Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Privacy Preserving and Content Protecting Location Based Queries

Mithila Bhandwalkar, Rohan Bhatia, Onkar Bhujbal, Akshata Shinde, Prof. B.B. Gite
Sinhgad Academy of Engineering, Savitribai Phule Pune University,
Maharashtra, India

Abstract – In this paper we present a solution to one of the location-based query problems. This problem is defined as follows: (i) a user wants to query a database of location data, known as Points Of Interest (POIs), and does not want to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. The location server desires to have some control over its data, since the data is its asset. We propose a major enhancement upon previous solutions by introducing a two stage approach, where the first step is based on Oblivious Transfer and the second step is based on Private Information Retrieval, to achieve a secure solution for both parties. The solution we present is efficient and practical in many scenarios. We implement our solution on a desktop machine and a mobile device to assess the efficiency of our protocol. We also introduce a security model and analyze the security in the context of our protocol. Finally, we highlight a security weakness of our previous work and present a solution to overcome it.

Keywords— POI, PIR, DES, LS, LBS.

I. INTRODUCTION

Location based Services (LBS) are those which provide information related to any field whether entertainment, utility services which can be easily accessible by mobile phones, tablets or any hand held device which is connected to a network. The LBS provides various services requested by the user with the help of their geographical position on the globe. The LBS is provided with a database as a backbone. By obtaining the Point of Interests (POI) from the server, the user will query the server by using their location. For example, a movie theatre located in the nearby area as the user. In this way, a user will use his/her own location so as to obtain the services from the user. While receiving such services from the user, the identity of the user as well as the data must be protected and secured. The data is secured in order to avoid it from being handed over to the unauthorized users. This can be achieved by encrypting the data. The Location Server (LS) has to spend its resources in order to retrieve the appropriate data for the user. Hence, the server does not offer services to the unauthorized users. This is the main, reason to advance the solution by encrypting the data. We have used DES for encryption of data. The proposed system provides a two-step process. In the first step, the user queries the server for a particular service using its location. The server then uses DES to encrypt the data and sends it to the user. In the second step, the server sends the decryption key to the user via an email gateway. Using this decryption key, the user decrypts data sent by the server and avails the service.

II. LITERATURE SURVEY

Location based mostly service (LBS) is associate degree info, entertainment and utility service. Typically accessible by mobile devices like, mobile phones, GPS devices, pocket PCs, and in operation through a mobile network. A LBS offers several services to the users supported the geographical position of their mobile device. The services provided by usually supported a degree of interest database. By retrieving the Points Of Interest (POIs) from the information server, the user will get answers to varied location based mostly queries, that embody however don't seem to be restricted to - discovering the closest ATM machine, petrol station, hospital, or station.

C. Bettini, X. Wang, and S. Jajodia [4]. They proposed a manuscript & we present a solution to one of the location predicated query quandaries. This quandary is defined as follows: (i) the user wants to query a database of location data, kenned as Points Of Interest (POIs) and is not willing to reveal his/her location to the server due to privacy concerns; (ii) the owner of the location data, that is, the location server, does not will to simply distribute its data to all the users. Here the location server wishes to have some control over its data, since the data is its asset. We recommend a major enhancement by using a two stage approach, wherein in the first stage according to the request of the user, the server encrypts the data and sends the data to the user as well as the decryption key via an email gateway and in the second stage, the user decrypts the data using the decryption key and receives the data in readable format.

III. PROPOSED SYSTEM

The following steps are carried out as follows:

i. The administrator of the server creates a database of the locations.

ii. The interested users register themselves with the server to avail the services.
iii. Besides having access to the database, the users can also add data to the server that can be beneficial to the other users.
iv. When the user wants to access data at the particular location, he/she has to send a query to the server which includes two parameters i.e. the type of data and his/her own co-ordinates.
v. The server then checks data at the user's given co-ordinates and sends the list of available data to the user.
vi. The user then selects the required data from the available list sent by the server.
vii. The requested data by the user is then encrypted by the server and sent to the user.
viii. The user then requests the server to send the decryption key for the data given by the server.
ix. The server then creates a .txt file including keys to decrypt the data sent to the user in the previous step.
x. The e-mail id used to send the .txt file is taken from the user and stored in the database at the time of user registration.
xi. This .txt file is then encoded and the key to decode this file is sent to the user via an email gateway.
xii. The user then uses this key to decode the .txt file and then uses the keys included in the .txt file to unlock the data.
xiii. Thus, we ensure that the data is inaccessible to the unauthorized users.
xiv. If during transmission, the data is hacked, it would still be in encrypted format and of no use to the hacker.

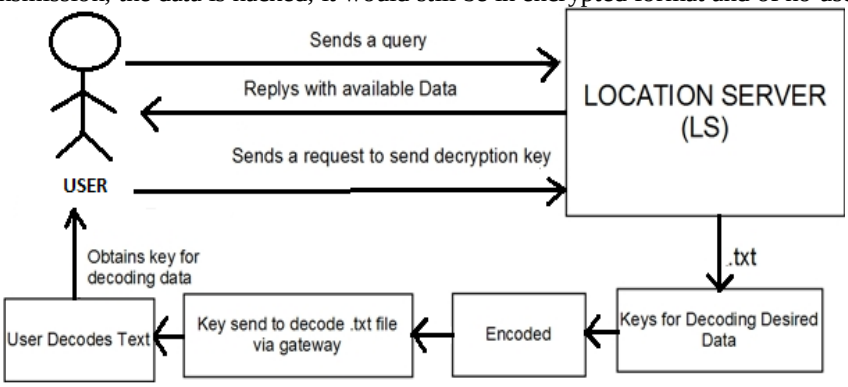

Figure I. Architecture of the system

IV. FUTURE SCOPE

In future, in case the data file is hacked by an unauthorized user, the details of the user can be obtained. These details can be reported in case of mishap in order to make a better system.

V. CONCLUSION

This system ensures that the data is preserved as well as protected from the unauthorized users. The two stage approach proposed in this system protects the privacy of the users and protects the content. Even if the data is hacked, it will be of no use due to the encoded format.

REFERENCES

[1] 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.
[2] B. Zheng, J. Xu, and D.L. Lee, "Cache Invalidation and Replacement Strategies for Location-Dependent Data in Mobile Environments," IEEE TranComputers, vol. 15, no. 10, pp. 1141-1153, Oct. 2002.
[3] B. Zheng and D.L. Lee, "Processing Location Dependent Queries in a Multi-Cell Wireless Environment," Proc. Second ACM Int'l Workshop Data Eng. for Wireless and Mobile Access, 2001.
[4] C. Bettini, X. Wang, and S.Jajodia, "Protecting the 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.
[5] B. Zheng, J. Xu, W.-C. Lee, and D.L. Lee, "On Semantic Caching and Query Scheduling for Mobile Nearest-Neighbor Search," Wireless Networks, vol. 10, no. 6, pp. 653-664, Dec. 2004.
[6] X. Gao and A. Hurson, "Location Dependent Query Proxy," Proc.ACM Int'l Symp. Applied Computing, pp. 1120-1124, 2005.

