International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10101-10108

http://www.ripublication.com

Mobile Based Privacy Protected Location Based Services With Three Layer Security

[1]Lakshmi Praba.N,[2]Nancy.V,[3]Vigneshwari.S
[1,2,3]Department of Computer Science and Engineering, Faculty of Computing, Sathyabama University, Chennai,Tamilnadu, India
E-mail: [1]prabaviji21@gmail.com, [2]nanzy.jesi@gmail.com ,[3]vikiraju@gmail.com

Abstract

In Location Based Services(LBS), the queries are given by the users and retrieve their locations through tedious search. This process is more time consuming and the user gets confused with the pathway of the router. Android and Cloud Computing can be integrated to reduce the delay. The Android user makes a query to the cloud server and the data can be retrieved on the basis of a Geo tagged query. Here to check off the privacy profile is occurred.Our proposed system is tuned to preserve the privacy of the user's location. Three layer of security levels, namely, High, Medium and Low are used in the proposed system. Fuzzy C-mean clustering technique is used for clustering and filtering the query groups. Based on this framework, we propose a data model to increase the precariousness to position data. Also imprecise queries are used to hide the user's exact location and this yields probabilistic results.

Keywords: Location-based Service FCM (Fuzzy C-mean), Location Privacy, Data Clustering, FCM Three Layer Security, Ontology.

Introduction

The act of position technologies had passed through rapid growth in the recent period. Location-Based Services(LBS) determine the user locations accurately and modify a new class of applications[19]. Although LBS applications defend the commitment of refuge, facility and new business chances, where the quality to locate exploiters and item precisely also grow new concern in invasion of location secrecy. In accordance of location secrecy, the chances of preventing other parties from finding ones new or old localization. Upon utilizing places of domain, a work supplier can extract the users' whereabouts and discover her personal habits. There are many chances of selling users personal details to unknown users. Government agencies can observe the individual behavior of the user and they can also track the user visited locations. It is most important to prevent the place privacy from being invaded. Data clustering is the

activity of partitioning data elements into classes or clusters[20]. Product of same classes having same potential and product of various classes is as different as possible. To utilize clustering, the design and the data are needed. It needs various precautions to form a cluster using classes with the item. Some examples of measures which are used for clustering are intensitying, making connection and distance.

Related Work

Jan [3] discussed about mobile cloud using location based services(LBSs). It has cognitive growth in modern years, especially in investing quick improvements in mobile technology. Mobile devices are used by many people.LBS helps in protecting the user personal work details. They have a huge popularity on individual advertisements. LBS help in business activities to gain profit and development. Analysts aims at the gross income for location-based services to become higher from $2.8 billion in the year 2010 to $10.3 billion before the year of 2015 [1]. Beresford and Stajano[4] defined location privacy as "the power to forestall other users from educating one's current or past position". They also mentioned that the state of data intrusion on location privacy can be obtained by a system. In this section, we describe location-based services that protect location privacy. After that, we define location anonymity The general anonymous communication has several researches like Crews [5] and Onion Routing [6]. Some common queries like "Who conveys the information?, "Through where collection of information has upraised?", etc have to be analyzed. Yet, the state of information has incomprehensibility in location base that takes the details for location anonymity. The discussion about fetching a demand with better places of anonymity could be defined by location anonymity. Zang and Bollet[7] discussed that, every user using location services can protect their identity. Minimization of identity is useful for data at a particular point. A significant number of places is confused, in order to safeguard the identity of a person from sensing the places.

Ghinita et al[9], used a reciprocal of the framework using various features with highest spatial indices. This is done using a partitioning method. Zhu et al[10] discussed about LBS on a cloud. This is improved for mobile communication by holding cryptographic fictions. Verma[11], proposed that indoor positioning method is used in the modern LBS program in mobile connection with respect to another mobile operational system.Baburaj and Mary[13] defined a Genetic Algorithm for improving the user webpage recommendation.Mary[14] discussed about the implementation of E-Commerce for clients using products. Vigneshwari and Aramudhan[15] proposed user profiling ontologies for the users.Srikanth and Madialagan[16] proposed various effects and algorithms in search of query results from spatial collection of data.[17]They discussed about the usage of subspace and pattern-based clustering and also compared them to provide an appropriate result.

Materials and Methods

Fig. 1 shows the overall architecture of the proposed system. Here the user given query location is tracked and encrypted. Then the encrypted detail is stored in the server's database. Fig 2 describes the user location identification process in a detailed manner.The cloacking agent will get user location and then it will find whether the user is moving towards the location or moving outwards the location. The current location is obtained using Global Positioning System(GPS) from the mobile user. The mobile user will carry with the GPS for getting the longitude & latitude values. These values are obtained via satellite communication. So, once the user sends the query to the cloaking agent, now the cloaking agent will get the exact location of the user using GPS values of the user.

