Privacy Control Protocol for Post Sharing in Online Social Network's using Cosine Similarity and Set Intersection

K. Sarath Kumar
P.G. Student
Department of Computer Science & Engineering
University College of Engineering, Anna University, BIT campus, Tiruchirappalli, India

V.M.Priyadharshini
Assistant Professor
Department of Computer Science & Engineering
University College of Engineering, Anna University, BIT campus, Tiruchirappalli, India

Abstract

The internet is being integrated into nearly every aspect of daily life of individuals. Social networks are made up of user profiles which are a collection of user's personal data and its relation to other users. Many relations between users are based on trust but trust and privacy are not captured and presented in profiles and personalized recommendations. An efficient privacy protection mechanism is important for OSNs that can be used to protect the privacy of online social relationships and users' data from third parties. Post sharing is one of the important aspects of an online social network. Sharing such data requires security. Unfortunately, it may reveal users' privacy if they are allowed sharing a photo freely. There must be some mechanism that enables the user to participate in decision- making the activity of user post who can able to view when his\her friends sharing the post. In this work, we propose a set intersection rule and cosine similarity for a privacy preserving manner.

Keywords: Trust, OSN, Privacy, Cosine similarity and Set Intersection

I. Introduction

A social network the digital level represents of member and their relationships. The concept of social clouds is an emerging illustration that allows users to mutually offer and consume services, such as interest sharing, activity planning, the organization of events, multimedia content exchange, Group chatting and so on. Social clouds offer an appealing way for users to expand and reflect their social relationships and then use them for social interaction or collaboration in business and leisure. Online Social Network is the easiest way to be connected with friends, colleagues as well as establish new contacts with the strangers. OSN enable people to connect with their friends as well as share information about their personal life. OSNs are mainly used for keeping in touch with friends, forming new contacts, as well as search for someone else on the OSN and establish contact with him by sending a friend request. Such contacts are used to share some information with each other as well as broadcast the information through a group. In current online social networks users do not have complete control over who can access their data. While most OSN services provide some privacy settings to limit the audience to which a user's content published some default setting make this content public. Because most users reveal an astonishing amount of information in their profiles and tend not to change the default privacy.

By making some secret / private fields accessible to everyone there are chances of personal information reveal. The personal information privacy oversight leads to the personal information reveal. Leery users take advantage of these profiles to collect other's private / secret information which leads to personal information manifest which is a threat to the privacy of the user. An online social networks has there are some privacy settings for upload the post\image in their timeline.

In many realistic scenarios, users need to make access control decisions involving other (possibly stranger) users, e.g., for sharing posts to construct distributed computing platforms. One important trust-enhancing factor, potentially guiding such decisions, is the existence of previously established social relationships. However, the process of discovering mutual friends may harm the privacy of the two parties and that of their friends. At least one party needs to disclose the identity of his friends and, depending on the application scenario, this could reveal the identity of the user, and possibly even information about his lifestyle and social attitudes.

Motivated by the above issues, this paper customize of an infrastructure supporting the secure discovery of mutual friends, which we denote as Mutual Friends. It allows two users friends list to decide whether their owners are friends or have mutual friends in a given social network. Similar to exiting survey [13, 14], network similarity between user i and a stranger j is computed based on the use of network information of both i and j. A general way to find this similarity is to count the number of common friends between i and j. However, in this method relationships among common friends of i and j are ignored, losing valuable information. In this paper compute set intersection and cosine similarity to ensure privacy and authenticity. The mutual friend's service is interesting in a number of realistic scenarios, where users can make trust and access control decisions in a privacy-preserving manner.

