ENHANCED SECURITY FOR CONTENT AND LOCATION BASED QURIES

VENKATA SAI PRAVATHI KUMARI PULUPULAM
Tech Student, Department of Computer Science, PBR Visvodaya Institute of Technology &Science
Email: saiparvathi.p1@gmail.com

THORAINELLORE MANJULA
Associate Professor, Department of Computer Science, PBR Visvodaya Institute of Technology & Science

ABSTRACT – *during this paper we have a tendency to gift an answer to at least one of the placement-based question issues. This downside is outlined as follows: (i) a user desires to question a information of location knowledge, called Points Of Interest (POIs), and doesn't wish to reveal his/her location to the server attributable to privacy concerns; (ii) the owner of the placement knowledge, that is, the location server, doesn't wish to easily distribute its knowledge to all or any users. The placement server wishes to possess some management over its data, since the information is its quality.We have a tendency to propose a significant sweetening upon previous solutions by introducing a 2 stage approach, wherever the primary step relies on Oblivious Transfer and therefore the second step relies on non-public info Retrieval, to attain a secure answer for each parties. The answer we have a tendency to gift is economical and sensible in several scenarios. We have a tendency to implement our answer on a desktop machine and a mobile device to assess the potency of ourprotocol. We have a tendency to additionally introduce a security model and analyze the safety within the context of our protocol. Finally, we highlight a security weakness of our previous work and gift an answer to beat it.*

Keywords— *POI, PIR, DES, LS, LBS.*

INTRODUCTION

The GPS location looking out service provided by mobile network on mobile devices like, mobile phones, GPS devices, pocket PCs square measure accustomed notice data, entertainment and utility service as per the peoples demand. LBS offer several services to the users supported the geographical position of their mobile device. The services provided by LBS square measure usually supported a degree of interest database.

By retrieving the Points of Interest (POI's) from the info server, the user will get answers to numerous location primarily based queries, that embody however don't seem to be restricted to discovering the closest ATM machine, petrol station, hospital, or station. In recent years there has been a dramatic increase within the range of mobile devices querying location servers for data regarding POI's. Among many challenging barriers to the wide readying of such application, privacy assurance may be a major issue. For example,users could feel reluctant to disclose their locations to the LBS, as a result of it should be attainable for a location server to be told who is creating a precise question by linking these locations with residential phone book info, since users square measure probably to perform several queries from home. The Location Server (LS), that offers some LBS, spends its resources to compile data regarding varied interesting

POI's. Hence, it's expected that the LS would not disclose any data while not fees. Thus the

LBS got to make sure that LS's information isn't accessed by any unauthorized user. Throughout the method of transmission the users shouldn't be allowed to find any data for which they need not paid. it's therefore crucial that solutions be devised that address the privacy of the users provision queries, but additionally forestall users from accessing content to that they do not have authorization.

LITERATURE SURVEY

Location based service (LBS) is degree data, amusement and utility service. Usually accessible by mobile devices like, mobile phones, GPS devices, pocket PCs, and operating through a mobile network. A LBS offersseveral services to the users supported the geographical position of their mobile device. The services provided by typically supported a degree of interest information. By retrieving the Points Of Interest (POIs) from the data server, the user will get answers to varied location based queries, that embody but do not appear to be restricted to - discovering the nearest ATM machine, service station, hospital, or station.C. Bettini, X. Wang, and S. Jajodia [4]. They projected a manuscript &amp; we tend to gift an answer to 1 of the placement predicated question quandaries. This quandary is outlined as follows: (i) the user needs to question a information of location knowledge, kenned as Points Of Interest (POIs) and isn't willing to reveal his/her location to the server because of privacy concerns; (ii) the owner of the placement knowledge, that is, the placement server, doesn't can to easily distribute its knowledge to any or all the users. Here the location server needs to possess some management over its knowledge, since the information is its plus. we tend to suggest a serious enhancement by employing a 2 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

PROPOSED SYSTEM

The following steps area unit distributed as follows:

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

ii. The interested users register themselves with the server to avail the services.

iii. Besides having access to the information, the users also can add knowledge to the server which will be useful to the opposite users.

iv. Once the user needs to access knowledge at the actual location, he/she must send a question to the server that includes 2 parameters i.e. the sort of knowledge and his/her own co-ordinates.

v. The server then checks knowledge at the user's given co-ordinates and sends the list of accessible knowledge to the user.

