VOL. 10, NO. 7, APRIL 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

LOCATION BASED QUERY SYSTEM BY SECURING PRIVATE INFORMATION

Farzana S. and Ramyadevi R.
Department of Computer Science and Engineering, Velammal Engineering College, Surapet, Chennai, India
E-Mail: Farza.yas92@gmail.com

ABSTRACT

Location based system are used for discovering the point of interests (POI)s from a specific location based search on the user queries. The GPS latitude and longitude is sent as an input to the location servers which is based on the GPS coordinate with the point of interests and the current location of user can be served back to the client from the location server. This issue is characterized as tails: (i) a user needs to inquiry a database of area information, known as Points Of Interest (POI) s, and would not like to uncover his/her area to the server because of security concerns; (ii) the manager of the area information, that is, the area server, would not like to just convey its information to all clients. The area server longings to have some control over its information since the information benefit for the location server. On the other concerns over how such possibly untrusted area servers can prompt client's private data revelation. This paper gives an exhaustive study of area based protection safeguarding, and present the different area security models and systems successful in the area anonymization based system.

Keywords: location based query, point of interest, private query, private information retrieval, oblivious transfer protocol.

1. INTRODUCTION

The amount of advanced mobile phones or cell phones is quickly expanding these days. As a result of the ubiquity of versatile system and the taking off patterns of distributed computing, so individuals can revel in the advantageous backgrounds offered by the cell phones and remote servers. One of the prominent administrations is LBS, in which clients can use the land data for picking up stimulation administrations. To engage Connection data uncovered by client versatility, we additionally consider the coordinates went to physical areas of clients in the information [4]. Since this data could be advantage got by GPS gadgets, it is henceforth alluded to as GPS areas. GPS areas assume a critical part in portable web seeks. For instance, if the client, who is searching down the data, from the location provider with service provider, here, we can see that the GPS areas, which is incorporated in the server.

To the best of our information a personalization schema is proposed in [3] that use a client's substance inclination and area inclination and the GPS areas in customizing query items. It was discovered that a noteworthy number of questions were area inquiries concentrating on area information [6]. With a specific goal to initialize the inquiries that concentrate on area data, were the various Location-based query system is included. An area based query framework for web records has been proposed in [1]. The latitude and longitude coordinates will acquired from the web data at the location point from its current location, where the framework makes a loop focused at the angle of the direction which misleads the user from varying data. A query search is related with a previous impression that points out the topographical zone of the client. The proposed work comprises of location data in which Servers can't mislead data with any dummies about the client's area from the inquiry history and the client's profiles, since the measure of movement has been mixed by client and the POIs data has likewise been encoded with respective method form the protocol.

2. RELATED WORK

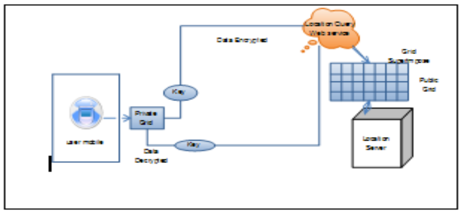
The first solution was proposed by comparing with the existing approaches to get the better result for previous problem. The privacy of the client is kept up by showing the variations of the client's name or alias inside some mix zone otherwise directing to the opposite direction. It could be shown that, because of the type of the information being exchanged between the client and the server, the changing of the client's name gives little assurance for the client's security but not the trustworthy. During the study of the mix zone approach has been connected to street navigation for the distributed customers. They explored the required number of clients to fulfill the unlinkability property where there rephrase the questions over an interim. This obliges watchful control of what number of clients is contained inside the mix zone, which is hard to accomplish in practice.

A correlative method to the mix zone approach is based around k-namelessness. The concept of k-secrecy was presented as a strategy for safeguarding security when admitting the fragile records. This is accomplished by generalization and concealment calculations to guarantee that a record couldn't be recognized from (k−1) different records. The report for this issue the LBS will utilize a trusted anon miser to give obscurity to the area information, such that the area information of a client can't be recognized from (k−1) different clients. An upgraded version of the trusted Anonymizer approach has likewise been proposed with new estimation technique, which permits the clients to set their level of security taking into account the estimation of k records. This implies that given overhead of the Anonymizer, has a little estimation of k records which could be utilized to build the proficiency. Alternatively, an extensive estimation method of k records could be decided to enhance the protection based on the history of the user query, in the event that the clients felt that their position information could be utilized malevolently. Picking a worth for k records, then again, it appears unnatural selection.

