Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.762 – 769

RESEARCH ARTICLE

SUSTENTATION OF USER INFORMATION RETRIEVAL WITH PRIVATE GRID USING LOCATION BASED SERVICES

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

[*1]Mtech Scholar, Department of Information and Technology
Hindustan University, Chennai, Tamilnadu, India
adorinit05@gmail.com

[*2]Assistant Professor, Department of Information and Technology
Hindustan University, Chennai, Tamilnadu, India
dwarakanath@hindustanuniv.ac.in

Abstract ---With mobile phones becoming first-class citizens in the online world, the rich location data they bring to the table is set to revolutionize all aspects of online life including content delivery, recommendation systems, and advertising. It is argued that even if the user identity is not explicitly released to the service provider, the geo-localized history of user-requests can act as a quasi-identifier and may be used to access sensitive information about specific individuals. . 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.

Index Terms---Location based query, point of Interest, private query, Private information retrieval

1. INTRODUCTION

The popularity of mobile devices with localisation chips and ubiquitous access to Internet give rise to a large number of location based services (LBS). Consider a user who wants to know where the nearest gas station is. He sends a query to a location-based service provider (LBSP) using his smart-phone with his location attached. The LBSP then processes the query and responds with results. Location-based queries lead to privacy concerns especially in cases when LBSPs are not trusted. "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.

As LBS is a developing technology, users might not be aware of the risks that it poses. New types of smart mobile devices enabled the emergence of Location-Based Services (LBS). A user of the service carries a mobile device that obtains its location via GPS or a Wireless Local Area Network (WLAN).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.

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 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. Location privacy is mandatory for every user to keep their location confidential .Every user needs to maintain the privacy level according to their spatial and temporal region. While the LBS helps users reach places or people easily, private information of users could be disclosed to other people. As users do not want their locations and mobility patterns to be revealed to other ones, the aim is to prevent people from making an identity-location binding. Identity-location binding means that one is able to tell that a specific user has been to a specific location. Privacy protection is of great importance for such service users in mobile and wireless networks. However, as mobile devices are highly autonomous and heterogeneous, it is challenging to design generic protection techniques and achieve high level of privacy protection.

2. RELATED WORK

The first solution to the problem was proposed by Beresford [2], in which 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 [10], [4]. The concept of k-anonymity was introduced as a method for preserving privacy when releasing sensitive records. This is achieved by generalisation and suppression algorithms to ensure that a record could not be distinguished from $(k-1)$ other records. The solutions for LBS use a trusted anonymiser to provide anonymity for the location data, such that the location data of a user cannot be distinguished from $(k - 1)$ other users. An enhanced trusted anonymiser approach has also been proposed, which allows the users to set their level of privacy based on the value of k. This means that, given the overhead of the anonymiser, a small value of k could be used to increase the efficiency.

New privacy metrics have been proposed that captures the users' privacy with respect to LBSs [5]. The authors begin by analysing 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 generalisation algorithms that coincide with the user's privacy requirements. As solutions based on the use of a central anonymiser are not practical, presented a scheme whereby a group of trusted users construct an ad-hoc network and the task of querying the LS is delegated to a single user. This idea improves on the previous work by the fact that there is no single point of failure. If a user that is querying the LS suddenly goes offline, then another candidate can be easily found. However, generating a trusted ad-hoc network in a real world scenario is not always possible.

3. PRODUCT PERSPECTIVE

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.

One popular cloaking technique is based on the principle of k-anonymity, where a user is hidden among k-1 other users. Queries from multiple users are typically aggregated at an anonymity server which forms an intermediary between the user and the LBS provider. This central anonymity server can provide spatial and temporal cloaking functions, so that an attacker will encounter difficulty matching multiple queries that are observed with users at particular locations and at particular points in time. Many cloaking solutions for location privacy suggest either a central anonymity server as describe or other means such as decentralized trusted peers or distributed k-anonymity.