vi. The user then selects the specified knowledge from the accessible list sent by the server.

vii. The requested knowledge by the user is then encrypted by the server and sent to the user.

viii. The user then requests the server to send the decipherment key for the information given by the server.

ix. The server then creates a .txt file as well as keys to decipher the information sent to the user within the previous step.

x. The e-mail id accustomed send the .txt file is taken from the user and keep within the information at the time of user registration.

xi. This .txt file is then encoded and also the key to decrypt this file is distributed to the user via associate degree email entry.

xii. The user then uses this key to decrypt the .txt file and so uses the keys enclosed within the .txt file to unlock the data.

xiii. Thus, we tend to make sure that the information is inaccessible to the unauthorized users.

xiv. If throughout transmission, the information is hacked, it might still be in encrypted format and of no use to the hacker.

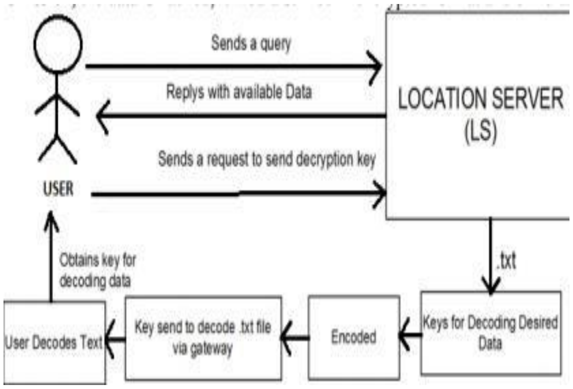
Sends a query
Replys with available Data
LOCATION SERVER (LS)
Sends a request to send decryption key
USER
Obtains key for decoding data
.txt
User Decodes Text
Key send to decode .txt file via gateway
Encoded
Keys for Decoding Desired Data

Figure-I. design of the system

CONCLUSION

In this paper authors have bestowed a location primarily based question solution that employs 2 protocols that allows a user to privately confirm and acquire location knowledge. the primary step is for a user to in camera confirm his/her location victimization oblivious transfer on a public grid. The second step involves a private data retrieval interaction that retrieves the record with high communication potency. Authors analyzed the performance of protocol and located it to be each computationally and communicationally a lot of economical than the solution by Ghinita et al., that is that the most up-to-date solution. Authors enforced a software system paradigm employing a desktop machine and a mobile device. The software system prototype demonstrates that protocol is at intervals sensible limits. Future work can involve testing the protocol on several different mobile devices. The mobile result that authors provide is also completely different than alternative mobile devices and software environments. additionally there's have to be compelled to cut back the overhead of the property check employed in the non-public data retrieval primarily based protocol.

REFERENCES

[1] M. Bellare and S. Micali, ”Non-interactive oblivious transfer and applications”, In Proc. CRYPTO, 1990, pp. 547ˆa557.

[2] A. Beresford and F. Stajano , ”Location privacy in pervasive computing”, IEEE Pervasive Comput., vol. 2, no. 1, pp. 46ˆa55, Jan.ˆaMar.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. 185ˆa199, LNCS 3674.

[4] 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.

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, ”Private queries in location based services: Anonymizers are not necessary”, in Proc. ACM SIGMOD, Vancouver, BC, Canada, 2008, pp. 121-132.

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

[7] B. Hoh and M. Gruteser,”Protecting location privacy through path confusion”, in Proc. 1st Int. Conf. SecureComm, 2005, pp. 194-205.

[8] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, ”Privacy preserving matching of spatial datasets with protection against background knowledge”, in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3-12.

[9] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, ”Preventing location-based identity inference in anonymous spatial queries”, IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719ˆa1733,Dec. 2007. [10] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, ”Private information retrieval”, Proc. Scientific and Statistical Database Management(SSDBM), 2007.

[11] G.R. Hjaltason and H. Samet, ”Distance Browsing in Spatial Databases ”, J. ACM, vol. 45, no. 6, pp. 965ˆa981, 1998.

[12] T. ElGamal, ”A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. Inform. Theory, vol. 31, no. 4, pp. 469ˆa472, Jul. 1985.

[13] R. Paulet, M. GolamKaosar, X. Yi, and E. Bertino, ”Privacy preserving and content-protecting location based queries”, in Proc. ICDE, Washington, DC, USA, 2012, pp. 44-53.

[14] V. Shoup, (2011, Jul. 7). Number theory library [Online], Available: http://www.shoup.net/ntl/.