II. RELATED WORK

In the literature, the term similarity has been used in different meanings (e.g., specify the mutual social connection, shared features or shared actions). [1] This paper propose the Mutual Friends service, a construction for finding common friends which protect the privacy of non-mutual friends and guarantees authenticity of friendships. In this author were design the common friends, an approach that enables two devices to adjudge if their owners re friends or share common friends in a given social network. Mutual friends combines private set intersection with bring capabilities to assured privacy and authenticity. [2] The authors of this paper propose an OSN that provides users with the control of encrypting their personal data from a third party. Although existing OSNs provide users with control over who can access and view your personal information, the OSN service itself can still access your information and use it for commercial purposes. Effects of User Similarity in Social Media [3] In this paper, analysis of user-to-user evaluations can be significantly strengthened by taking into account the similarity in characteristics of users — such as the extent to which their contributions to the site have involved similar content, or have involved interactions with a common set of other users. The basis of these studies is user similarity measures. In this paper, [4] approach user similarity from two angles. First, a network similarity measure that considers only the graph structure and that, differently from existing techniques, takes into consideration also how two users are indirectly connected. Secondly, profile a similarity measure based on user profile information, such to find semantic similarities between users. In this paper, [5] present a method for solving the Entity Resolution (ER), a problem for matching user profiles across multiple OSNs. This paper proposes an algorithm is able to match two user profiles from two different OSNs based on machine learning techniques, which uses features extracted from each one of the user profiles. Using supervised learning techniques and extracted features, they constructed different classifiers, which were then trained and used to rank the probability that two user profiles from two different OSNs belong to the same individual. These classifiers utilized 27 features of mainly three types: name based features (i.e., the Soundex value of two names), general user info based features (i.e., the cosine similarity between two user profiles), and social network topological based features (i.e., the number of mutual friends between two users' friends list). This paper starts with an explanation of two types of profile cloning attacks in OSNs. Afterward, a new approach for detecting the clone identities is proposed by defining profile similarity and strength of relationship measures. According to similar attributes and strength of relationship among users which are computed in detection steps, it will be decided which profile is a clone and which one is genuine by a predetermined threshold. Profile cloning attack (also called identity clone attack) attempts to create a fake identity of the victim in OSNs to trick their friends in to believing the validity of the fake identity, to make social links, and catch private information of victim's friend successfully which is not shared in their public profiles [6]. In this paper, [7] represent leverage community structures to redefine the OSN model and propose a realistic asymmetric social proximity measure between two users. Then, based on the proposed asymmetric social proximity, the author design three private matching protocols, which provide different privacy levels and can protect users' privacy better than the previous works. Private Set Intersection (PSI) protocols allow one party ("client") to compute an intersection of its input set with that of another party ("server"), such that the client learns nothing other than the set intersection and the server learns nothing beyond client input size. Prior work yielded a range of Private Set Intersection protocols secures under different cryptographic assumptions. Protocols operating in the semi-honest model offer better (linear) complexity while those in the malicious model are often significantly more costly. In this paper,[8] the author constructs PSI and Authorized PSI (APSI) protocols secure in the malicious model under standard cryptographic assumptions, with both linear communication and computational complexities. This paper [9] motivates and introduces the concept of Private Discovery of Common Social Contacts, which allows two users to assess their social proximity through interaction and learn the set of contacts (e.g., friends) that are common to both users while hiding contacts that they do not share. Trust - aware paper, a trust model for social media is first presented. Based on the trust model, a trust-aware privacy control for social media [10] propose a privacy control protocol is proposed, that exploits the underlying inter-entity trust information. The objective is to design a fine-grained privacy scheme that ensures a user's online information is disclosed only to sufficiently trustworthy parties. In this paper [11] based friend recommendation system for social networks, which recommends friends to users based on their lifestyles instead of social graphs. By taking advantage of sensor-rich smartphones, Friendbook discovers lifestyles of users from user-centric sensor data, measures the similarity of lifestyles between users, and recommends friends to users if their lifestyles have high similarity. Zhang et al. [12] also propose a privacy preserving verifiable profile matching scheme which is based on symmetric cryptosystem and thus improves efficiency. It relies on a pre-determined ordered set of attributes and uses it as a common secret shared by users.

III. EXISTING SYSTEM

An online social network is most popular to the people. Post/image sharing is one of the important things in the online social network. A user uploads a post in their timeline. There are some privacy settings in an online social network such as friends, public, custom and only me. The user objective is that post can be viewed their friends only.so the user selects the friends option from osn privacy setting. But anyone his/her friend can be the share that post.so user privacy can be reveal.
Disadvantages of Existing system

1) Privacy
   - Data identity theft.
2) Authenticity
   - Anyone can be view the post.

3) Potential for misuse
   - Bullying
   - Falsifying personal information.

IV. PROBLEM STATEMENT

To enable sharing of post in secure manner so that privacy is maintained and there will less possibility of loss of information.

V. SYSTEM ARCHITECTURE

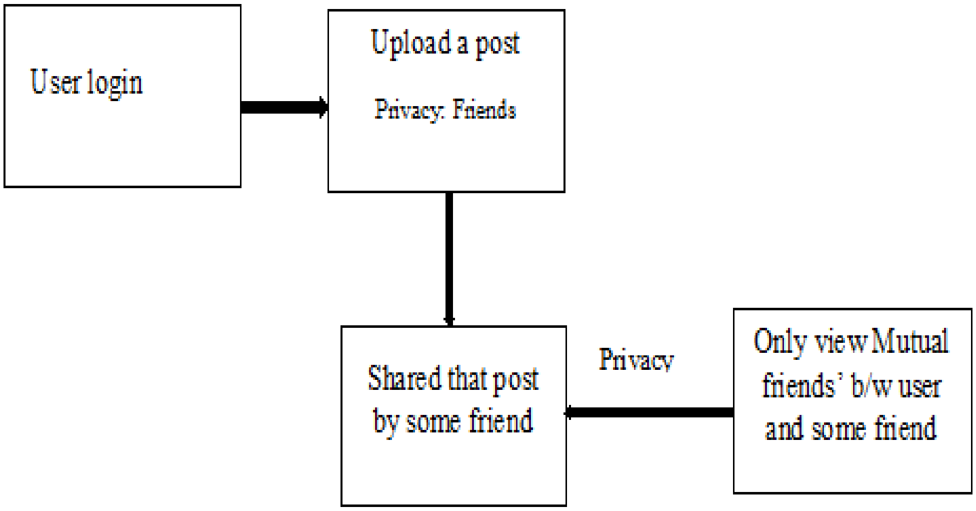
User login
Upload a post
Privacy: Friends
Shared that post by some friend
Privacy
Only view Mutual friends' b/w user and some friend