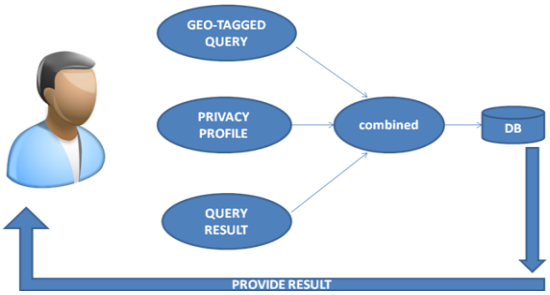

Figure 1: Architecture design for system

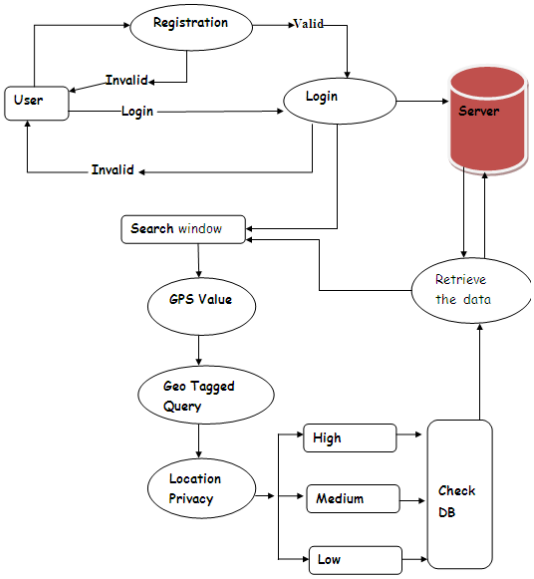

Figure 2: User Location Identification

Safe region manipulation

Whenever a cloaking agent receives a query from the client, it will check the query and find the safe region for the client. Safe region is calculated from the exact user

location. First we have to fetch the direction of the user. If the direction of the user is towards forward then the cloaking agent will calculate the safe region with respect to the main location. For example, user sends a request from Habibullah Road and then the user is moving towards the location of T.Nagar region, (both the regions are located in Chennai, Tamilnadu, India). Then, here the secure region is T.Nagar. If the user is moving in the opposite direction, then the cloaking agent will specify the safe region as Nungambakkam. After finding safe region, the cloaking agent will send the request to the Cloud server. The Cloud server will send the result for the safe region to the cloaking agent. Now, it wil find the nearest location from the result and send the location information to the client.

Query request to the cloud server

The cloaking agent manipulates the safe region for the client and the send the query to the Cloud server. The Cloud server checks the query and retrieve the results according to the safe region[22]. It then sends the result to the cloaking agent. If the user requested for ATM Bank from Habibullah Road, first the query is sent to the Cloaking Agent. Cloaking agent will manipulate the safe region as T.Nagar, then the query is forwarded to the Cloud Server.

Retrieval of results in accordance with safe region and ontology

Cloaking agent will send the query to the cloud server. The cloud server manipulates the user query and it will send the results to the cloaking server based on the area and ontology. The main cloud will retrieve the results with respect to the nearest place of the user, as well as the ontology process. Ontology is the study of relativities. Using ontology, cloud server can get relevant information and this information is also retrieved back to the user. If the query ‘Bank’ from the T.nagar location is safe, then the

FCM Three layer security

After getting the query result from the cloud server, the cloaking server will filter the results in accordance to the user’s exact location. The cloud server will retrieve the bank information or ATM, whichever is nearest to the user in accordance to T. Nagar to the cloaking agent, using Fuzzy C Means (FCM) clustering algorithm. So this technique fetches the current location and then, cluster the GPS value into three section security, which are high,low,medium. This helps the , user to find exact search location in a secured manner.The standard RSA algorithm[18] is used for encryption.

First layer(low level)

Low level (or)first layer consists of location privacy for the user.It helps in identifying the nearest place forward or else backward of user's exact position.For example, if the user types the query as a hotel, then through GPS it captures the exact location and fetches the nearest hotels to the user from the database server.

Second layer(middle level)
Middle level(or)second layer comprises of location privacy. It searches the query result, where the medium level is half the range of high security ranges. For example, if the user is in Usman road in T. Nagar, then the hub will be half the range around T.nagar from user location. It helps in avoiding the hacker, to track the exact location. For the medium security, the cost will be less than the high security.

