matrix m, n, and outputs a query Q1 and secret s1, denoted as (Q1, s1) = QG1(i, j, m, n).
2)ResponseGeneration1(Server) (RG1):
Takes as input the key matrix Km×n, and the query Q1, and outputs a response R1, denoted as (R1) =RG1(Km×n,Q1).
3)ResponseRetrieval1 (Client) (RR1):
Takes as input indices i, j, the dimensions of the key matrix m, n, the query Q1 and the secret s1,and the response R1, and outputs a cell-key ki,j and cell-id IDi,j , denoted as (ki,j, IDi,j) = RR1(i, j, m, n, (Q1, s1),R1).

6.2 Private Information Retrieval Phase

With the knowledge about which cells are contained in the private grid, and the knowledge of the 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 [5]. The user will successfully acquire the block that contains the encrypted POI records. With the knowledge of the cell key ki, j, the user can decrypt Ci and obtain the requested data, thus concluding one round of the protocol. In the PIR protocol we fixed a 15 × 15 private matrix, which contains the data owned by the server. We chose the prime set to be the first 225 primes, starting at 3.The powers for the primes were chosen to allow for at least a block size of 1024 bits (3647, 5442, ..., 142998). Random values were chosen for each prime power e = Ci (mod πi), and the Chinese Remainder Theorem was used to determine the smallest possible e satisfying this system of congruence's.

Once the database has been initialised, the user can initiate the protocol by issuing the server his/her query. The query consists of finding a suitable group whose order is divisible by one of the prime powers πi. We achieve this in a similar

manner to Gentry and Ramzan. We choose primes q0 and q1 and compute "semisafe" primes Q0 = 2q0πi + 1 and Q1 = 2q1 + 1. We set the modulus as N = Q0Q1 and group order as φ(N) = φ(Q0Q1) = (Q0 − 1)(Q1 − 1). Hence, the order φ(N) ha πi as a factor. We set g to be a quasi-generator, such that the order of g also contains πi. In our experiment, we set |q0| = |q1| = 128.This results in a modulus N which is roughly 1024 bits in length, which is equivalent to an RSA modulus. Access gRigCj , since the discrete logarithm is hard in the outer group, the client must operate in the outer group to remove the blinding factors. This contributed to faster execution in the first stage [2].

6.2.1 Private Information Retrieval Algorithm

1) QueryGeneration2 (Client) (QG2):
   Takes as input the cell-id IDi,j , and the set of prime powers S, and outputs a query Q and secrets 2,denoted as (Q2, s2) = QG2(IDi,j , S).
2) ResponseGeneration2 (Server) (RG2):
   Takes as input the database D, the query Q2, and the set of prime powers S, and outputs a response R2, denoted as (R2) = RG2(D,Q2, S).
3) ResponseRetrieval2 (Client) (RR2):
   Takes as input the cell-key ki,j and cell-id IDi,j ,the query Q2 and secret s2, the response R2,and outputs the data d, denoted as (d) =RR2(ki,j, IDi,j , (Q2, s2),R2)[7].

7. Results

We used above algorithm to check retrieval of information with the desktop and Mobile devices.

Table 1: Oblivious Transfer experimental results for desktop and mobile device

Component	*Average Time (in sec)*	
	Desktop	*Mobile*
InitialisationOT	1.70958	_
Query Generation	_	0.00108
Response Generation	0.00969	_
Response Retrieval	_	0.00004

We analysed the performance of our algorithm and found it to be both computationally and communicationally more efficient.

8. Conclusion

The software prototype demonstrates the efficiency with respect to speed and practicality of our approach for desktop and mobile devices within practical limits. Further to this work, the privacy of user information who try to retrieve the data can be maintained by applying the private information retrieval algorithm.

References

[1] Beresford, F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46-55, 2012.
[2] Hoh and M. Gruteser, "Protecting location privacy through path confusion," Proc. *SecureComm'05*, 2005, pp. 194 - 205.
[3] Damiani ML, Bertino E, Silvestri C (2010) The probe framework for the personalized cloaking of private locations. Trans Data Privacy 3:123–148
[4] Dewri R, Ray I, Whitley D (2010) Query m-invariance: Preventing query disclosures in continuous location-based services. In: Eleventh international conference on mobile data
[5] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection," *GeoInformatica*, pp. 1 - 28, 2010.
[6] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, Private queries in location based services: anonymizers are not necessary," Proc. *SIGMOD'08.*, 2008, pp. 121 - 132.
[7] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacy preserving matching of spatial datasets with protection against background knowledge," Proc. *GIS '10*, 2010, pp. 3 - 12.
[8] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking," Proc. *1st international conference on Mobile systems, applications and services*, 2003, pp. 31 - 42.
[9] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," Proc. *UbiComp'07*, 2007, pp. 372 - 390.
[10] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," Proc. *CRYPTO'89*. 1990, pp. 547 - 557.

Author Profile

B. Dwarakanath received the B.E. and M. Tech. degrees in Computer Science and Engineering from Bangalore University and Vellore Institute of Technology in 2000 and 2004, respectively. During 2001-2002, he stayed in Muthayammal Engineering College. His research interests are Data Mining, Image Processing and Network Programming. He is now with Hindustan University.

P. Adorin Rini received the M. Sc degree in Computer Science from Vivekananda College. Her areas of interest are Mobile Computing and Data Mining. Currently, she is a M. Tech scholar in Hindustan University.