ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Peer to Peer Privacy Preserving Query Service for location Based Service

Manoj T, Parry Siddharth V.M.M

U.G Student, Department of Information Technology, Panimalar Engineering college, Chennai, India

Assistant Professor, Department of Information Technology, Panimalar Engineering college, Chennai, India

ABSTRACT: Location-Based Service (LBS) becomes increasingly popular with the dramatic growth of smartphones and social network services (SNS), and its context-rich functionalities attract considerable users. Many LBS providers use users' location information to offer them convenience and useful functions. However, the LBS could greatly breach personal privacy because location itself contains much information. Hence, preserving location privacy while achieving utility from it is still an challenging question now. This paper tackles this non-trivial challenge by designing a suite of novel fine-grained Privacy-preserving Location Query Protocol (PLQP). Our protocol allows different levels of location query on encrypted location information for different users, and it is efficient enough to be applied in mobile platforms.

KEYWORDS: Servers,Privacy, Peer-to-peer computing, Protocols, Computer architecture, Security, Mobile nodes

I. INTRODUCTION

Location Based Service (LBS) has become one of the most popular mobile applications due to the wide use of smartphones. The smartphones, equipped with GPS modules, have powerful computation ability to process holders' location information, and this brought the flood of LBS applications in the smartphone ecosystem. A good example is the smartphone camera: if one takes a photo with a smartphone camera, the location where the photo is taken is embedded in the picture automatically, which helps one's remembrance. Furthermore, the explosive growth of social network services (SNS) also assisted its growth by constructing connections between location information and social network. When a picture taken by a smartphone (location embedded) is uploaded to the Facebook album, the system automatically shows the location of the picture on the map, and this is shared with the owner's friends in the Facebook (unless the privacy setting specifies otherwise). Many similar applications exploit both LBS and SNS. They offer several attractive functions, but location information contains much more information than barely the location itself, which could lead to unwanted information leakage.

A.Existing system

In Current Location based Service System there is a chance for affecting the user privacy user request directly hit to the location server with the exact user location so if any intruder want personal information about the user he can easily get by continuous monitor the user location, and also the point of interest of an user *B.Proposed system*

Our System would be user to protect the user privacy , as accessing location based service system without revel the user individual identity to location server. So that the location server may not know the user whom requesting the server for accessing the location service so, that the user privacy would be protected.

User privacy can be protected by using P2P network i.e. (Peer –to- Peer) Architecture. Peer to Peer would be added advantage as the individual identity of any user may not be revel to any third party server that user to protect the user privacy as each node communicate with each other but they need not to known to each other as group of mobile user in the particular locality form the group and generate the group id all the request will be hit from any centralize medium from the group the centralized medium would be change dynamically based in the user

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

II. RELATED WORK

There are several works achieving privacy-preserving location query [1]–[4], which are based on k-anonymity model. The k-anonymity model [5] has been widely used to protect data privacy. The basic idea is to remove some features such that each item is not distinguishable among other k items. However, relevant techniques which achieve k-anonymity of data cannot be used in our case for the following four reasons: 1) Those techniques protect the privacy of the data stored in servers. In our PLQP, we do not store the data at all.

III.MODULES

A.User Registration & Login

Initially user need to register their name in the app server by providing all the necessary detail , app server or location based server will not fetch any location based information to any user without user knowledge. User can login by providing the username and password that are given at the time of registration. When user login user would provide the user gps location i.e (Latitude and longitude) as user gps location cannot be send to server the locatio0n will be perform locally in the app based on the user latitude and longitude user profile will be change.

B.User Profile Generation

Once user login user need to set the profile by providing the location at which he need to change the setting profile name, profile location, Latitude and longitude at which the profile would be change. Setting parameter like Bluetooth, Wi-Fi, Sync ,Ringtone type and the user selected screen brightness . Once user update or add the profile then based on the mobile location or user gps position profile will automatically change.

C.Peer to Peer Network Formation

A Peer to Peer Formation can be done based on the number of user available on the region here Chennai is taken to be one region , any user that enter to the network would provide the detail as location he was present and type of place he interested and place he checked in.

