Location Information Sharing on Mobile Online Social Networks Using Facial Recognition Method

Sherin Annie Thomas[1], Salitha M.K[2]

[1]Dept.of CSE, Caarmel Engineering College, M G University, Kottayam, Kerala, India
Email: sherinanniethomas@gmail.com
[2]Assistant Professor in CSE, Caarmel Engineering College, M G University, Kottayam, Kerala, India
Email: salitha.mk@bccaarmel.ac.in

***Abstract*—** *Online social networks allows the users to share their data with their friends. With the advent of mobile computing, traditional social networks have gradually adapted to a fresh paradigms called mobile online social networks. The Mobile online social networks (mOSNs) had become more popular, and compared with traditional OSNs, mOSNs provide the location-based services, which raise significant privacy concerns. Location sharing is a fundamental component of mOSN, but users may be hesitant to share their location and extract sensitive information due to the privacy concern. The mOSNs collect a large amount of location information over time, and the users' location privacy is compromised if their location information is used by other third party adversaries controlling the mOSNs. While the location-based features make mOSNs popular, they also raise significant privacy concerns. The threat is even more serious when it comes to mOSNs, because user's locations are being correlated with their profiles. Here, the system achieves social network privacy and location privacy. The system cannot be linked to the same user. The identity of each user in the query set will be replaced with a pseudo identity before sending the query to the location servers. It improves the privacy of users in mobile online social networks. The proposed system provides a face recognition for the privacy-preserving of the users. The given image will be encrypted to a key format and this key will uniquely identify the user. The system uses private photos in a privacy-preserving manner for each user.*

Keywords*— *Facial recognition, location based services, location privacy, location sharing, mobile Online Social Networks.

I. INTRODUCTION

The evolution of mobile computing had made a significant influence on individuals, organizations and society. Mobile computing helped to adapt the traditional web based online social networks to the mobile platform. This made the growth of mobile online social networks (mOSNs) paradigm. While comparing with the web based social networks, mOSNs provides better connectivity with users from wherever they are. As the shifting of technology from the traditional web based social network to the mobile online social network had increased, it is important to analyse the impact of mOSNs from a privacy standpoint.

Location based services are the fundamental component of the mobile online social networks (mOSNs). By taking in account of the mobile devices geographical location different types of services can be provided to the user. Location sharing for the location based services has increased various privacy issues. Online social networks increasingly allow mobile users to share their location with their friends. The third parties can learn user's location from localization and location visualization services.

While the location based features make mOSNs more popular, they also raise significant privacy concerns. The threat is more serious when it comes to mOSNs, where the user's physical locations are correlated with their profiles. As indicated in the previous work [2], shows how to flexibly share presence by preserving user privacy with both friends and strangers. Another research [3], shows how untrusted third-party servers are treated simply as encrypted data stores. This approach significantly improves user's location privacy. Mobishare [5] and Mobishare+ [6] are two another approaches providing privacy in location sharing in mOSNs. Mobishare, which uses the bloom filter to prevent adversary attack. Mobishare+ employs dummy queries besides dummy location and identities. N-Mobishare [7], is simple and more consistent with the characteristics of social networks. Compared with Mobishare, N-Mobishare is more practical and efficient.

However, no schemes proposed so far does not meet the security requirements of social network privacy. The previous works cannot prevent the location service provider from getting the sensitive information of the user. In this paper, we propose a novel solution for achieving both location privacy and social network privacy. The new architecture proposed here is with multiple location servers. Each location servers contain the location information of the users. When a request for friend's location is submitted by a user, this set will sent to the location server. Each location server will have a subset of user's friends list. In this way queries cannot be linked to the same user and privacy have been improved. While registering to the online server and updating the location in the location server, each user have a sign which will be generated using the image which has been given by the user. In this way privacy of each user will be achieved in this new architecture.

II. SYSTEM ARCHITECTURE AND THREAT MODEL

2.1 System Model

The new construction provides a way for preserving privacy of users who shares their location with their friends and strangers. There are three entities in our architecture. They are users, online social network server and location server. The users who have mobile devices, shares their location information with their trusted friends and untrusted strangers. This users can query location servers about nearby friends and strangers locations. The users who are using the mOSN have to get registered with the online social network server. Users have to give their profile related information to the online social network server. The Online social network server provides all the services related to the online social network to its users. Location server is used to store all the location information of the users. It provides the location based services according to the request of the users.