Third layer(high level):
The third layer is included in the privacy settings. If the user gives the Query, it will cover the maximum area around the user and provides all the related query results. Users exact location is encrypted in the server, so that it becomes hard for the hackers to find out the exact location. The user has to pay more money in order to have a high profile, if the version is a paid version. Our proposal aims at providing a free service to high officials, military officers, businessmen, police officers.

The FCM technique is used for partitioning the elements $A=\{a_1,a_2...a_n\}$ with c fuzzy clusters. Finite number of data sets are given as inputs.The algorithm yields some 'c' clusters with 'V' centers. The details are given in equations 1 and 2[21].

$$X=x_i,\ i=1,2,....p \quad (1)$$

$$Y=y_{ij},\ i=1,.....p,j=1,....n \quad (2)$$

Here Y is the partition matrix, Y_{ij} is a numerical value in the range[0, 1] and it is said to be the degree of element a_j as the i-th cluster.Fuzzy Logic is implemented from the following description of FCM algorithm.

Step 1: In order to select clusters use $p(2\leq p\leq n)$.

Step 2: Function that has exponent weight can be selected using $w(1<w<\infty)$

Step 3: Select the starting point value matrix as Y^0.Then,ending value criterion τ
Also, fix the iteration pointing from l to 0.

Step 4: Compute centers$\{x_i^1 \mid i=1,2,...,p\}$ using Y^1 to find fuzzy clusters.

Step 5: $\{x_i^1 \mid i=1,2,...,p\}$ is used to find a separate fresher matrix Y^{i+1}

Step 6: Dividing the fresher matrix was computed by $del=\| Y^{i+1}-Y^1\|=max_{ij}|y_{ij}^{i+1} - y_{ij}^1$

Step 7: Suppose, $del> \tau$,we have to fix i =i + 1.

Step 8: Move to 4th step. Suppose $del \leq \tau$, we have to terminate the process.

This technique is applied to the GPS value .The cluster location which is greater than the current GPS value it assigned as high cluster. The GPS value lower than the current value is assigned to a lower cluster.

Results and Discussions

The impact of FCM techniques helps to easily filter the queries from the server and gives the query result quickly to the user.It provides the query result and divides the large data into smaller data sets.It is better than K-means algorithm.Using FCM technique in Android application reduces the time consumption. Without using the

FCM algorithm in Android, it will slow down the process of filtering the data from the database. It may take more time to fetch the result from the server to the user.

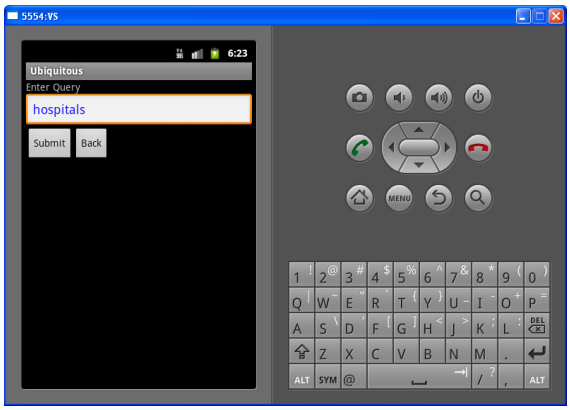

Figure 3: Query process to the server

This figure3 shows that the query is given by the user.Next, the user has to choose either forward or backward from the exact location.

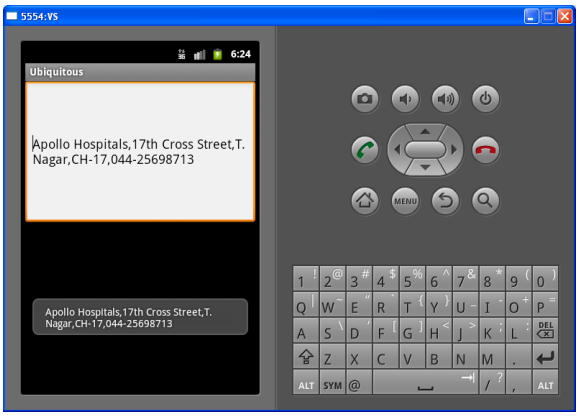

Figure 4: Query result from the database

This figure4 shows that,after the query process,the server encrypts the user location.Next,query result is retrieved from the database.

