A Secure Protocol for Location Based Queries

Kajal Chauhan[1] Shweta Dhawale[2] Poonam Ithape[3] Sonam Pawar[4]
[1,2,3,4]Department of Computer Engineering

Abstract— In this paper we are going to present a solution to one of the location-based query problems. This problem is defined are as follows: (i) a user wants to query a database of location data, called as Points Of Interest, and does not want to reveal person 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. The location server desires to have some control over its data, since the data is its asset. We propose a major enhancement upon previous solutions we are introducing a two stage approach, first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. The solution we are going to present is efficient and practical in many scenarios. We are implementing our solution on a desktop machine and a mobile device to assess the efficiency of our protocol. We are introducing a security model and analyse the security in the context of our protocol. Finally, we highlight a security weakness of our previous work and present a solution to overcome it. The paper formally defines a framework to evaluate the risk in revealing a user identity via location information and presents preliminary ideas about algorithms to prevent this to happen. The popularity of location-based services leads to serious concerns on user privacy. A common mechanism is to protecting users' location and query privacy is spatial generalization. The paper sets out a formal framework within which obfuscated location-based services are defined.

Key words: Location based Query, Private Query, Private Information Retrieval, Oblivious Transfer

I. INTRODUCTION

A Location based service is an information, entertainment and utility service generally accessible by mo-bile devices such as, mobile phones, GPS devices, pocket PCs, and operating through a mobile network. A LBS can offer many services to the users based on the geographical position of their mobile device. The services provided by a Location Based Server are typically based on a point of interest.

A database By retrieving the Points Of Interest 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. In recent years there has been a dramatic increase in the number of mobile devices querying location servers for information about POIs.

A challenge barriers to the wide deployment of such application, privacy assurance is a major issue. For instance, users may feel reluctant to disclose their locations to the LBS, because it may be possible for a location server to learn who is making a certain query by linking these locations with a residential phone book database, since users are like to perform many queries from home. The Location Based Server, which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the Location Server would not disclose any information without fees. Therefore the LBS has 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.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things are satisfied, then next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

A. Location Based Service

Location based service 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. A LBS can offer many services to the users based on the geographical position of their mobile device. The services provided by a 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.

B. Private Information Retrieval

In cryptography, a private information retrieval (PIR) protocol allows a user to retrieve an item from a server in possession of a database without revealing which item is retrieved. PIR is a weaker version of 1-out-of-n oblivious transfer, where it is also required that the user should not get information about other database items.

III. PROPOSED SYSTEM

In this paper, we propose a novel protocol for location based queries that have major performance improvements with respect to the approach by Ghinita at el and Like such protocol, our protocol is organized according to two stages. In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR, to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.

Our protocol thus provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage. In other words, users cannot gain any more data than what they have paid for. We also provide results from a working prototype showing the efficiency of our approach.

A. Architecture

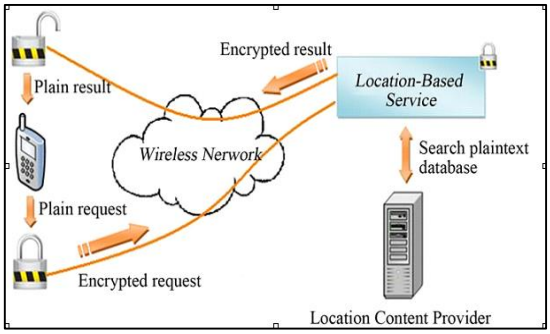

Fig. 1: System architecture.

B. Modules Descriptions

The users in our model use some location-based service provided by the location server LS. Each record describes a POI, giving GPS coordinates to its location (xgps, ygps), and a description or name about what is at the location. We assume that the mobile service provider SP does not interfere with the communications between the user and the location server. This means that the mobile service provider does not collude with the location server to attack the privacy of the user. As a consequence of this assumption, the user is able to either use GPS (Global Positioning System) or the mobile service provider to acquire his/her coordinates. Since we are assuming that the mobile service provider SP is trusted to maintain the connection, we consider only two possible adversaries. One for each communication direction. We consider the case in which the user is the adversary and tries to obtain more than he/she is allowed. Next we consider the case in which the location server LS is the adversary, and tries to uniquely associate a user with a grid coordinate.

IV. Algorithm

A. Initialization

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. The user also decides on the accuracy of this cloaking region by how many cells are contained within it, which is at least the minimum size defined by the server. This information is combined to form the public grid P and submitted to the location server, which partitions its records or superimposes it over pre-partitioned records. This partition is denoted Q (note that the cells don't necessarily need to be the same size as the cells of P). Each cell in the partition Q must have the same number rmax of POI records. Any variation in this number could lead to the server identifying the user. If this constraint cannot be satisfied, then dummy records can be used to make sure each cell has the same amount of data. We assume that the *LS* does not populate the private grid with misleading or incorrect data, since such action would result in the loss of business under a payment model.

