Content-Protecting & Privacy-Preserving Location Based Quest

Terli Madhava Rao, Y.Divyabharathi, A.Atchyuta Rao
Gokul institute of technology and sciences

***Abstract* - In this paper we present a solution to one of the location-based query problems. 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. 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 by introducing a two stage approach, where the 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 present is efficient and practical in many scenarios. We implement our solution on a desktop machine and a mobile device to assess the efficiency of our protocol. We also introduce 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.**

I. EXISTING SYSTEM

The Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the LS 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.

Disadvantages of Existing System

- Among many challenging barriers to the wide deployment of such application, privacy assurance is a major issue
- The user can get answers to various location based queries,

II. PROPOSED SYSTEM

In this paper, we propose a novel protocol for location based queries that has 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 remark that this paper is an enhancement of a previous work.

Advantages of Proposed System

- Redesigned the key structure.
- Added a formal security model. The privacy issue which is available in existing system, will be solved here.
- Implemented the solution on desktop machine.

System Architecture

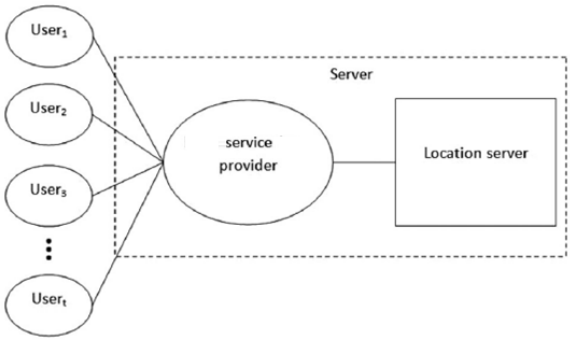

Fig 1

III. SYSTEM MODEL

The system model consists of three types of entities (see above figure): the set of users1 who wish to access location data *U*, a mobile service provider *SP*, and a location server *LS*. From the point of view of a user, the *SP* and *LS* will compose a server, which will serve both functions. The user does not need to be concerned with the specifics of the communication.

The users in our model use some location-based service provided by the location server *LS*. For example, what is the nearest ATM or restaurant? The purpose of the mobile service provider *SP* is to establish and maintain the communication between the location server and the user.

We reasonably assume that the mobile service provider *SP* is a passive entity and is not allowed to collude with the *LS*. We make this assumption because the *SP* can determine the whereabouts of a mobile device, which, if allowed to collude with the *LS*, completely subverts any method for privacy. There is simply no technological method for preventing this attack. 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. SECURITY MODEL

Definition 1. (*k* out of *N* adaptive oblivious transfer ($OT^N_{k\times1}$)). *$OT^N_{k\times1}$ protocols contain two phases, for initialization and for transfer. The initialization phase is run by the sender (Bob) who owns the N data elements $X_1, X_2, \ldots, X_N$. Bob typically computes a commitment to each of the N data elements, with a total overhead of O(N). He then sends the commitments to the receiver (Alice). The transfer phase is used to transmit a single data element to Alice. At the beginning of each transfer Alice has an input I, and her output at the end of the phase should be data element X_I. An $OT^N_{k\times1}$ protocol supports up to k successive transfer phases.*

Oblivious Transfer Phase

1) *QueryGeneration* (*Client*) (QG1): Takes as input indices *i, j*, and the dimensions of the key matrix *m, n*, and outputs a query Q_1 and secret s_1, denoted as $(Q_1, s_1) = QG_1(i, j, m, n)$.
2) *ResponseGeneration*1(*Server*) (RG1): Takes as input the key matrix $\boldsymbol{K_{m\times n}}$, and the query Q_1, and outputs a response R_1, denoted as $(R1) = RG_1(K_{m\times n}, Q_1)$.
3) *ResponseRetrieval* (*Client*) (RR1): Takes as input indices *i, j*, the dimensions of the key matrix *m, n*, the query *Q*1 and the secret s_1, and the response R_1, and outputs a cellkey ki,j and cell-id IDi,j, denoted as $(ki,j, IDi,j) = RR_1(i, j, m, n, (Q1, s_1), R_1)$.

Private Information Retrieval Phase

4) *QueryGeneration*2 (*Client*) (QG2): Takes as input the cell-id IDi,j, and the set of prime powers *S*, and outputs a query *Q*2 and secret *s*2, denoted as $(Q2, s2) = QG2(IDi,j, S)$.
5) *ResponseGeneration*2 (*Server*) (RG2): Takes as input the database *D*, the query *Q*2, and the set of prime powers *S*, and outputs a response *R*2, denoted as $(R2) = RG2(D, Q2, S)$.
6) *ResponseRetrieval*2 (*Client*) (RR2): Takes as input the cell-key ki,j and cell-id IDi,j, the query *Q*2 and secret *s*2, the response *R*2, and outputs the data *d*, denoted as $(d) = RR2(ki,j, IDi,j, (Q2, s2), R2)$.