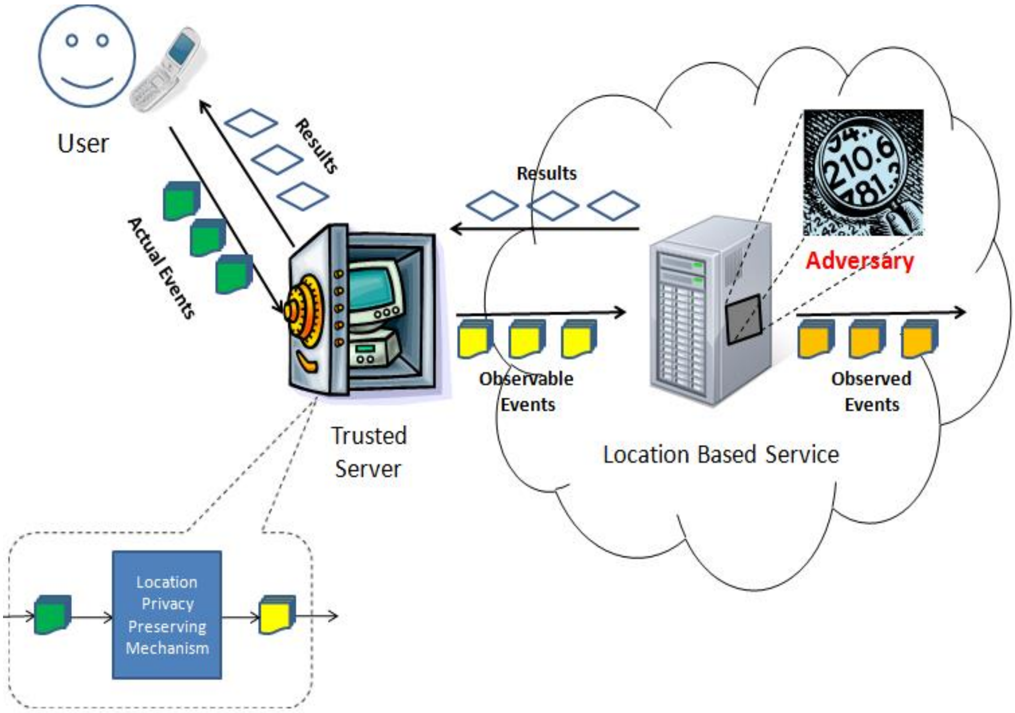


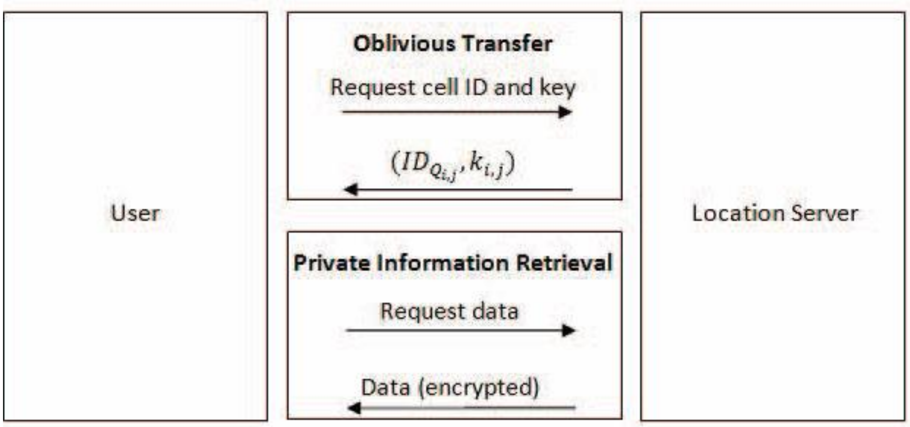
Fig 1: Communication between a user and a Location Based Service

4. 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. We proposed 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 communicationally efficient PIR. The oblivious transfer based phase 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 phase to obtain and decrypt the location data.



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

Fig 2: Architecture Diagram

4.1 CHARACTERISTICS OF USER CLASSES

A user u from the set of users U initiates the phase 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, whose size cannot be smaller than the minimum size defined by the location server. This is at least the minimum size defined by the server. This information is combined with the dimensions of the CR 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 ram 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 do not populate the private grid with misleading or incorrect data, since such action would result in the loss of business under a payment model.

5. IMPLEMENTATION

The server encrypts each record ri within each cell of Q, Qi,j , with an associated symmetric key ki,j . 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. Using the private partition Q, the server represents each associated (encrypted) data as an integer Ci, with respect to the cloaking region. For each Ci, the server chooses a set of unique prime powers πi = pci I, such that Ci < πi. We note that the ci in the exponent must be small forthe phase to work efficiently. Finally, the server uses the Chinese Remainder Theorem to find the smallest integer e such that e = Ci (mod πi) for all Ci. The integer e effectively represents the database. Once the initialisation is complete, the user can proceed to query the location server for POI records.