Each user in the online social network server has a unique key which provides privacy for the users. This key is generated by the image which has been given by the user to online social network server. For every activity in the mOSN, user have to provide this image to verify his/her identity to the system. By this way privacy of each user has been satisfied in the online social network server and the location server.

2.2 Threat Model

We assume that the social network server and the location server are not trusted to access user's personal information and location details. Here, we assume that users might be dishonest and they will try to access information's that are outside their privileged access. Another assumptions are, online social network server might be honest but curious and it will try to access the location updates that has been done by the users. Location servers also be honest but curious and it will also try to access the sensitive information's about the users from their profiles.

Another assumption is that either the social network server or the location server can be controlled by an adversary which tries to link users identities to their location details. The social network server and the location server cannot collude with each other and cannot access the information's that are out of their privileged access area.

III. SYSTEM DESIGN

3.1 Notations

The notations used in this paper are summarized in Table 1.

TABLE 1
SUMMERY OF NOTATIONS

Symbol	Description
ID	Users social network identifier
LS	Location Server
SOSN	Social Network Server
FID	Fake identifier including real and dummy ones
*f*ID	User ID's friend-case threshold distance
*s*ID	User ID's stranger-case threshold distance

3.2 User Registration

In this location sharing systems for mOSNs, each user have to do two types of registrations. 1) Registration in the social network server and 2) Registration in the location server. The proposed system architecture is shown in Fig. 1.

3.2.1 Social network server registration

In the social network server registration users have to fill up all the profile related information. All the personal information of the user will be kept by the social network server. The $U = \{ID1, ID2, . . .IDn\}$ is the identity set of all of the users involved in the system, and a social network graph $G = (V,E)$ on U has been stored at *S*ocial network server, where $V \subseteq U$ is a set of identity vertices and $E \subseteq V \times V$ is a set of edges in G. Each user will define his access control policy by providing two threshold distances *f*ID and *s*ID. The value of *f*ID denotes which distance the user with identity ID is willing to share location with his/her friends, and *s*ID denotes the threshold distance within which he/she agrees to share location with strangers. After the registration, the social network information and his/her friend relations at *G* are updated.

While registering in the social network server, user have to give a signature using image. The facial recognition system is used here to validate the user by verifying the digital image signature given by each user.

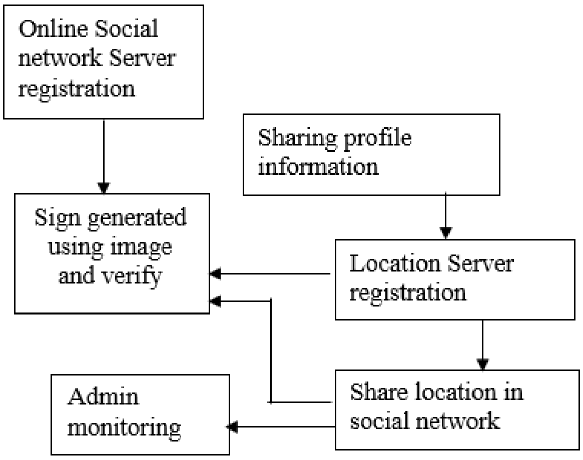
Online Social network Server registration
Sharing profile information
Sign generated using image and verify
Location Server registration
Admin monitoring
Share location in social network

FIG. 1 SYSTEM ARCHITECTURE

3.2.2 Location server registration

The user need to register their identity in the location server to provide location updates. The user who login in location server, can view their friend's locations and share their locations within his/her group of friends. Here also digital image signature will be verified to validate the user.

3.3 Location Updates

User can updates their locations when their location changes and these locations will be updated in the location server. To update the location information user have to verify his/her identity with digital image signature.

3.4 Location Query

Each registered user can do two types of queries in the system. They are friend's location query and stranger's location query.

3.4.1 Friend's location query

To know the location of his/her nearby friends' current locations, the user queries the social network server and the location server and receives the location information of friends whose specified access control setting is satisfied by the querying user. For viewing the location, the user have to be validated with the digital image signature.

