A Novel Approach for Trust-based Friend Recommendation in Online Social Network

Pooja P[1], Vartika Sharma[2], Syed Thouheed Ahmed[3]

[1]*MTech student, Dept. of CSE, GSSSIETW, Mysuru.*
[2]*Associate Professor, Dept. of CSE, GSSSIETW, Mysuru*
[3]*Sr.Research Engineer, Thinksoft and Information technologies, Bangalore*

Corresponding Email:** ***[1]lakshmihs20@gmail.com

ABSTRACT

OSNs is increasing day by day by using which people can exchange their knowledge, data or can share different information by connecting to the internet. In cyberspace people can make new friends easily by communicating with each other by using online social networks (OSNs). OSN users' existing social relationship can be characterized as 1-hop trust relationship, and further establish a multi-hop trust chain during the recommendation process. The social relationship on the OSNs is an asymmetric context-aware trust relationship between two friends, in which the privacy concerns are regarding their identities and social relationships, as well as the recommended information during the information exchange, all of which should be well addressed. In this paper, we propose a trust-based privacy-preserving friend recommendation scheme for OSNs, where OSN users apply their attributes to find matched friends, and establish a social relationship with strangers via a multi-hop trust chain to protect privacy of social networks and to establish a trust based recommendation by trust of existing users.

INTRODUCTION

OSNs is increasing day by day by using which people can exchange their knowledge, data or can share different information by connecting to the internet. Here people exchange and share information with different groups such as their colleagues, family, friends and so on. People communicate by using popular social networking sites such as Facebook, Twitter and LinkedIn. Depending on platform called social media, members may be able to contact any other member. In other cases, members can contact anyone they have a connection to, and subsequently anyone that contact has a connection to, and so on.

In cyberspace people can make new friends easily by communicating with each other by using online social networks (OSNs). Similar to what people usually do in real life, OSN users always try to expand their social circles in order to satisfy various social demands, e.g., business, leisure, and academia. In such cases, OSN users may ask for the help from their existing friends to obtain useful feedback and valuable recommendations, and further establish new connections with friends of friends (FoFs).

The social relationship on the OSNs is an asymmetric context-aware trust relationship between two friends, by which there is a possibility of establishing a multi-hop trust chain between two strangers by using existing 1-hop trust of existing friends on the OSNs. This process poses several crucial privacy breaches in the cyberspace, such as OSN users' privacy concerns regarding their identities and social relationships, as well as the recommended information during the information exchange, all of which should be well addressed. Otherwise, it would be very easy for malicious users to perform serious cyber and physical attacks, such as identity theft, inferring attack on social relationships, and profile leakage.

Current approaches cannot achieve the fine-grained and context-aware results automatically, due to the fact that OSN users have to determine the recommended friends based on their own judgments on the recommendation query which includes privacy leakages and preservation approaches regarding the identity, social attributes, and their trust relationships of OSN users during the recommendation process. This issue can be overcome by considering the possibility of using OSN users' social attributes to establish the multi-hop trust chain based on each context-aware 1-hop trust relationship, where most of trust relationships are formed and strengthened by the shared social attributes. Hence in this paper, we propose a trust-based privacy-preserving friend recommendation scheme for OSNs, where OSN users apply their attributes to find matched friends, and establish a social relationship with strangers via a multi-hop trust chain to protect privacy of social networks and to establish a trust based recommendation by trust of existing users.

RELATED WORK

In Online social network privacy plays a major role when the users communicate with each other. So Several works concentrate on privacy issues in online social network, Trust management issues, Friend recommendation and privacy preserving profile matching.

Fong et al. [1] propose an access model that formalize and generalize the privacy preservation mechanism for Facebook. Carminati. et al. also pro-pose an access control mechanism for the information sharing in web-based social networks in [2], which jointly considers the relationship type, trust metric, and degree of separation in the policy design. The schemes use the decentralized architecture for the access control, which may incur potential security breaches, like fabricating identity, attributes, and trust information.

In terms of discovering friendships, Daly and Haahr in [3] discuss the establishment of friendship chains using social attributes. Similarly, Chen and Fong in [4] use trust factor in collaborative filtering (CF) algorithm to recommend OSN users on Facebook, where they analyze the similarity based on users' interests and attributes. However, the above works fail to consider users' privacy concerns on both identity and their social attributes.