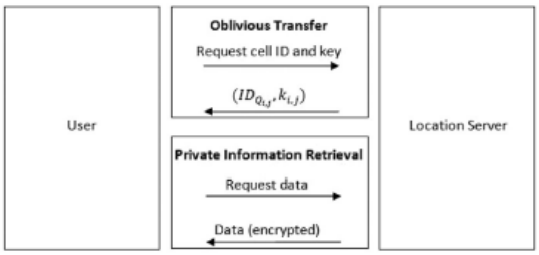

Fig. 2. High level overview of the protocol.

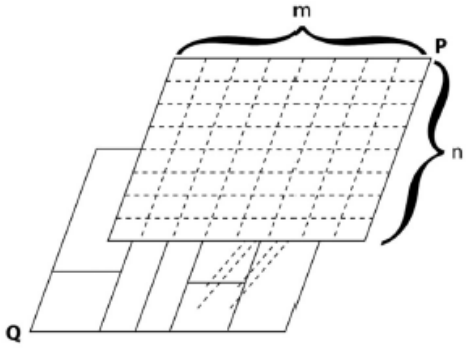

Fig. 3. Public grid superimposed over the private grid.

V. PROTOCOL DESCRIPTION

Protocol Summary

The ultimate goal of our protocol 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. We achieve this by applying a two stage approach shown in Fig. 2. The first stage is based on a two-dimensional oblivious transfer and the second stage is based on a communicationally 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. The user determines his/her location within a publicly generated grid *P* by using his/her GPS coordinates and forms an oblivious transfer query2. The minimum dimensions of the public grid are defined by the server and are made available to all users of the system. This public grid superimposes over the privately partitioned grid generated by the location server's POI records, such that for each cell *Qi,j* in the server's partition there is at least one *Pi,j* cell from the public grid. This is illustrated in Fig. 3.

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. Assuming the server has initialized the integer *e*, the user *ui* and *LS* can engage in the following private information retrieval protocol using the *IDQi,j* , obtained from the execution of the previous protocol, as input. The *IDQi,j* allows the user to choose the associated prime number power πi, which in turn allows the user to query the server.

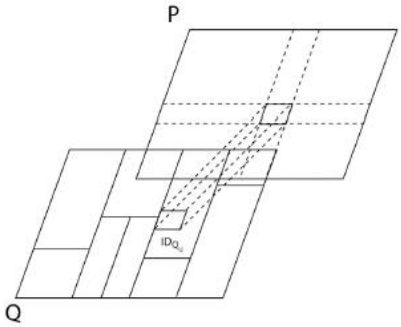

Fig. 4. Association between the public and private grids.

Client's Security

Fundamentally, the information that is most valuable to the user is his/her location. This location is mapped to a cell *Pi,j*. 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.

Server's Security

Intuitively, the server's security requires that the client can retrieve one record only in each query to the server, and the server must not disclose other records to the client in the response. Our protocol achieves the server's security in the oblivious transfer phase, which is built on the Naor-Pinkas oblivious transfer protocol.

VI. CONCLUSION

In this paper 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 oblivious transfer on a public grid. The second step involves a private information retrieval interaction that retrieves the record with high communication efficiency. We analysed the performance of our protocol and found it to be both computationally and communicationally more efficient.

We implemented a software prototype using a desktop machine and a mobile device. The software prototype demonstrates that our protocol is within practical limits. Future work will involve testing the protocol on many different mobile devices. The mobile result we provide may be different than other mobile devices and software environments. Also, we need to reduce the overhead of the primality test used in the private information retrieval based protocol. Additionally, the problem concerning the LS supplying misleading data to the client is also interesting.

Privacy preserving reputation techniques seem a suitable approach to address such problem. A possible solution could integrate methods. Once suitable strong solutions exist for the general case, they can be easily integrated into our approach.

VII. REFERENCES

[1] (2011, Jul. 7) *Openssl* [Online]. Available: http://www.openssl.org/

[2] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," in *Proc. CRYPTO*, 1990, pp. 547–557.

[3] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.

[4] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in *Proc. 2nd VDLB Int. Conf. SDM*, W. Jonker and M. Petkovic, Eds., Trondheim, Norway, 2005, pp. 185–199, LNCS 3674.

[5] 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.

[6] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *J. ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[7] M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," *Trans. Data Privacy*, vol. 3, no. 2, pp. 123–148, 2010.

[8] 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.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[10] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proc. ICDCS*, Columbus, OH, USA, 2005, pp. 620–629.

[11] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in *Proc. ICALP*, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.

[12] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in *Proc. Adv. Spatial Temporal Databases*, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.

[13] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," *GeoInformatica*, vol. 15, no. 14, pp. 1–28, 2010.

[14] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in *Proc. ACM SIGMOD*, Vancouver, BC, Canada, 2008, pp. 121–132.