Privacy Preserving Grid System for Location Based Queries

Priya.S[1] Shobana.D[2]
[1]Research Scholar [2]Assistant Professor
[2]Department of Information Technology
[1,2]Sri Krishna Arts & Science College, Bharathiyar University, Coimbatore, India

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. In the project we proposed 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. We propose a major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Advanced Symmetric key Transfer and the second step is based on Private Information based on Advanced Symmetric key Retrieval, to achieve a secure solution for both parties. The solution we present is efficient and practical in many scenarios. We implement the solution using a real cloud location server and android mobile application.

Key words: Location Based Service (LBS), Point of Interest (POI), Personal Information Retrieval (PIR)

I. INTRODUCTION

A 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.

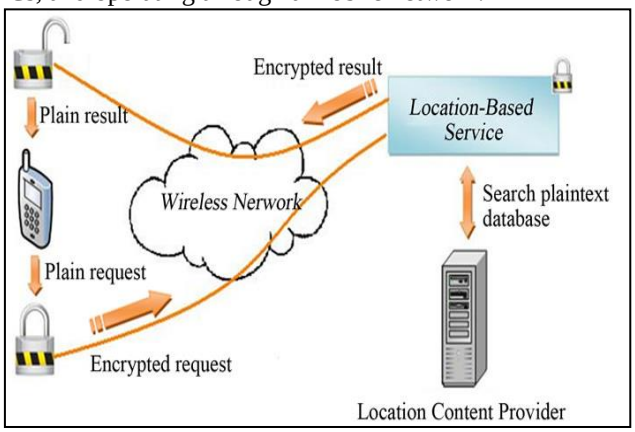

Fig. 1: Architectural diagram

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. In recent years there has been a dramatic increase in the number of mobile devices querying location servers for information about POIs. Among many challenging 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 likely to perform many queries from home. 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.

A. Related Work

In this paper, we propose a novel protocol for location based queries that have major performance improvements with respect to the approach. Like such protocol, our novel 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. In particular, the following contributions are made.

1) Redesigned the key structure
2) Added a formal security model
3) Implemented the solution on both a mobile device and desktop machine

As with our previous work, the implementation demonstrates the efficiency and practicality of our approach.

II. ALGORITHM

The request sent by the client will use the Advanced Symmetric encryption key to encrypt all the data. Further the connection between server and client will be secure.

All rights reserved by www.ijsrd.com

A. Advanced Symmetric key algorithm

Advanced Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption etc. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. Other terms for symmetric-key encryption are secret-key, single-key, shared-key, one-key, and private-key encryption. Use of the last and first terms can create ambiguity with similar terminology used in public-key cryptography.

B. Point of Interest(POI)

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.

III. PROTOCOL DESCRIPTION

We now describe our protocol. We first give a protocol summary to contextualize the proposed solution and then describe the solution's protocol in more detail.

A. 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 [26] and the second stage is based on a communicationally efficient PIR [11]. 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. Since PIR does not require that a user is constrained to obtain only one bit/block, the location server needs to implement some protection for its records. This is achieved by encrypting each record in the POI database with a key using a symmetric key algorithm, where the key for encryption is the same key used for decryption. This key is augmented with the cell info data retrieved by the oblivious transfer query. Hence, even if the user uses PIR to obtain more than one record, the data will be meaningless resulting in improved security for the server's database. Before we describe the protocol in detail, we describe some initialization performed by both parties.

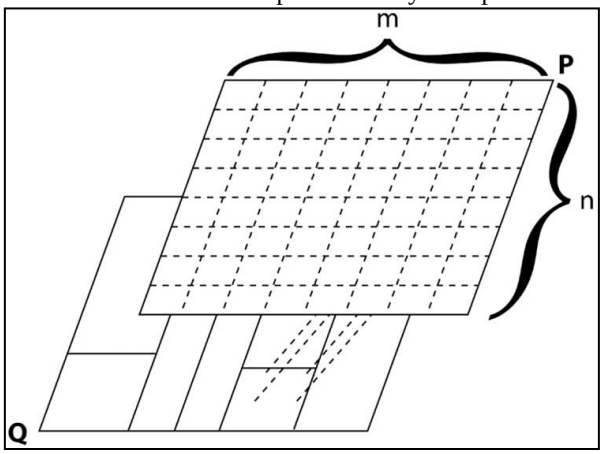

Fig. 2: Public grid superimposed over the private grid

B. 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, 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 repartitioned records (see Fig. 2). 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. Next, 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 $\pi i = pci\ i$, such that $Ci < \pi i$. We note that the ci in the exponent must be small for the protocol to work efficiently. Finally, the server uses the Chinese Remainder Theorem to find the smallest integer e such that $e = Ci \pmod{\pi i}$ for all Ci. The integer e effectively represents the database. Once the initialization is complete, the user can proceed to query the location server for POI records.

