ISSN 2348 – 9928
IJAICT Volume 3, Issue 11, March 2017 Doi:01.0401/ijaict.2017.03.08 Published on 05 (04) 2017

SECURED LOCATION SHARING SERVICES FOR SOCIAL NETWORKS

Prof. T. Arun kumar
Assistant professor

Ms. G. Sugandasree
UG Scholar

Mr. M. Muthukumar
UG Scholar

Mr. G. Ajay
UG Scholar

Ms. S. Sindhu
UG Scholar

Department of Computer Science and Engineering,
RVS College of Engineering and Technology,
Coimbatore, Tamilnadu, India

Abstract— Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. It requires a trusted third party that has access to the exact location of all users in the system or relies on expensive algorithms or protocols in terms of computational or communication overhead. To overcome these limitations, we propose an encryption technique ORE (Order Retrievable Encryption) for Social networking applications. 1) Allows a group of friends to share their exact locations without the need of any third party. 2) Achieves low computational and communication cost. 3) Supports dynamic location updates.4) Provides personalized privacy protection within a group of friends.

Keywords— Location Privacy, Location Sharing Services, Encryption Technique ,Location-Based Social Networking.

I. INTRODUCTION

Many Of the location based service providers provide service to users related to location by GPS enabled mobile devices or wireless communication. Recently, location-based services have been combined with online social networks. A common thing in location sharing services is that it allows user to discover the current location. e.g., Facebook's Places, Google Plus [1][2].

Existing location-based social networking systems with location sharing services rely on a central server which receives location information from all users in the system. The problem with this approach is that the central server can generate a detailed movement profile of each user. However, in some existing schemes, the central server still knows the user's approximate location [3][4].

Other schemes requires several messages to be exchanged not only between the user and the central server but also directly between the user and the user's friends and increasing the communication cost. In already existing Privacy-Preserving location sharing scheme is to protect the user location privacy against the central server, but they still allow the server to provide the user with the necessary services [6][7].

In this paper we propose the ORE encryption for social networking systems. The users send their location information in encrypted form to the database server. When a user wants to locate his/her friends the user logs onto the social networking system, sends a location query to the database server, and obtains the requested location information in encrypted form . The user then recovers the actual location of his/her friends from the encrypted information returned by the database server .The distinguishing characteristics are (1) Secure location privacy (2) Low computational and communication cost. (3)Efficient data updates. Our scheme supports highly dynamic location updates from individual users efficiently. (4) Personalized privacy within a group of friends. The database server handles queries, stores data received from users and sends data to users who are making queries without interfering with the data [8][9].

II. LITERATURE REVIEW

Mascetti et al. in uses three different protocols called SP Filtering, Hide&Seek and Hide&Crypt.
Hide &Seek starts a direct interaction between two users to get a more precise distance measurement. *Hide &Crypt* also requires direct interaction between users but uses secure computation to leak less information about the respective position of users [10].

Sik snys et al. present an approach based on encrypted grid indices Sik snys et al. present an approach based on encrypted Grid indices. Users share a list of grids with different levels each cell in a grid of a specific resolution can be mapped to a unique number through a one-to-one function such as AES. A server can then determine proximity by comparing these numbers, asking users to switch to a finer resolution if necessary .This requires

several rounds of communication when two users are close, making it more expensive in terms of communication [11][12].

Herrmann et al .makes use of identity-based broadcast encryption (IBE) to realize a location-sharing service that affords location privacy with respect to the central server. One version of the scheme shares the location with friends irrespective of their relative location, leading to more data being transferred than necessary [13].

III. PROBLEM DESCRIPTION

In this paper we have proposed a encryption technique to find the location of friends at any distance .The already existing methods have proposed only to a limited distance to find their friends location and need a centralized server to store the data's of all queries and to update the location .It does not update the location dynamically .It also needs a third party to access the location of all users in the system or by using an expensive algorithms or protocols and increase in communication and computational cost .

IV. PROPOSED METHODOLOGY

Personalized Privacy Region

We further improve the privacy of individual users in our PPLSS using the ORE or ORE-Index scheme by allowing them to define their personalized privacy regions. In the ORE and ORE-Index schemes described in respectively, the querying user u is theoretically free to choose a location marker at a considerably larger distance than is practical (e.g., 1000 km). The database server would return all friends in u's group within that distance, allowing u to learn their location even though there is no practical need to know their location at such large distances. Personalized privacy regions are an extension to the PPLSS which help prevent this situation, by allowing individual users to specify a maximum distance disprove up to which members of their groups are allowed to locate them .

Security Analysis

In our security model, we consider the database server as an adversary which tries to locate one user in a group of n users, all of which are mutually friends with each other. The group is denoted as G = {u1, u2, ・・・ , un} where the secret keys shared by the group members are (SKG, SKD). The adversary (i.e. the database server) has access to data received from all the members in G. It can also collude with eavesdroppers and all other users in the system who are not in G. We say that the adversary is considered to have broken our PPLSS if the adversary is able to find out the location of any user in G solely from the data received from the n group member's u1 to UN. We do not consider physical or side-channel attacks such as the adversary finding out a user's location through other means, for example, by tracking the cell towers that are communicating with the user.Highlight all author and affiliation lines.

