International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 5
May 2018

Privacy Preserving and Content Protecting Location Based Queries

P. Tara Kumari, Lorna Anna Burder*,G. Ravi Teja*, A. Pranay Varma***
** Assistant Professor, Department of Computer Science and Engineering, India
*Scholar, Department of Computer Science and Engineering, Hyderabad, India

ABSTRACT: *A solution is being given for a major problem that occurs with the location-based queries. The problem with this can be explained as i) when the user wants to know the details of a location which is known as Point of Interest (POI) and do not want everyone to know the location details because of their privacy worries, ii) The location data owner does not want to share the data to everyone's POI as he/she is the owner and want the control over it. A two-step solution is being proposed for this problem i.e., Step one is to find a secure solution for an Oblivious Transfer so that it is secure for both the parties, Step two is where the private information is sent to the user from the server. The utmost harmful problem can be solved using this security model that is being designed using DES encryption.*

KEYWORDS: location data, POI (Points of Interest), valid region (VR), location server

1. INTRODUCTION

The one which provide information regarding any services is known as a Location Based Services (LSB) which can be accessible from any hand-held devices that is connected to a network. The LSB has the database of the locations which plays a major role during the requested queries. The services are being given with the POI that is queried by the user and the result is being viewed with the help of Global Positioning System (GPS). The identification of the user must be secured so that their personal data and POI are not being misused. To secure the data it is being encrypted using AES. There are various resources that has to be spent by the server to gain the data. During the transmission of the data the server has to make sure that the information should not be misused by unauthorized users. This is the important reason about why we use this proposed security model.

2. RELATED WORK

The existing system is a live example that is being used within us. For example, if we want to know the location of a school which is at a particular place. The data for that particular school is easily known to anyone who has asked for it. We even find other locations which are close to the requested locations with their information. The reason for it can be on a genuine purpose or for misusing it. We miss the privacy for the data that has owner has given to the server. The data is being shared without any costing or security over it and the owner does not have a control over the data. The private information is being private here as the private data is being known to uncountable number of people with ease. We miss the security that has to be given to the private data of the owner. The owner no more feels his rights over the private data that he has as it is easily sharable. Transmission of the private information from the server to the user does not take much longer time. There is no record in the database about the number of people who have requested for the information. Security about the transmission of data is the major issue with the existing system.

3. DISADVANTAGES OF EXISTING SYSTEM

The disadvantages that we have with the existing system are:

- Privacy to the user is the major issue and the owners do not have any information about how many people have accessed his/ her information.
- The user can get a lot of suggested locations when asked for one.

4. PROPOSED SYSTEM

The proposed system is where the security for the private data is being given to the owner and a database is allotted where the information about the number of people accessing the data can be known to both the server and owner.

The step by step procedure of the proposed system can be explained below in brief:

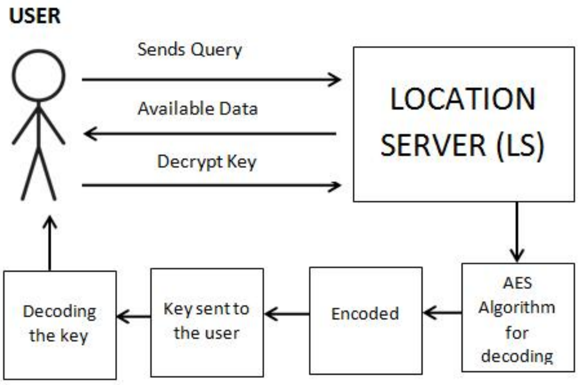
- The LBS will keep the locations in a particular database
- Users will have to register to access the data from the database which is being present.
- The user after registering can access the data from the database using a query which needs to have his/ her required location information.
- The selection of data by the user is done from the results the LBS has sent.
- The LBS will check if the data is available and sends a reply to the user if it is existing in the database.
- The LBS will check if the data is available and sends a reply to the user if it is existing in the database.
- The selection of data by the user is done from the results the LBS has sent.
- The Admin has the rights to activate or deactivate the account. If the user is retrieving the data for a genuine use then a security key is being sent to the user.
- The user has to activate his/ her account by decoding the Security Key that is received from the Admin.
- The Security key is sent in an encrypted form and even when the data is being hacked there is no use because it is sent it is encrypted

The system architecture consists of three types of entities: The set of users1 who wish to access location data U, a mobile service provider SP, and a location server LS. From the user view, the SP and LS together compose server, which serve all the functions. The user need not be concerned about the specifics of communication. A location based server is being used by the user which is provided by the location server LS. For example, the nearest Bus Bay. The purpose of mobile server provider SP is to establish and maintain the communication between the location server and the user.