D.User Recommendation

User Can login and Profile would be change based on the user location . User can access the service from location based server based on the user preference app would suggest the place for the user. But for these process also user location need to be protected as user will send as query to centralized medium for his location that query will be encrypted and send centralized medium will ask the server to process the query and provide the data reply back to the user the reply will be also done by using peer to peer so that the user may not be knows.

IV.SYSTEM ARCHITECTURE DIAGRAM

A.Architecture Diagram

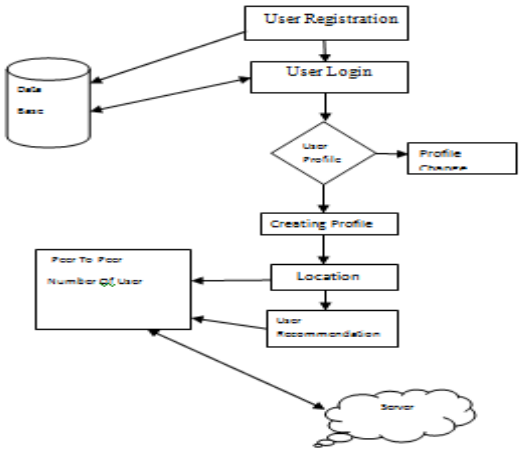

Fig.1 Architecture diagram for peer to peer privacy preserving querying system

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

We further assume that every user communicate with each other via an anonymized network (e.g., Tor: https://www.torproject.org) or other anonymized protocol ([16]) such that the privacy is not compromised by the underlying network protocol.

V. REQUIREMENTS

A. HARDWARE REQUIREMENTS

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the systems do and not how it should be implemented.

- Hard Disk : 500GB and Above
- RAM : 4GB and Above
- Processor : I3and Above
- Android Mobile

B. SOFTWARE REQUIREMENTS

The software requirements are the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team's progress throughout the development activity.

- Windows 7 and above
- JDK 1.8
- Servlet
- Tomcat 6
- NetBean 1.8

VI.CONCLUSION

In this paper, we proposed a novel method to protect location privacy not only for static local queries but also for dynamic global queries such as assignment queries. Our main contribution is the introduction of a location privacy-aware method. The proposed method does not require any trusted third party or intermediary. It uses square spiral encoding to provide privacy and to preserve some of the spatial properties. Our contributions may be summarized as follows: efficient implementation of capacity and coverage-constrained assignment query on outsourced databases; a novel spatial transformation strategy (square spiral encoding) to achieve privacy efficiently for approximate query results; and adapting the idea of the HG-tree [36], which is implemented for the Hilbert curves to the square spirals, and introducing the SS-tree.

REFERENCES

[1] T. Hashem and L. Kulik, "Safeguarding location privacy in wireless ad-hoc networks," Ubicomp 2007: Ubiquitous Computing, pp. 372–390, 2007.
[2] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against locationbased personal identification," Secure Data Management, pp. 185–199, 2005.
[3] M. Mokbel, C. Chow, and W. Aref, "The new casper: query processing for location services without compromising privacy," in Proceedings of the 32nd international conference on Very large data bases, VLDB Endowment, 2006, pp. 763–774.
[4] K. Vu, R. Zheng, and J. Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing." in IEEE INFOCOM, 2012.
[5] L. Sweeney et al., "k-anonymity: A model for protecting privacy," International Journal of Uncertainty Fuzziness and Knowledge Based Systems, vol. 10, no. 5, pp. 557–570, 2002.
[6] H. Zang and J. Bolot, "Anonymization of location data does not work: A large-scale measurement study," in Proceedings of the 17th annual international conference on Mobile computing and networking, 2011, pp. 145–156.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

[7] H. Kido, Y. Yanagisawa, and T. Satoh, "Protection of location privacy using dummies for location-based services," in 21st International Conference on Data Engineering Workshops, 2005, pp. 1248–1248.
[8] A. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004, pp. 127– 131.
[9] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J. Herrera, A. Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in Proceeding of the 6th international conference on Mobile systems, applications, and services, ACM, 2008, pp. 15–28.
[10] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in Proceedings of the 5th ACM workshop on Privacy in electronic society, 2006, pp. 19–28.
[11] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy." in IEEE INFOCOM 2012.
[12] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in Proceedings of 25th IEEE International Conference on Distributed Computing Systems, 2005, pp. 620–629.