To get the information of friends' locations, the user with an identity ID submits a friends' location query (ID, 'f', *l*) to social network server , where *l* denotes the distance threshold specified by the user and "f" denotes the symbol of friend query. Upon receiving the query, social network server finds the appropriate entry (ID, FID, *f*ID, *s*ID) in the local user information table. Social network server first finds the user's friend set and send the query to the locations servers. While getting the query, the location server get the locations by decrypting the digital signature. For each of the nearby users, the location server will enforce access control based on these users' friends threshold distance. Finally, the user decrypts and gets all of the nearby friends' identities and locations.

3.4.2 Stranger's location query

If a user wants to get nearby strangers' current locations, he/she queries the social network server and location server and receives the location information of someone whose specified access control setting is satisfied by the user. The users first submit his query with his digital signature to validate his/her identity. The digital image signature submitted by the user can uniquely identify his identity.

While receiving the request, the location server will first get the locations by validating the identity of the user. For each of these nearby users, the location server will enforce access control based on these users' stranger-case threshold distance.

3.5 Facial Recognition System

Facial recognition system identifies person from a digital image. In our system, we uses facial recognition method to generate a digital image signature to validate each users in the system. While registering in the online social network server we give a digital image as a signature for each individual and using this signature a key will be generated. While doing each procedure we have to give the digital image to verify each user. Here, the facial recognition system will identify the digital image given by the user.

IV. EVALUATION

The performance of the proposed system is evaluated using the encryption and decryption performance of the location sharing system. Here, we evaluate the time of cost for the encryption related with the number of nearby friends in the system. Fig 2. Plots the time of cost versus number of nearby friends for encryption. We can see that the encryption time is linear with the number of friends. Even the number of friends is bigger than 100, the execution time will be less, and thus, it is efficient and practical.

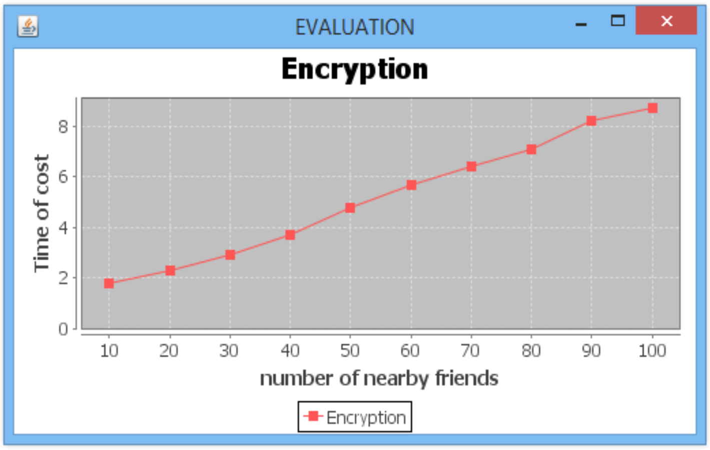

FIG. 2 TIME OF COST VERSUS NUMBER OF NEARBY FRIENDS GRAPH

Another evaluation which is done in the system is the time of cost needed for both encryption and decryption process in BE scheme and it is plotted in Fig. 3. Here the decryption time is higher than the encryption time because we are concerning about the security performance of the system. As the decryption time increases it increases the security of the system.

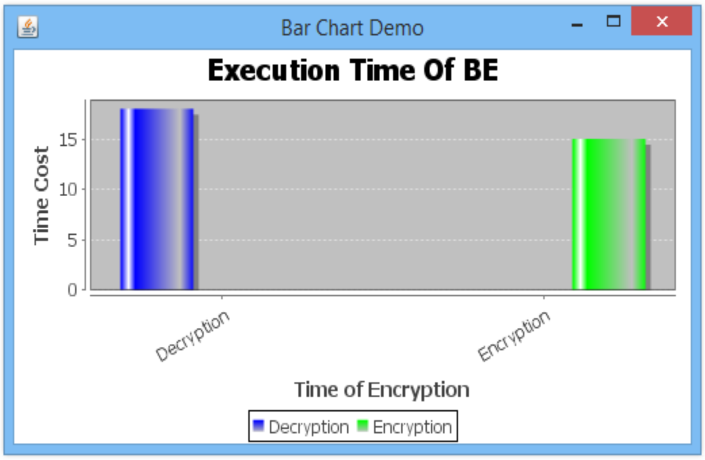

FIG. 3 EXECUTION TIME OF BE

The comparison between the existing system and the proposed system is analysed using a bar chart which compares the time of cost, execution time and the secuity of both systems. This graph is plotted in Fig. 4.