All rights reserved by *www.ijsrd.com*

IV. INTERFACE & PERFORMANCE

We are using two parameters for execution time one is encryption value and second is decryption time which is shown in table 1 and table 2 Here I am doing compare execution time of encrypting plaintext on different existing cryptographic algorithms with my proposed cryptography algorithm. In each cycle, same plaintexts are respectively encrypted by "Advanced Advanced Symmetric key Cryptography Algorithm using extended MSA method: DJSA Advanced Symmetric key algorithm", "Effect of Security Increment to Advanced Symmetric Data Encryption through AES Methodology" and "Proposed Algorithm (PA)" by copying them. Finally, the outputs of the evaluation system execution time, and measured in numeric form. Actually, for an encryption algorithm, the execution time of encryption not only depends on the algorithm's complexity, but also the key and the plaintext have certain impact. Result Comparison in Tabular Form: - In this I am going to represent our result in the form of table. After comparison the results that were obtained can be well represented in form of tables. Here, The Proposed Algorithm (with 265bit block size in this thesis) and "A new Advanced Symmetric key Cryptography Algorithm using extended MSA method: DJSA Advanced Symmetric key Cryptography Algorithm (with 128-bit block size) and "Effect of Security Increment to Advanced Symmetric Data Encryption through AES Methodology" algorithm (with 128-bit block size) have been implemented on a number of different data files like text, pdf and image varying types of content and sizes of a wide range. But here we are only showing result of text file.

Plain Text Size	DJSA algorithm	Data Encryption through AES Methodology	Proposed Algorithm
1.66 mb	0:01:34	0:01:32	0:01:25
560 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

Table 1: Encryption time comparisons of text files

Plain Text in Size	DJSA symmetric key algorithm	Data Encryption through AES Methodology	Proposed Algorithm
1.66 mb.txt	0:01:34	0:01:32	0:01:25
560 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

Table 2: Description time comparisons of text files

Encryption and Decryption time of Various Text files comparisons shown in table 1 and table 2 respectively.

graphical representation for the table 1 and table 2 is shown in figure 9 and figure 10 with blue line and orange line for encryption time and decryption time of "Advanced Advanced Symmetric key Cryptography Algorithm using extended MSA method: DJSA Advanced Symmetric key algorithm" and "Effect of Security Increment to Advanced 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 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

V. SECURITY ANALYSIS

In this section, 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.

A. 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. We will now describe both cases separately. In the oblivious transfer phase, each coordinate of the location is encrypted by the encryption scheme. In the private information retrieval phase, the security of the client is built on the Gentry-Ramzan private information retrieval protocol, which is based on the phi-hiding (φ-hiding) assumption. On the basis of the above security analysis, we can conclude with the following theorem.

Theorem 3: Assume that the ElGamal encryption scheme is semantically secure and the Gentry-Ramzan PIR has client security, our protocol has client security, i.e., the server cannot distinguish any two queries of the client from each other.

B. 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.

VI. PERFORMANCE ANALYSIS

We now analyze the performance of our solution and show that it is very practical. The performance analysis consists of the computation analysis and the communication analysis. We supplement this analysis with a comparison with the Protocol.

All rights reserved by *www.ijsrd.com*

A. Experimental Evaluation

We implemented our location based query solution on a platform consisting of: a desktop machine, running the server software of our protocols; and a mobile phone, running the client software of our protocols. For both platforms, we measured the required time for the oblivious transfer and private information retrieval protocols separately to test the performance of each protocol and the relative performance between the two protocols.

B. Experimental Results

In both phases of our solution, there are 3 major steps: the user's query, the server's response, and the user decoding. Table 3 displays the average runtime on the desktop and mobile platforms, for each component of the oblivious transfer phase. Similarly, Table 4 presents the average times for each component of the private information retrieval protocol.