5. ALGORITHM

R Tree algorithm:

R-trees can be more efficient for data storage and speed at search execution time, though they are generally tied to the internal structure of a given data storage system. R-trees are tree data structures used for spatial access methods, i.e., for indexing multi-dimensional information such as geographical coordinates, rectangles or polygons. A common real-world usage for an R-tree might be to store spatial objects such as restaurant locations or the polygons that typical maps are made of: streets, buildings, outlines of lakes, coastlines.



Grid index algorithm:

The individual cells of a grid system can also be useful as units of aggregation, for example as a precursor to data analysis, presentation, mapping, etc. A grid index is a used for spatial indexing purposes. A wide variety of such grids have been proposed or are currently in use, including grids based on "square" or "rectangular" cells, triangular grids or meshes, hexagonal grids, grids based on diamond-shaped cells, and possibly more. The range is broad and the possibilities are expanding.

Melkman's algorithm:

The Melkman's algorithm to compute the convex polygon of the updated EVR to remove the unnecessary vertices and achieve a larger region size. The convex polygon serves as the final updated EVR .

6. PROTOCOL MODEL

Before describing our protocol we introduce the system model, which defines the major entities and their roles. The description of the protocol model begins with the notations and system parameters of our solution.

6.1 Notations

Let $x \leftarrow y$ be the assignment of the value of variable y to variable x and $E \Leftarrow v$ be the transfer of the variable v to entity E. Denote the ElGamal [7] encryption of message m as E(m, y) = A = (A1, A2) = (gr , gmyr), where g is a generator of group G, y is the public key of the form y = gx, and r is chosen at random. This will be used as a basis for constructing an adaptive oblivious transfer scheme [8]. Note that A is a vector, while A1, A2 are elements of the vector. The cyclic group G0 is a multiplicative subgroup of the finite field Fp, where p is a large prime number and q is a prime that divides (p − 1). Let g0 be a generator of group G0, with order q. Let G1 be a multiplicative subgroup of finite field Fq, with distinct generators g1 and g2 where both have prime order q |(q − 1). Based on this definition, groups G0 and G1 can then be linked together and have the form g gx 1g y 2 0 , where x and y are variable integers. This will be used in our application to generate an ElGamal cryptosystem instance in group G1. We denote |p| to be the bit length of p, $\oplus$ to be the exclusive OR operator, a||b to be the concatenation of a and b, and |g|to be the order of generator g. We require for security reasons, that |q| = 1024 and p has the form p = 2q+ 1. We also require that the parameters G0, g0, G1, g1, g2, p, qbe fixed for the duration of a round of our protocol and be made publicly accessible to every entity in our protocol.

7. SECURITY MODEL

Definition 1.•(k out of N adaptive oblivious transfer (OTN k×1)). OTN k×1 protocols contain 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 OTN k×1 protocol supports up to k successive transfer phases.

7.1 Oblivious Transfer Phase

1) Query Generation (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) ResponseRetrieval (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 cellkey ki,j and cell-id IDi,j, denoted as (ki,j, IDi,j) = RR1(i, j,m, n, (Q1, s1),R1).

7.2 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 Q2 and secret s2, 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).

8. 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 analyzed the performance of our protocol and found it to be both computationally and communicational more efficient than the solution by Ghinita et al., which is the most recent solution. 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 primarily 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 from. Once suitable strong solutions exist for the general case, they can be easily integrated into our approach.

9. ACKNOWLEDGEMENTS

The authors express their gratitude towards the Institution for providing us this opportunity. We also are grateful to Dr. Raja M, Head of Department, Department of Computer Science & Engineering, St. Peter's Engineering College, Hyderabad, for supporting us throughout the research.

10. REFERENCES

[1] Paulet, R., Kaosar, M. G., Yi, X., &Bertino, E. (2014). Privacy-preserving and content-protecting location based queries. IEEE transactions on knowledge and data engineering, 26(5), 1200-1210.

[2] 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.

[3] D. Lee, B. Zheng, and W.C. Lee, "Data Management in Location Dependent Information Services," IEEE Pervasive Computing, vol. 1, no. 3, pp. 65-72, July Sept. 2002.

[4] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacywith mix-zones over road networks," in *Proc. ICDE*, Hannover,Germany, 2011, pp. 494–505.

[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]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.

[8] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in Proc. CRYPTO, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791.