Report Generation

We introduce an Order-Retrievable Encryption (ORE) scheme; a new encryption notion for Privacy-Preserving Location Sharing Services (PPLSS) in social networking applications. ORE is designed to answer location queries that allow a user to view the exact location of his/her friends within a user-specified distance without revealing any location information about the user and his/her friends to the database server and any other users in the system. The distinguishing characteristics of ORE compared to existing algorithms are that ORE provides secure location privacy, achieves low communication and computational cost, and supports dynamic location updates.

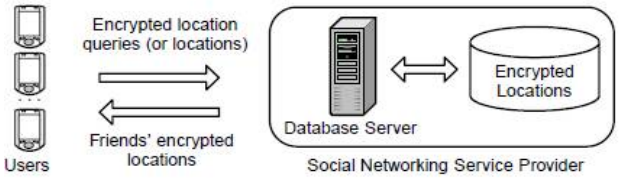
Comparing ORE and CRT

To evaluate the performance of our Privacy-Preserving Location Sharing Services (PPLSS) using the Order-Retrievable Encryption with the sequential scan (ORE) scheme and ORE with the proposed index structure (ORE-Index), and also to compare them to the state-of-the-art cryptography-based privacy-preserving query processing technique for spatial data, namely, the CRT scheme described in, we implemented a simulator in Java to run both our ORE and ORE-Index schemes and the CRT scheme. CRT is an interactive protocol for location queries over spatial data, making use of R*-trees and cryptography-based transformations on location data to protect the privacy of the data.

Extension to the ORE-Index Scheme

The extension of the ORE-Index scheme to support personalized privacy regions is very similar to the ORE scheme. The only difference is that the database server first searches the index constructed for a querying user u to find a candidate answer set A. For each member, if the ORE comparison algorithm ORE comparison indicates that member in A is a false positive as in the original ORE-Index scheme the querying user is outside mi's privacy region, mi is removed from A. After that a set of the AES encrypted location of each remaining member in A constitutes a query answer returned to users.

V. SYSTEM DESIGN



The users here are friends who are known by admin and will give request to users/friends .The friend/users accept the friend request if only they know them and it will be stored in database server.

Database Server

The database server used in our proposed system is the online database server .In already existing system they have used the centralized database server.

Encrypted Locations

The database stores the query send by the user in an encrypted format.

VI. CONCLUSION

In this paper it allow a user to view the exact location of his/her friends within a user-specified distance without revealing any location information about the user and his/her friends to the database server and any other users in the system. It achieves low communication and computational cost, and supports dynamic location updates.

References

[1] E. Toch et al., "Empirical models of privacy in location sharing," in Proceedings of the ACM International Conference on Ubiquitous Computing, 2010.

[2] S. Consolvo et al., "Location disclosure to social relations: Why, when, & what people want to share," in Proceedings of the ACM Conference on Human Factors in Computing Systems, 2005.

[3] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper*: Query processing for location services without compromising privacy," ACM Transactions on Database Systems, vol. 34, no. 4, pp. 1–48, 2009.

[4] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services, 2003

[5] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services withoutcompromising privacy," in Proceedings of the International Conference on Very Large Data Bases, 2006.

[6] T. Wang and L. Liu, "Privacy-aware mobile services over road networks," in Proceedings of the International Conference on Very Large Data Bases, 2009.

[7] H. Anandakumar and K. Umamaheswari, Supervised machine learning techniques in cognitive radio networks during cooperative spectrum handovers, Cluster Computing (2017), 1–11. doi: 10.1007/s10586-017-0798-3

[8] L. Siksnys, J. R. Thomsen, S. Saltenis, and M. L. Yiu, "Private and flexible proximity detection in mobile social networks," in Proceedings of the International Conference on Mobile Data Management, 2010.

[9] L. Siksnys, J. R. Thomsen, S. Saltenis, M. L. Yiu, and O. Andersen, "A location privacy aware friend locator," in Proceedings of the International Symposium on Spatial and Temporal Databases, 2009.

[10] S. Mascetti, C. Bettini, and D. Freni, "Longitude: Centralized privacy preserving computation of users' proximity," in the International Workshop on Secure Data Management, 2009.

[11] S. Triukose, S. Ardon, A. Mahanti, and A. Seth, "Geolocating ip addresses in cellular data networks," in Passive and Active Measurement, ser. Lecture Notes in Computer Science, 2012, vol. 7192, pp. 158–167.

[12] M. L. Yiu, G. Ghinita, C. S. Jensen, and P. Kalnis, "Enabling search services on outsourced private spatial data," The International Journal on Very Large Data Bases, vol. 19, no. 3, pp. 363–384, 2010.

[13] O. Goldreich, Foundations of Cryptography, volume I, Basic Tools. Cambridge University Press, 2007.