Li. et al. [5] propose a privacy-preserving personal profile matching schemes for mobile social networks, by using polynomial secret sharing. In [6], Dong et al. design a secure friend discovery scheme based on verifiable secure dot product protocol by using homomorphic encryption. Due to their distributed approaches, both of the above schemes lack the ability to prevent active attacks when users change their attributes to satisfy the query requirements.

B. zhou and J. Pei in [7] address that preserving privacy in publishing social network data becomes an important concern and most of the previous studies on privacy preservation can deal with relational data only, and cannot be applied to social network data. So authors here take an initiative towards preserving privacy in social network data by identifying an essential type of privacy attacks: neighbourhood attacks. If an adversary has some knowledge about the neighbours of a target victim and the relationship among the neighbours, the victim may be re-identified from a social network even if the victim's identity is preserved using the conventional anonymization techniques.

Dwyer et. Al., [8] proposes an online survey of two popular social networking sites, Facebook and MySpace, compared perceptions of trust and privacy concern, along with willingness to share information and develop new relationships. Here the author suggests that in online interaction, trust is not as necessary in the building of new relationships as it is in face to face encounters. They also show that in an online site, the existence of trust and the willingness to share information do not automatically translate into new social interaction. This study demonstrates online relationships can develop in sites where perceived trust and privacy safeguards are weak.

PROPOSED SYSTEM

In the proposed scheme OSN users' social attributes and trust relationship is utilized to develop the friend recommendation scheme in a progressive way while preserving the privacy of OSN users' identities and attributes. To establish anonymous communication channels OSN users' closed friends are considered. Based on the 1-hop trust relationships the existing friendship is extended to multi-hop trust chains without compromising recommenders' identity privacy. The proposed trust level scheme enables strangers to obtain an objective trust level on a particular trust chain.

The architecture of the trust based privacy preserving friend recommendation scheme consists of two modules that is the admin module and the user creation module. In the user creation module the online privacy preserving algorithm is implemented.

As shown in Figure 1 social media has admin profile and user creation profile. In the admin profile the admin will have some higher privileges such as monitoring, event creation and event authentication. In monitoring the admin performs activity management and load management. The privileges of the admin are stored in the database. Then in the user profile creation the user having account will login and user without the account will create a new account. On logging in the user will be authenticated. After that the user will establish a network in online social network for various activities. After establishing the network the user will establish some events to search for friends in Online Social Network and this established event will be verified with the events created by the admin. Also the user can share event form the set of events created by the admin.

The events will be established by the user to search for friends in online social network and here for secure friend recommendation the online privacy preserving algorithm will be implemented. Here the user will search for friends with some attributes or by creating some events. Based on the attributes or the events the search result will be displayed. That is some set of users will be displayed. Then the user may view the profile of these users later by applying some privacy techniques the recommendation will be fetched.

The Online Privacy Preserving algorithm mentioned is used to establish a friendship chain by ensuring trust between the users by providing privacy. To achieve this following steps are used in the algorithm.

Step1: Identify the close friend set.

Step2: Compute the trust level.

Step 3: Link verification.

First if friendship chain needs to be established between two users the close friend set of one user is identified by other user who wants to establish the friendship chain by friend recommendation.

Then the trust level of the user is computed that is, the user who wants to send recommendation to other user will identify the trust level of that user by identifying the friends and close friends of both the users who are in common to both.

Thirdly Link verification is done. This is another level of identifying how well the user can be trusted and how well this user is trusted by various other users in the network. Here the common close friends between both the users will be identified and the trust level of that user will be identified to increase the level of trust to establish the trust on recommended friend.

The possible outcome of this Online Privacy Preserving algorithm is that the trust based recommendation will be established between two users by the trust of existing users and the privacy of the social network users will be protected.