New protection measurements have been suggested that catches the clients' protection concerning LBS. The start of dissecting the inadequacies of basic k-namelessness in the connection of area inquiries. Next, they propose protection measurements that empower the clients to point out qualities that better match their inquiry protection necessities from their GPS coordinates with their current location. From these protection measurements they additionally propose spatial generalization for the calculations that correspond with the client's protection. Strategies have additionally been proposed to confound the user and mutilate the area information by giving different regions, it was designed for the trusted anonymiser for the gathering of the clients agreeing to a cloaking region (CR), therefore making it harder for the LS to recognize a single person for the user privacy. The same error with general CR methods is that there may exits some similar data about the layout of an area that roles out the client's area. A structure that comprises of a deviation that takes a client's profile, with alternate view. This thought enhances the existing work by the certainty that there is no single distraction. An alternate mechanism for maintaining a strategic distance from the utilization of a trusted Anonymizer is to utilize areas [5], [7]. The fundamental thought is to redistribute the area of the client by sending numerous irregular different areas to the server, such that the server can't recognize the exact area from the fake areas. The majority of the issues are tackled with the presentation of a private information retrieval (PIR). The essential thought is to utilize PIR to empower the client to inquiry the area database without trading off the protection of the inquiry of data without reviling its private information to the location server.

3. SYSTEM ARCHITECTURE

The framework model comprises of three sorts of elements the set of users1 who wish to get to area information of user location from location server, a portable administration supplier SP, and an area server LS. From the perspective view of a client, the service provider (SP) and location server (LS) will form a server, which will serve both parties. The client does not have to be concerned with the specifics of their correspondence. The clients in our model utilize some area based administration that given by the area server (LS). In this paper it utilizes the expression "client" to assign the element issuing inquiries and recovering inquiry results. The closest ATM or restaurant or nearby attractions. The motivation behind the administration supplier SP is to make and keep up the correspondence record between the area server and the client. The area server LS contain a set of POI records. Each one record contains a POI, giving GPS coordinates to its current location to its area (xgps, ygps), and a area name into the cell to check what is at the area which is plotted into cell with it id. Therefore it sensibly accept that the feasible administration supplier SP is a removed substance and is not permitted to connected with the LS.As a result of this pre assumption, the client can either utilize GPS or the versatile administration supplier to secure his/her coordinates. Since it is expected that the versatile administration supplier SP is trusted to keep up the association. Then it considers the case in which the client is to get more than he/she is permitted to access.



The working principle of the system is described with the help of an architecture diagram. The proposed work is using the smart phone with GPS integrated in it .In above fig User search the data location based on POIs an private grid will be generated internally with map in GPS of the device it is differentiated into two stage for preserving privacy of user data .Using oblivious transfer protocol it request for the cell id and key, cell id will be generated into rows and columns , user publicly determines his/her location in public grid .The second PIR is used to obtain only one record from cell in public grid p, the public grid is known by both the parties then PIR will request data and decrypt it using the same symmetric key, then association between the public and private grid takes place, user data is secured because the server unable to determine his/her location and unauthorised access is denied.

4. PROTOCOL DESCRIPTION

a) Protocol instantaneous

An objective of our protocol is to get a situated of POI records from the LS, which are near the client's position, without compromising the security of the client or at the server accomplish this by applying a two stage approach indicated. The primary stage is focused around a two-dimensional unaware exchange [8] and the second stage is focused around a communicationally effective PIR. The negligent exchange based convention is utilized by the client to acquire the cell ID, where the client is placed, and the comparing symmetric key.

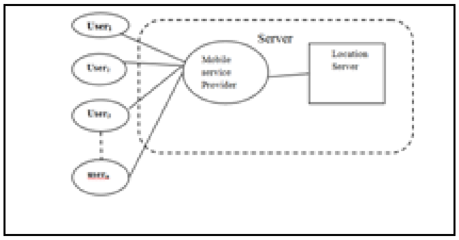


Figure-1. Scheme exemplary [8].

The user determines his/her location in publicly generated grid structure with respect to user current location, the constructed grid contains the cell each cell contains the random generated id and the symmetric key The information of the cell ID and the symmetric key is then utilized as a part of the PIR based convention to get and decode the area information. The base measurements of the general population framework are characterized by the server and are made accessible to all clients of the framework. The superimposition of public grid over the privately divided framework produced by the location server's POI records, such that for each one cell .PIR will used to encrypted data from the service provider. This is accomplished by encoding each one record in the POI database with a key utilizing a symmetric key calculation, where the key for encryption is the same key utilized for decoding.

b) Initialization

A client from the set of clients starts the convention handle by choosing a suitable square shading district CR, which holds his/her area. All client inquiries will be concerning this location district. The client chooses on the precise of this location district number of cells that contains inside it, any combination in this number could appear on the server distinguishing the client. On the other way that this obligation can't be fulfilled, then same records might be used to verify each one cell has the same measure of information.

The motivation behind this convention is for the client to get random one record from the cell.

c) Oblivious transfer phase

The function of this protocol is used for user to retrieve one and only record from public grid by obtaining the single cell from the grid this is achieved by constructing a 2-dimensional oblivious phase, the public grid is known by the both the parties, where each cell contains the unique is and symmetric key for acquiring the privacy for the user private data

d) Private information retrieval phase

The function of this phase is to gain the information about each cell which contained in the private grid, the user can initialize the private information from location server to acquire the encrypted POI data, by using this phase the user can decrypt and acquire the original data from the server.

