International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Secure Location Sharing Services Using ORE for Social Networks

GADIPALLY KRANTHI KUMAR [1], KIRAN PARUCHURI [2], KARRE MAHESH [3], TELUGU MANOHER [4]

[1]B-Tech, Lords Institute Of Engineering And Technology, Mail Id: kranthi.g.50@gmail.com

[2]B-Tech, Lords Institute Of Engineering And Technology, Mail Id: kiranparuchuri9@gmail.com

[3]B-Tech, Lords Institute Of Engineering And Technology, Mail Id: biswadipcsebora@gmail.com

[4]Assistant Professor, Lords Institute of Engineering and Technology,
Mail Id: telugumanoher@gmail.com

Abstract

A common functionality of many location-based social networking applications is a location sharing service that allows a group of friends to share their locations. With a potentially un-trusted server, such a location sharing service may threaten the privacy of users. Existing solutions for Privacy-Preserving Location Sharing Services (PPLSS) require a trusted third party that has access to the exact location of all users in the system or rely on expensive algorithms or protocols in terms of computational or communication overhead. Other solutions can only provide approximate query answers. To overcome these limitations, we propose a new encryption notion, called Order-Retrievable Encryption (ORE), for PPLSS for social networking applications. The distinguishing characteristics of our PPLSS are that it allows a group of friends to share their exact locations without the need of any third party or leaking any location information to any server or users outside the group, achieves low computational and communication cost by allowing users to receive the exact location of their friends without requiring any direct communication between users or multiple rounds of communication between a user and a server, provides efficient query processing by designing an index structure for our ORE scheme, supports dynamic location updates, and provides personalized privacy protection within a group of friends by specifying a maximum distance where a user is willing to be located by his/her friends. Experimental results show that the computational and communication cost of our PPLSS is much better than the state-of-the-art solution.

Keyword: - PPLSS, Database Server, Data Users, ORE Index

1. INTRODUCTION

Many location-based service providers today provide users with services related to their locations by making use of GPS-enabled mobile devices, wireless communication and spatial database management systems. A popular type of such services is for a user to search for points of interest in the vicinity (e.g., dining and shopping). Recently, location-based services have been combined with online social networks, where user-generated, geo-tagged information is shared among people who are part of a social network. A common functionality of many existing location-based social networking systems is location sharing services that allow users to discover the current location of their friends and notify the users when a friend is in the vicinity or within a certain distance

2. RELEGATED WORK

Existing System

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 (e.g., the location, time and frequency of each place which has been visited by each user) and that raises privacy concerns. Existing privacy-preserving location sharing schemes aim to protect the user location privacy against the central server, but they still allow the server to provide the user with the necessary services. However, in some existing schemes, the central server still knows the user's approximate location. Other schemes require 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, increasing the communication cost and making those schemes less practical.

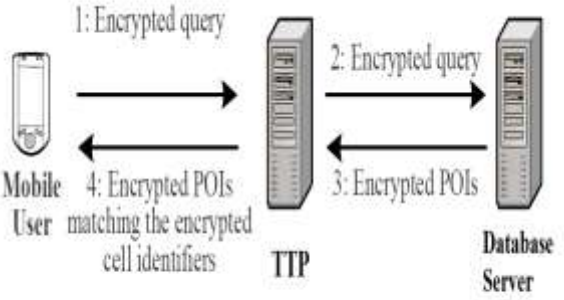

Fig:-1 Existing System Flow

Disadvantages

- A detailed movement profile of each user such as the location, time and

frequency of each user raises privacy concerns.

- Existing privacy-preserving location sharing schemes aim to protect the user location privacy, but they still allow the server to provide the user with the necessary services.
- Increases the communication cost and making those schemes less practical.
- Only return approximate results, making them less useful

Proposed System

Our Privacy-Preserving Location Sharing Services for social networking systems. In particular, our scheme enables users to browse their friends' exact locations within a certain distance without revealing any information about their locations to any other users or a social networking service provider. The users send their location information in encrypted form to the database server according to our scheme. When a user wants to locate his/her friends in the vicinity, the user logs onto the application and find the user encrypted location. The user then recovers the actual location of his/her friend by decrypting with the password.