5.1 OBLIVIOUS TRANSFER

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 or (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.

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 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, 1 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.

K out of N adaptive oblivious transfer (OTNk×1**).**OTN k×1 phases contains two phases, for initialization and for transfer. The initialization phase is run by the sender (Bob) who owns the N data elements X1, X2... XN. 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 XI. An OTNk×1 protocol supports up to k successive transfer phases.

OBLIVIOUS TRANSFER PHASE

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).

5.2 PRIVATE INFORMATION RETRIEVAL

In the PIR phase 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 congruences.

Once the database has been initialised, the user can initiate the phase 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 "semi safe" 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.

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 phase with the location server to acquire the encrypted POI data. 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 phase.

PRIVATE INFORMATION RETRIEVAL PHASE

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).

6. EXPERIMENTAL RESULTS

We implemented our location based query solution on a platform consisting of a desktop machine, running the server software of our phase, and a mobile phone, running the client software of our phase.

For both Platforms, we measured the required time for the oblivious transfer and private information retrieval phase separately to test the performance of each protocol and the relative performance between the two phases.

The implementation on the mobile phone platform is programmed using the Android Development Platform, which is a Java-based programming environment. The mobile device used was a Sony X peria S with a Dual-core1.5 GHz CPU and 1 GB of RAM. The whole solution was executed for 100 trials, where the time taken (in seconds) for each major component.

	Average Time (s)	
Component	**Desktop**	**Mobile**
InitialisationOT	1.80959	_
Query Generation 1	_	0.00109
Response Generation 1	0.00979	_
Respons Retrieval 1	_	0.00004

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

	Average Time (s)	
Component	**Desktop**	**Mobile**
QueryGeneration2	—	23.90676
ResponseGeneration2	4.57147	—
ResponseRetrieval2	—	0.49323

Table 2: Private Information Retrieval experimental results for desktop and mobile platforms

In both phases solution, there are 3 major steps: the user's query, the server's response, and the user decoding. Table 1 displays the average runtime on the desktop and mobile platforms, for each component of the oblivious transfer phase. Similarly, Table 2 presents the average times for each component of the private information retrieval protocol. This contributed to faster execution in the first stage.

7. CONCLUSION

In this project we 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.

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 phase

ACKNOWLEDGMENT

I thank the Lord Almighty who has been with me through every walk in my life, for guiding me and for the blessings showered on me to complete the project in successful manner. I convey my sincere thanks to my guide Mr.B.Dwasrakanath M.E., Assistant Professor, Department of Information Technology, Hindustan University who give her valuable guidance throughout and it is great privilege to express my gratitude to him.

REFERENCES

[1] “Openssl,” http://www.openssl.org/, 2011, [Online; accessed 7-July-2013].

[2] A. Beresford, F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46-55, 2012.

[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, “Privacypreserving 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] B. Hoh and M. Gruteser, “Protecting location privacy through path confusion,” Proc. *SecureComm’05*, 2005, pp. 194 - 205.

[10] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing location-based identity inference in anonymous spatial queries,” *IEEE T Knowledge and Data Engineering*, vol. 19, no. 12, pp. 1719 - 1733, 2007.

[11] M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” Proc. *CRYPTO’89*. 1990, pp. 547 - 557.

[12] H. Kido, Y. Yanagisawa, and T. Satoh, “An anonymous communication technique using dummies for location-based services,” Proc. *ICPS’05*, 2005, pp. 88 - 97.

[13] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, pp. 391 - 399, 2009.

[14] E. Kushilevitz and R. Ostrovsky, "Replication is not needed: single database, computationally-private information retrieval," Proc. *Foundations Computer Science*, 1997, pp. 364 - 373.

[15] L. Marconi, R. Pietro, B. Crispo, and M. Conti, "Time Warp: How Time Affects Privacy

[16] S. Mascetti and C. Bettini, "A comparison of spatial generalization algorithms for lbs privacy preservation," Proc. *2007 International Conference on Mobile Data Management*, 2007, pp. 258 – 262.

AUTHORS PROFILE

P.Adorin Rini received the B.Sc and M.Sc degree in Information Technology from Vivekananda Institute of Engineering and Technology College in 2010 and 2012.The areas of interest are Mobile Computing and Data Mining. She is currently pursuing her M.Tech in department of Information Technology in Hindustan University.

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.