CONCLUSION

Social network is a type of application or a website which allows the users to communicate with each other. The basic foundation for the users to communicate with each other is through internet. In cyberspace people can make new friends easily by communicating with each other by using online social networks (OSNs). The social relationship on the OSNs is an asymmetric context-aware trust relationship between two friends, by which there is a possibility of establishing a multi-hop trust chain between two strangers by using existing 1-hop trust of existing friends on the OSNs. This process poses several crucial privacy breaches in the cyberspace, such as OSN users' privacy concerns regarding their identities and social relationships, as well as the recommended information during the information exchange. To address these problems light-weighted privacy-preserving friend recommendation scheme for OSNs by utilizing both users' social attributes and their existing trust relationships to establish a multi-hop trust chain between strangers is designed Currently by considering privacy leakages and preservation approaches regarding the identity, social attributes, and their trust relationships of OSN users during the recommendation process also the Online Privacy Preserving algorithm is proposed.

REFERENCES

[1] P. W. L. Fong, M. Anwar, and Z. Zhao, "A privacy preservation model for facebook-style social network systems," in Proc. 14th Eur. Conf. Res. Comput. Security, 2009, pp. 303–320.

[2] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," ACM Trans. Inf. Syst. Security, vol. 13, no. 1, pp. 6:1–6:38, Nov. 2009.

[3] E. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant manets," IEEE Trans. Mobile Comput., vol. 8, no. 5, pp. 606–621, May 2009.

[4] W. Chen and S. Fong, "Social network collaborative filtering framework and online trust factors: A case study on face-book," in Proc. 5th Int. Conf. Digital Inf. Manage., Jul. 2010, pp. 266–273.

[5] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacy-preserving personal profile matching in mobile social networks," in Proc. IEEE 30th Conf. Comput. Commun., Apr. 2011, pp. 2435–2443.

[6] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proc. IEEE 30th Conf. Comput. Com-mun., Apr. 2011, pp. 1647–1655.

[7] B. Zhou and J. pei, "preserving privacy in social networks against neighborhood attacks," in Proc. IEEE 24th Int. Conf. Data Eng., 2008, pp. 506-515.

[8] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and Privacy concern within social networking sites: A Comparision of facebook and myspace," in Proc. 13th Amer. Conf. Inf. Syst., 2007, p. 339

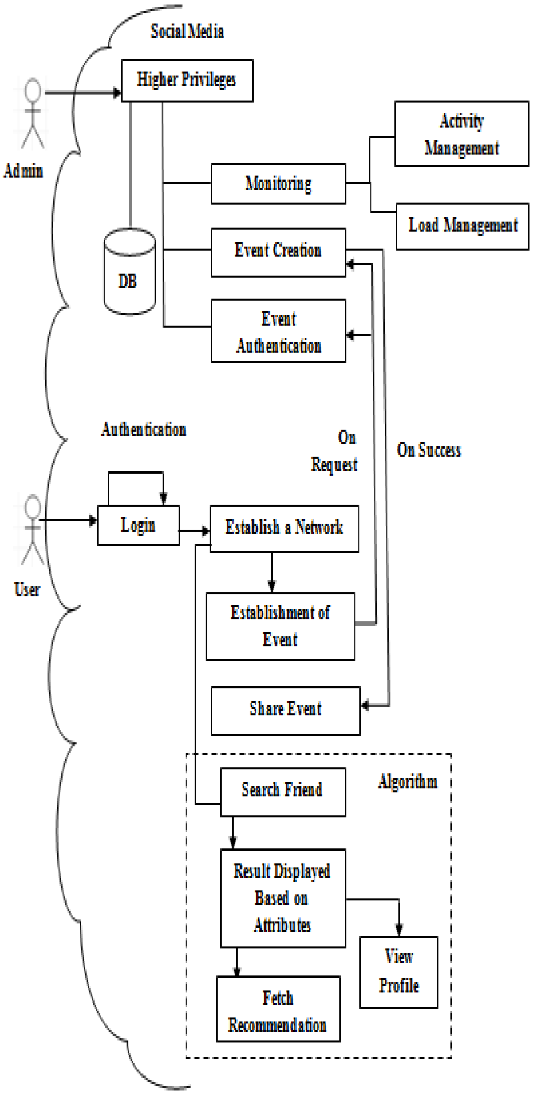

Figure 1: Architecture Diagram