Fig. 1: Privacy control protocol architecture

VI. PROPOSED SYSTEM

Privacy concerns and privacy controls on OSN are ever changing. When you post a picture of your kids at a family gathering, which one of your OSN friends can share it? A user uploads a post in their timeline, that post can be viewed their friends only. But anyone his/her friend can be the share that post.so user privacy can be leakage. There must be some mechanism that enables the user to participate in decision- making the activity who can able to view when his\her friends sharing the post. In this work, propose set intersection for finding mutual friends between the users and cosine similarity for control mutual friends only view that shared the post by his/her friends.

Mutual Friends: The mutual friends specify the mutual social connection between the users.

$$MF_i = U_i \cap F \qquad (1)$$

Where,
MF_i = Mutual Friends
U_i = Target profile
F = Friends profiles

Cosine Similarity: Cosine similarity, which is defined on two users of friend list, calculates the cosine value of the similarity between the two users. It can be represented by the dot product and magnitude product of the two vectors, as:

$$S_c(i,j) = \mathrm{Cos}(L_I , L_j) \qquad (2)$$

$$\mathrm{Cos}\left(L_I , L_j \right) = \frac{L_I . L_j}{\|L_i\|\|L_j\|} \qquad (3)$$

Where
L_i = list of friends from user i
L_j = list of friends from user j

Advantages of proposed system
   - Sharing of post efficient.
   - Security of sharing photo is increased.
   - Less possibility of loss of information.

VII. CONCLUSION

The wide use of social networks raises privacy issues encountered by OSN users. The privacy preserving protocol is fully customizable to satisfy user's privacy needs. Post sharing is most popular and usual trend in an online social network. Such kind of data sharing may manifest user's policy. This paper integrated cosine similarity with set intersection for control privacy leakage. This proposed scheme be very useful in protecting user's privacy in post/photo sharing over online social networks.

REFERENCES

[1] Marcin Nagy, Emiliano De Cristofaro, N. Asokan and Ahmad-Reza Sadeghi. Do I know you? : Efficient and privacy-preserving common friend-finder protocols and applications. Proceedings of the 29th Annual Computer Security Applications Conference.

[2] Randy baden, Adam bender, Neil spring, B Bhattacharjee. Persona: An Online Social Network with User-Defined Privacy in proceedings of the ACM SIGCOMM 2009 conference on Data communication pages 135-146.

[3] Anderson, A., Huttenlocher, D., Kleinberg, J., Leskovec, J.: Effects of user similarity in social media. In: Proceedings of the Fifth ACM International Conference on Web Search and Data Mining, pp 703-712. ACM 2012.

[4] C. Akcora, B. Carminati, E. Ferrari. Network and Profile-based Measures for User Similarities on Social Networks. In Proc. of the 12th IEEE International Conference on Information Reuse and Integration (IRI 2011), August 2011.

[5] Olga Peled, Michael Fire, Lior Rokach1 and Yuval Elovici. Entity Matching in Online Social Networks in proc. of the SOCIALCOM'13 International Conference on Social Computing pages 339-344.

[6] M.R. Khayyambashi, F.S. Rizi. An approach for detecting profile cloning in online social networks in proc. of the 7th International Conference on e-Commerce in Developing Countries: With Focus on e-Security (ECDC), April 2013.

[7] Arun Thapa, Ming Li, Sergio Salinas and Pan Li. Asymmetric Social Proximity Based Private Matching Protocols for Online Social Networks in proc IEEE TRANSACTIONS PARALLEL AND DISTRIBUTED SYSTEMS VOL: PP NO: 99 YEAR 2014.

[8] Emiliano De Cristofaro, Jihye Kim, and Gene Tsudik. Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model. In Abe, M. (ed). ASIACRYPT 2010. LNCS, vol 6477, pp. 213-231.springer, Hiedelberg (2010)

[9] Emiliano De Cristofaro,Mark Manulis ,Bertram Poettering. Private discovery of common social contacts in Applied in cryptography and network security (pp. 147-165). .springer, Hiedelberg (2011).

[10] Na Li, Maryam Najafian Razavi and Denis Gillet. Trust-aware Privacy Control for Social Media In. Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems p (1597-1602).ACM

[11] Zhibo Wang, Jilong Liao, Qing Cao,Hairong Qi, and Zhi Wang, "Friendbook: A Semantic-based Friend Recommendation System for Social Networks", IEEE Transactions on Mobile Computing. (Vol 14, issue 3).

[12] L. Zhang and X.-Y. Li. Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks. http://arxiv.org/abs/1207.7199, 2012.

[13] T. M. Cover and J. A. Thomas. Elements of information theory. Wiley-Interscience, New York, NY, USA, 1991.

[14] M. Deshpande and G. Karypis. Item-based top-n recommendation algorithms. ACM Trans. Inf. Syst., 22:143–177, January 2004.