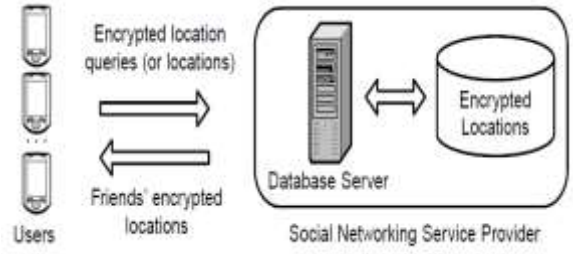

Fig:-2 Proposed System Flow

Advantages

- Secure location privacy.
- Low computational and communication cost.
- Efficient data updates.
- Personalized privacy within a group of friends.

3. IMPLEMENTATION

PPLSS

In PPLSS, assume that the database server is honest-but curious, i.e., it follows our designed protocol, but it attempts to infer the user's location. On the other hand, the user trusts his/her friends (i.e. other users in his/her friend list in the social network context). The user constructs a trusted group in which they share their locations through private location queries according to our ORE scheme.

Database Server

The database server is maintained by a social networking service provider, in which each user sends his/her location in encrypted

form according to our ORE scheme to the database server. The database server is equipped with a privacy-aware query processor that has the ability to provide an exact query answer for the user based on the user's encrypted location and his/her friends' encrypted locations without knowing any location information about the query and the users.

User

When a user wants to query the exact location of his/her friends who are within a distance specified by the user, the user sends a location query in the form of a private location-based range query, (like Send me the location of my friends within 2 km of my current location) to the database server. Data server return results to user. Finally, the user decrypts the query answer and browses his/her friends' locations displayed on a road map. It is important to note that all user locations and location queries are encrypted using our ORE scheme

Algorithm for ORE

Input: User location (x, y), Query location (x_q, y_q)

Output: User's Query data Q.

Initialization:

i. Let G is a group of members, m-members in G.

ii. User set location, defined x, y (Current exact Location).

iii. SK_G ← Symmetric key (d+1) x (d+1) invertible matrix. (Sharable to Group members).

let x_q,y_q ∈ G, distance d (nearby results)

Q= x_q,y_q;

C ← QGen(SK_G, Q); //Encrypted Query

Compute distance,

for each m : G

C_0=m(x, y);

C_1=m_i(x_i,y_i); //Decrypt with SK_G

dist=Cmp(C_0,C_1);

if dist>dist

C_1→ R;

end if;

end for;

Sort(R);

4. EXPERIMENTAL RESULTS

Fig:-3 Home Screen

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Fig:-4 Authentication

Fig:-6 Location Sharing

Fig:-5 Group Manage Screen

Fig:-7 User Queries

5. CONCLUSION

In this paper, 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. To improve query processing efficiency, we propose a tree-like index structure for our ORE scheme (ORE Index) to facilitate range searches over the encrypted locations of a group of friends. In addition, a personalized privacy region scheme is proposed to further improve user privacy within a group of friends by enabling a user to specify a maximum distance up to which his/her friends are allowed to locate the user. We also perform experiments to evaluate ORE and ORE-Index and show that their performance is much better compared to the state-of-theart cryptography-based technique designed for spatial queries.

REFERENCES

[1] Facebook Places, "http://www.facebook.com/places

[2] Foursquare, "http://www.foursquare.com."

[3] Google Plus, "https://plus.google.com."

[4] Loopt, "http://www.loopt.com."

[5] L. Barkhuus, B. Brown, M. Bell, S. Sherwood, M. Hall, and M. Chalmers, "From awareness to repartee: Sharing location within social groups," in Proceedings of the ACM Conference on Human Factors in Computing Systems, 2008.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.