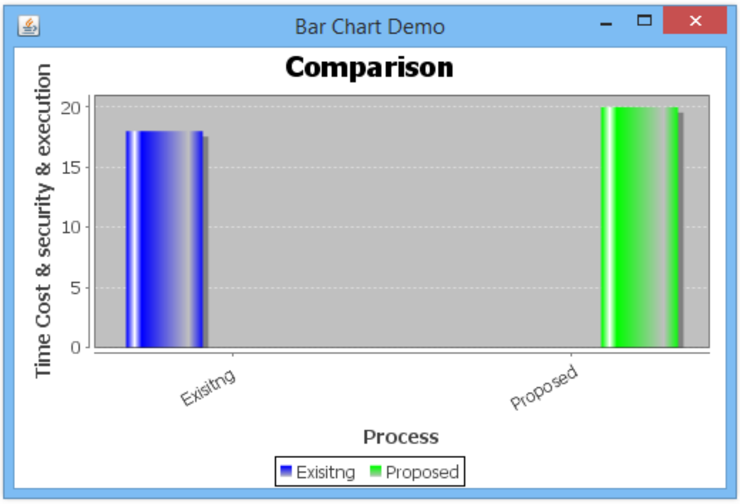

FIG. 4 COMPARISON OF EXISTING AND PROPOSED SYSTEMS

V. CONCLUSION

In this work, we have addressed the problem of privacy in online social network. Online social network security and the location server security are the main security concerns in the location based services. Without enough privacy users may be hesitant to share location information to mOSNs. Therefore by considering the privacy of users here proposes a face recognition method. In this a digital image signature is used as a key to uniquely identify each user in the location sharing system. While registering to the online server and updating the location in the location server, each user have a sign which will be generated using the image which has been given by the user. In this way privacy of each user will be achieved in this new architecture.

REFERENCES

[1] Jin Li, Hongyang Yan, Zheli Liu, Xiaofeng Chen, Xinyi Huang, and Duncan S. Wong, "Location - sharing systems with enhanced privacy in Mobile Online Social Networks," in IEEE system journal, 2015.

[2] L. P. Cox, A. Dalton, and V. Marupadi, "SmokeScreen: Flexible privacy controls for presence-sharing," in *Proc. MOBISYS*, 2007, pp. 233–245.

[3] K. P. N. Puttaswamy and B. Y. Zhao, "Preserving privacy in location based mobile social applications," in *Proc. Hotmobile*, 2010, pp. 1–6.

[4] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," 2011, pp. 494–505.

[5] W. Wei, F. Xu, and Q. Li, "Mobishare: Flexible privacy-preserving location sharing in mobile online social networks," in *Proc. INFOCOM*, 2012, pp. 2616–2620.

[6] J. Li, J. Li, X. Chen, Z. Liu, and C. Jia, "Mobishare+: Security improved system for location sharing in mobile online social networks," in *Proc. 5th Int. Workshop MIST*, 2013.

[7] Z. Liu, J. Li, X. Chen, J. Li, and C. Jia, "New privacy-preserving location sharing system for mobile online social networks," in *Proc. 3PGCIC*, 2013, pp. 214–218.

[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in *Proc. 29th Annu. ACM STOC*, New York, NY, USA, 1997, pp. 506–516.

[9] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in *Information Theoretic Security*, ser. ser. Lecture Notes in Computer Science, A. Smith, Ed. Berlin Germany: Springer-Verlag, 2012, vol. 7412, pp. 37–61.

[10] P. Golle and I.Mironov, "Uncheatable distributed computations," in *Proc. Conf. Topics Cryptology—CT-RSA*, 2001, pp. 425–440.