Algorithm 1 *Initialisation*

Input: $X_{1,1},...,X_{m,n}$, where $X_{i,j} = ID_{Q_{i,j}} || k_{i,j}$
Output: $Y_{1,1},...,Y_{m,n}$

1: $K_{i,j} \leftarrow K_{i,j} = g_0^{g_1^{R_i} g_2^{C_j}}$, for $1 \leq i \leq n$ and $1 \leq j \leq m$, where R_i and C_j are randomly chosen
2: $Y_{i,j} \leftarrow X_{i,j} \oplus H(K_{i,j})$, for $1 \leq i \leq n$ and $1 \leq j \leq m$, where H is a fast secure hash function
3: **return** $Y_{1,1},...,Y_{m,n}$ {Encryptions of $X_{1,1},...,X_{m,n}$ using $K_{i,j}$}

Fig. 2: Algorithm

B. Oblivious Transfer Based Protocol

The purpose of this protocol is for the user to obtain one and only one record from the cell in the public grid P. We achieve this by constructing a 2-dimensional oblivious transfer, based on the ElGamal oblivious transfer, using adaptive oblivious transfer3 proposed by Naor et al. The public grid P, known by both parties, has m columns and n rows. Each cell in P contains a symmetric key ki,j and a cell id in grid Q i.e., (IDQi,j, ki,j), which can be represented by a stream of bits Xi,j . The user determines his/her i, j coordinates in the public grid which is used to acquire the data from the cell within the grid. The protocol is initialized.

C. Private Information Retrieval Protocol

The oblivious transfer based protocol there are 3 major steps: the user's query, the server's response, and the user decoding. The average time required for each of these major components are presented in Table IV. Based on these experimental results, most of time is taken by the generation of the user's query. This is due to the primality testing of Q0 and Q1. This requirement must be satisfied, otherwise . The average of the response time and the decoding time are much smaller in comparison. We assume that the server has much more computational power at its disposal. Hence, if there are many users, the server can use parallel processing to increase the throughput of the protocol. The main concern is keeping the query time for the user as low as possible, and on average the user query time is reasonable, given the amount of data that is exchanged in one round of the protocol.

Algorithm 3 *PIRProtocol*

Input: **User:**$ID_{Q_{i,j}}$
Output: **User:**C_i

1: **User** (*QG2*)
2: $\pi_0 \leftarrow \pi_i$, where π_i is chosen based on the value of $ID_{Q_{i,j}}$
3: Generate random group G and group element g, such that π_0 divides the order of g
4: $q \leftarrow |\langle g \rangle| / \pi_0$
5: $h \leftarrow g^q$
6: $Server \Leftarrow G, g$
7: **Server** (*RG2*)
8: $g_e \leftarrow g^e$
9: $User \Leftarrow g_e$
10: **User** (*RR2*)
11: $h_e \leftarrow g_e^q$
12: $C_i \leftarrow log_h h_e$, where log_h is the discrete log base h
13: **return** C_i {The requested (encrypted) data}

Fig. 3: Algorithm

V. CONCLUSION AND FUTURE WORK

In this paper we presented a LBS query solution that employs two protocols that enables a user to privately determine and acquire location data. The first step is to for a user to privately determine person's location using oblivious transfer on a public sector. The second step is to involve a private information retrieval interaction that retrieves the record with high communication efficiency.

We are analysing the performance of our protocol and found it to be both computationally and communicationally more efficient than the solution by Ghinita which is the most recent solution. We are implementing a software prototype using a desktop machine and a mobile device. Future work will involve testing the protocol on many different mobile devices. The mobile result we provide may be different than other handset devices and software environments. Also, we have need to reducing the overhead of the primality test used in the private information retrieval based protocol. Additionally, the problem concerning the Location Server supplying misleading data to the client is also interesting. The Privacy preserving reputation techniques seem a suitable approach to address such a problem.

REFERENCES

[1] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino.
[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] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791.
[4] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468.
[5] A. Beresford and F. Stajano, "Location privacy in pervasive computing,"IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.
[6] M. R. Clarkson, A. C. Myers, and F. B. Schneider. Quantifying information flow with beliefs. Journal of Computer Security, 17(5):655–701, 2009.
[7] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacypreserving matching of spatial datasets with protection back ground knowledge,"in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12.
[8] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second- generation Onion router. In Proc. 13th USENIX Security Symposium, 2004.
[9] M. Duckham, L. Kulik, and M. F. Worboys. Imprecise navigation. 7(2):79–94, 2003.
[10] M. Duckham, K. Mason, J. Stell, and M. Worboys. A formal approach to imperfection in geographic information. Computers, Environment and Urban Systems,25:89–103, 2001.
[11] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh and J-M. Tang.Framework for security and privacy in automotive telematics. In Proc. 2nd International Workshop on Mobile Commerce, pages 25–32. ACM Press, 2002.
[12] F. Espinoza, P. Persson, A. Sandin, H. Nystr¨om, E. Cacciatore, and M. Bylund. GeoNotes: Social and navigational aspects of location-based information systems. In G. D. Abowd, B. Brumitt, and S. Shafer, editors, Ubicomp 2001: Ubiquitous Computing, volume 2201 of Lecture Notes in Computer Science, pages 2–17. Springer, 2001.
[13] General Assembly of the United Nations. Universal declaration of human rights. United Nations Resolution 217 A (III), December 1948