Table 1: Tabulation of location based service time

Source	Destination	Distance covered(km)	LBS time(milliseconds)
Tnagar	Nungabakkam	3.1	5,40,000
Guindy	Adyar	5.7	7,20,000
Velachery	Guindy	4.5	7,20,000
Tnagar	Vadapalani	3.8	6,60,000
Royapuram	Paris	3.9	6,00,000

Table 2: Comparison table

Using FCM enabled LBS Time(ms)	Without using FCM enabled LBS(ms)
3,40,000	7,40,000
5,20,000	9,20,000
5,20,000	9,20,000
4,60,000	8,60,000
4,00,000	8,00,000

Table 2 gives the comparative values of FCM and without using FCM technique. Using FCM technique, the user can save the time.

Conclusion

This paper concludes that a set of ideas about LBS on mobile cloud based on three layers of security. It provides the privacy protection for the user. It facilitates the access control for the directions and validation process. So that hacker cannot identify the current search, spatial query of the user thanks to the FCM technique.

Refrences:

[1] Warrior, J., McHenry, E., McGee, K.: They know where you are. IEEE Spectrum 40(7) (2003) 20- 25

[2] Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking. In: Proc. 1st Intl. Conf. on Mobile Systems, Applications, and Services. (2003)

[3] Jan Ten Sythoff. Location-based services, market forecast, 2011-2015. Technical report, Pyramid Research, 2010.

[4] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing, 2(1):46–55,2003.

[5] D. Goldschlag, M. Reed, and P. Syverson. Onion routing for anonymous and private internet connections. Communications of the ACM (USA), 42(2):39–41, 1999.

[6] M. Reiter and A. Rubin. Crowds: Anonymity for web transactions.ACM Transactions on Information and System Security,1(1):66–92, June 1998.

[7] H. Zang and J. Bolot, "Anonymization of Location Data Does NotWork: A Large-Scale Measurement Study," Proc. 17th Ann. Int'l Conf. Mobile Computing and Networking, pp. 145-156, 2011.

[8] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," Proc. Seventh Int'l Conf. Pervasive Computing,pp. 390-397, 2009.

[9] G. Ghinita, K. Zhao, D. Papadias, and P. Kalnis, "A Reciprocal Framework for Spatial k-Anonymity," J. Information Systems,Vol. 35, no. 3, pp. 299-314, 2010.

[10] Yan Zhu,Di Ma,Dijiang Huang,changjun Hu,"Enabling Secure Location Based Services in Mobile Cloud Computing",MCC 13,Aug 12,2013,Hong Kong,china 2013 ACM 978-4503-2180-8/13/08.
[11] Nidhi Verma,"Determining the Algorithm for Location based services using Indoor Positioning Techniques",Volume 2,Issue 7,July 2012,ISSN:2277128X.
[12] J. Sythoff and J. Morrison, Location-Based Services: Market Forecast,2011-2015, Pyramid Research, 2011.
[13] S. Prince Mary and Dr.E.Baburaj, ,Journal of Computer Science 9(11);1589-1601,2013.
[14] S.Prince Mary and Dr.E.Baburaj,Genetic Based Approach To Improve E-Commerce Web Site Usability,Fifth International Conference on Advanced Computing,2013
[15] S.Vigneswari and Dr.Aramudhan,A Technique To user Profiling Ontology Mining And Relationship Ranking,Journal of Theoretical and Applied Information Technology,Vol.58 No.3 pp-635-640,Jan 2014.
[16] Srikanth S.R and Madialagan M.K,Concise Range Queries,International Journal on Information Sciences& Computing,Vol.7 No.1 January 2013.
[17] Debahuti Mishra,Shruti Mishra,Sandeep Kumar,Satapathy,Amiya Kumar Rath and Milu Acharya"A Comparative Study in Sub Space and Pattern Based Clustering",National Journal on Advance in Computing & Management,Vol.2,No.1,April 2011.
[18] Rinku Dewri and RamaKrishna Thurimella "Exploiting Service Similarity For Privacy in Location-Based Search Queries",IEEE Transactions on Parallel and Distributed Systems Vol.25, No.2, February 2014.
[19] Reynold Cheng. "Preserving User Location Privacy in Mobile Data Management Infrastructures", Lecture Notes in Computer Science, 2006
[20] Dewangan, Revati Raman. "Fuzzy Clustering Technique for Numerical and Categorical dataset", International Journal on Computer Science & Engineering/09753397, 20110102
[21] Chen, W, and Chai Quek. "GA-FRB : A Novel GA-Optimized Fuzzy Rule System", Intelligent Systems Technology and Applications Six Volume Set, 2002.
[22] Dan Lin. "Position transformation", Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS - SPRINGL 08 SPRINGL 08, 2008