5. IMPLEMENTATION AND RESULTS

In this segment, the security of the customer and the server is preserved while the customer would not like to surrender the protection of his/her area, to the server.

1. User queries

User will search for information asking for the Point of interest say a shopping mall nearby or any route from source to destination The location provider will return the point of interest to the user queries by displaying nearby attraction for given query. The server will return the data based on search with its GPS coordinates.

2. Location identification

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.

3. Configuring location privacy

The request sent by the client will use the symmetric encryption key to encrypt all the data. Further the connection between server and client will be secure. The server will also send all the information encrypted using the key sent by the client. The communication between client and server will be secure. The Client will never send the GPS coordinate but will send an information grid of its location. Client with help of the application will send the user grid cell information to the server and the security key to decrypt the data is by using same key then server will super imposed the user cell information with the server location grid and find the location server’s grid cell information. The server’s cell Information will be sent back to user. It just shows some nearest geographic position of user but does not show the exact location based on the movement of mobile device here the privacy is preserved.

6. CONCLUSIONS AND FUTURE WORK

In this paper we develop a secure solution for the location based query system by employing the two protocols which enables the user to privately acquire the location data, by the first step using oblivious transfer for the user to determine his/her location on a public grid, the second phase is used to retrieves the data from the LS using PIR phase. Thus the performance of the two stage protocol is efficient than the previous solutions has been analyzed. Thus executed a product model utilizing a desktop machine and a Smartphone’s, the product model exhibits that the protocol is within a practical confinement. Future work will simply by examining the protocol on various mobile devices. Thus the versatile result may be not quite same from other devices and application software domain. Likewise, the overhead of primality test is decreased by using the PIR phase. Moreover, the issue concerning the LS supplying mislead data to the customer is the additional attribute of this technique. Preserving privacy estimation techniques is suitable method to address such issue. A suitable result exists for the user query, they can be effectively implemented using real time applications.

REFERENCES

[1] M. Bellare and S. Micali. 1990. “Non-interactive oblivious transfer and applications,” in Proc. CRYPTO, pp. 547–557.

[2] A. Beresford and F. Stajano. 2003. “Location privacy in pervasive computing,” IEEE Pervasive Compute. Vol. 2, No. 1, pp. 46–55, January–March.

[3] X. Chen and J. Pang0 2012. “Measuring query privacy in location-based services,” in Proc. 2nd ACM CODASPY, San Antonio, TX, USA, pp. 49–60.

[4] B. Chor, E. Kushilevitz, O. Goldreich and M. Sudan. 1998. “Private information retrieval,” J. ACM, Vol. 45, no. 6, pp. 965–981.

[5] M. Duckham and L. Kulik. 2005. “A formal model of obfuscation and negotiation for location privacy,” in Proc. 3rd Int. Conf. Pervasive Computation., H. Gellersen, R. Want, and A. Schmidt, Eds., pp. 243–251, LNCS 3468.

[6] C. Gentry and Z. Ramzan. 2005. “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, pp. 803–815, LNCS 3580.

[7] H. Kido, Y. Yanagisawa and T. Satoh. 2005. “An anonymous communication technique using dummies for location-based services,” in Proc. Int. Conf. ICPS, pp. 88–97.

[8] Privacy-Preserving and Content-Protecting Location Based Queries Russell Paulet, Md. Golam Kaosar, Xun Yi and Elisa Bertino. 2014. Fellow, IEEE, IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 5, May.

[9] An anonymous communication technique using dummies for location-based services. Hidetoshi Kido. Pervasive Services, 2005. ICPS '05. Proceedings.

[10] MobiMix: Protecting location privacy with mix-zones over road networks. By Palanisamy, B. Coll. of Comput., Georgia Tech, Atlanta, GA, USA Ling Liu. Data Engineering (ICDE), 2011 IEEE 27th International Conference. pp. 494 – 505, 11-16 April 2011.

[11] Location-based Personalized Mobile Search. The 9th International Conference on Computer Science & Education (ICCSE 2014) August 22-24, 2014. Vancouver, Canada. By Kunhui Lin Software School of Xiamen, University Xiamen, China.

[12] Preserving User Location Privacy Based on Web Queries and LBS Responses. Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY 20-22 June 2007 by Calvert L. Bowen.

[13] Private Queries in Location Based Services: Anonymizers are not necessary by G Ghinita - 2008 work has been funded by NSF grant NSF-0742811.

[14].Protection of Query Privacy for ContinuouSLocation Based ServicesAniket Pingley∗, Nan Zhang∗, Xinwen Fu†, Hyeong-Ah Choi∗, Suresh Subramaniam∗, and Wei Zhao [8]

[15].Search Me If You Can: Privacy-preserving Location Query ServiceXiang-Yang Li‡ and Taeho Jung†NSF ECCS-1247944, [7]

[16].Farzana S., Ramya Devi R., Dr. V. vijayach-amundesswari. 2015.”A Survey on Location Based Query System” in 14 Th International Conference & International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Vol. 3, Issue-2, February. By IRAJ Research Forum, ISBN: 978-93-84209-55-1.