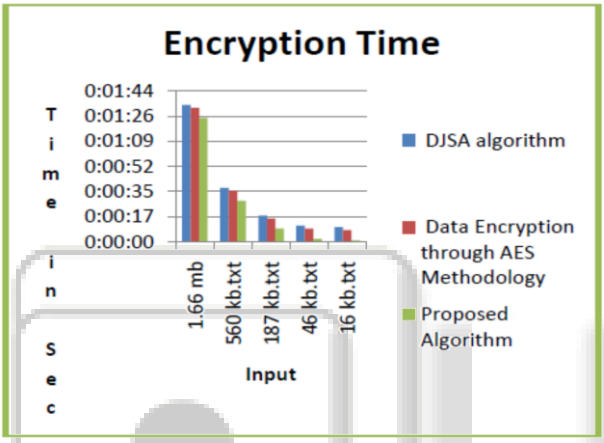

Fig. 3: Encryption time comparison of text files between various algorithms with proposed algorithm

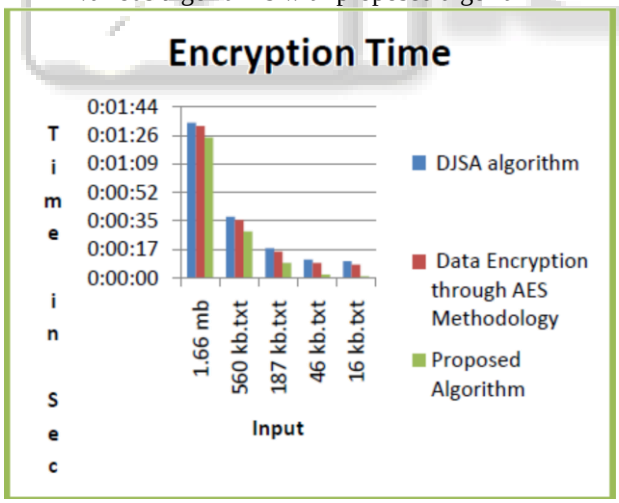

Fig. 4: Encryption time comparison of text files between various algorithms with proposed algorithm

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 through Proposed Algorithm is much smaller than encryption/decryption time for compared algorithms.

VII. 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.

ACKNOWLEDGMENT

This research was supported/partially supported by [Sri Krishna Arts and Science College]. I thankful to my guide {Shobana.D] who provided expertise that greatly assisted the research, although they may not agree with all of the interpretations provided in this paper.

References

[1] M. Gruteser and D. Grunwald, "Anonymous usage of location based services through spatial and temporal cloaking," in Proc. 1st Int. Conf. MobiSys, 2003, pp. 31–42.
[2] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," in Proc. 9th Int. Conf. UbiComp, Innsbruck, Austria, 2007, pp. 372–390.
[3] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in Proc. 1st Int. Conf. SecureComm, 2005, pp. 194–205.
[4] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.
[5] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. Int. Conf. ICPS, 2005, pp. 88–97.
[6] J. Krumm, "A survey of computational location privacy," Pers. Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, Aug. 2009.
[7] E. Kushilevitz and R. Ostrovsky, "Replication is not needed: Single database, computationally-private information retrieval," in Proc. FOCS, Miami Beach, FL, USA, 1997, pp. 364–373.
[8] L. Marconi, R. Pietro, B. Crispo, and M. Conti, "Time warp: How time affects privacy in LBSs," in Proc. ICICS, Barcelona, Spain, 2010, pp. 325–339.
[9] S. Mascetti and C. Bettini, "A comparison of spatial generalization algorithms for lbs privacy preservation," in Proc. Int. Mobile Data Manage., Mannheim, Germany, 2007, pp. 258–262.
[10] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in Proc. VLDB, Seoul, Korea, 2006, pp. 763–774.
[11] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791.
[12] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. EUROCRYPT, vol. 1592, Prague, Czech Republic, 1999, pp. 223–238.

All rights reserved by *www.ijsrd.com*

[13] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino, "Privacypreserving and content-protecting location based queries," in Proc. ICDE, Washington, DC, USA, 2012, pp. 44–53.
[14] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in Proc. ICDE, Hannover, Germany, 2011, pp. 494–505.
[15] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (corresp.)," IEEE Trans. Inform. Theory, vol. 24, no. 1, pp. 106–110, Jan. 1978.
[16] V. Shoup, (2011, Jul. 7). Number thoery library [Online]. Available: http://www.shoup.net/ntl/
[17] L. Sweeney, "k-Anonymity: A model for protecting privacy," Int. J. Uncertain. Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002.
[18] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," in Proc. CRYPTO, 1990, pp. 547–557.
[19] A. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.
[20] 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.
[21] 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.
[22] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," J. ACM, vol. 45, no. 6, pp. 965–981, 1998.
[23] 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.

All rights reserved by *www.ijsrd.com*