ISSN 2395-1621

Oblivious and Secure Location Based Service

[#1]Mandar Angarkhe,[#2] Prathamesh Bajare,[#3] Raviandra Khandagale,[#4]Shreyash Waghunde

[1]mandar00a@gmail.com
[2]prathmeshnajare@gmail.com
[3]khandagale.ravindra999@gmail.com
[4]shreyash.waghunde@gmail.com

[#1234] Computer Department, JSPM NTC, Savitribai Phule Pune University, India

ABSTRACT

In today's tech-savvy world, a person can easily know his/her location by using electronic devices having GPS facility. It is possible for user to know all location dependent information like location of friends or Nearest Restaurant, whether or traffic conditions, by providing user's location to LBS. The extreme usages of mobile devices have made the creation of wireless networks easier and that can be used to exchange location based information. The privacy of the user could be in harmful, if the exchange of location information is done between entrusted parties. The first issue with existing protocol is that it doesn't support many different mobile devices and second issue is, Location Server (LS) may provide misleading data to user. So we are working on enhancement of this protocol

.

ARTICLE INFO

Article History

Received :12th February 2016

Received in revised form :

13th February 2016

Accepted :15th February , 2016

Published online :

17th February 2016

I. INTRODUCTION

location based service is a service accessible with electronic devices like mobile phones, pocket pc's, gps devices. mobile devices which are having positioning capabilities (e.g. gps) facilitate access to location based services which can provide the user's geo-spatial context information. vast numbers of users uses these services to retrieve points of interest from their current location.

but there are certainly many problems while lbs is concerned that it can collect and use large amount of information about the user for a various purposes. location information is sensitive and users don't want to share such information to untrustworthy lbs servers. because of the private information of users might be obtained by wide number of malicious adversaries. also, queries searched by the user may contain sensitive information about individuals, including health condition, lifestyle habits. so he/she may not want to disclose it to anyone. privacy concerns are expected to increase as lbs is becoming more popular. location privacy means privacy of data which is stored on server. so here assurance of privacy is major issue. on the other hand, location server has their own database which contains number of point of interest records. so server needs to prevent unauthorized user database access.

II.PROPOSED SYSTEM

Existing system contains two phases namely Oblivious Transfer and Private Information Retrieval. First user's GPS coordinates are determined and then user identifies private location using oblivious transfer. After obtaining cell id and related symmetric key from server, user enter query using private information retrieval and receive exact information from the database. This system gives convict the security for user as well as server.

By referring this research work done by intellectuals we are going to modify this system. Because of the user needs to provide location every time and in conformity with location user needs to enter query to the server. So there are excrescent steps to achieve exact information. So we are going to introduce system with multiple users in same public region will get information using single point.

Here we are going to take concept of generalization i.e. in a specific grid, there are multiple unknown users use point of interest. So for each user, he has to determine his location and send to the server. So we are going to make single point in the grid for communication with server using centroid. Using this, there is no need to the user to determine its location grid every time.

III.EXISTING SYSTEM

In the existing system there are two phases Oblivious Transfer Phase and Private Information Retrieval Phase**.**
THE existing system consisting of User(Client) and Location Server(Server),LSB server.

Oblivious Transfer Phase: The protocol is used for the user to obtain the cell-id. User sends query() to the Location Server, Location server sends cell id and symmetric key The public grid *P*, known by both parties, has *m* columns and *n* rows. Each cell in *P* contains a symmetric key and a cell id in grid *Q*. The user gets determination his/her coordinates in the public grid that is used to acquire the data from the cell within the grid.

Private Information Retrieval Phase: User sends point of interest data to server whereas after receiving the Location Server, process the data and send the response in encrypted format. Then using symmetric key user decodes the encrypted data.

System architecture

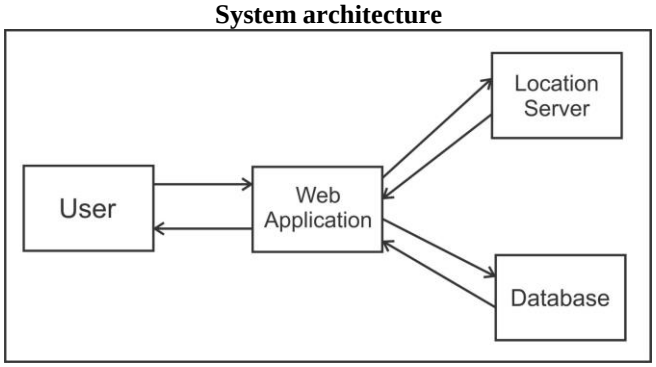

Fig. System Architecture

the proposed system consist user, web application, location server, database. user is the one who wants to get his/her point of intrest from location server. we are goiing to use the web application as an interface. this web based application can be accesd from stationary and moblie devices with the help of internet. location server is the one who accepts the query, process the data and send back to user. the database will contain information about point of interest, user information and admin information.

IV.CONCLUSION

In this paper we have done survey on Oblivious and Secure Location Based Queries. We have studied all the references by intellectuals for developing a protocol for both i.e. for user and server to assure their privacy. Nowadays to provide high level privacy for user and server in location based services is major necessity. Our proposed work shows that we are providing privacy to the number of users at a time and also confirm the safety of the contents stored on the server.

REFRENCES

[1] Russell Paulet, Md. Golam Kaosar, Xun Yi, and Elisa Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries" IEEE Transaction on Knowledge and Data Engineering, vol. 26, NO. 5, MAY 2014.

[2] A. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.

[3] 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.

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

[5] 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.

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

[7] 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.

[8] J. Krumm, "A survey of computational location privacy," Pers. Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, Aug. 2009.

[9] 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.

[10] 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.

[11] 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.

