



ISSN(Online): 2320-9801  
ISSN (Print) : 2320-9798

## International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

# Survey on Friend Recommendation Methods for Online Social Networks

Nilesh Kulal, Vidhya Dhamdhare

Student, Department of Computer Engineering, GHRCEM, Savitribai Phule Pune University, Pune, India

Faculty Member, Department of Computer Engineering, GHRCEM, Savitribai Phule Pune University,  
Pune, India

**ABSTRACT:** Online social networking sites, like Facebook and Google+, provides a new communication service for online users to stay in contact. With this service, user can share any kind of information with their friends and family over internet. Such communication among user generates the huge amount of data on social networking sites. But with this facility, question is arises regarding mining useful knowledge from such huge amount of data. The analysis of such data will be used in various applications for identification of potential users and promotion of items according to the user interest. From another point of view, online users of such sites often want to make new friends, so the need of good friend recommendation system is arises. It will be helpful to online users to increase the social connections and sharing of information. Old friend recommendation system makes use of users profile for recommendation purpose. But such methods are not reliable if the user wants privacy of their profiles. So another need is arises for privacy preserving friend recommendation approach based on the security of user profiles. Such methods achieve the privacy of personal information of users like friend list. In this paper, we present the comparative survey of recent privacy preserving friend recommendation system based on their advantages and limitations.

**KEYWORDS:** online social networks, privacy, trust, social relationship.

### I. INTRODUCTION

Online service provision generally happens between parties who have never executed with each other before, in a domain where the service customer regularly has lacking data about the service provider and about the goods furthermore, services offered. This strengths the consumer to acknowledge the "risk of prior performance", i.e. to pay for services and goods before accepting them, which can leave him in a defenseless position. The consumer generally has no chance to see and try products, i.e. to "squeeze the oranges", before he purchases. The service provider, then again, knows precisely what he gets, as long as he is paid in money. The inefficiencies resulting from this data asymmetry can be mitigated through trust and reputation. The idea is that even if the consumer can not try the product or service in advance, he can be confident that it will be what he expects as long as he trusts the seller. A trusted seller therefore has a significant advantage in case the product quality cannot be verified in advance.

Online social networks (OSNs) give people a simple approach to communicate with each other and make new friends in the internet. Similar to what people generally do in real life, OSN clients dependably attempt to grow their social circles in order to satisfy various social demands, e.g., business, leisure, and academia. In such cases, OSN clients may request the help from their existing friends to obtain useful feedback and valuable recommendations, furthermore, establish new connections with friends of friends (FoFs). As several works shows, the social relationship on the OSNs is an asymmetric context-aware trust relationship between two friends, by which they consider the possibility of establishing a multi-hop trust chain two outsiders by utilizing existing 1-hop trust of existing friends on the OSNs. However, the recommendation procedure represents a several crucial privacy breaches in the internet, for example, OSN clients' privacy concerns with respect to their identities and social relationships, as well as the recommended information during the information exchange, all of which should be well addressed. Else, it would be simple for malicious clients to perform serious cyber and physical attacks, for example, identity theft, inferring attack on social relationships, and profile leakage.



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

## II. RELATED WORK

Privacy concerns [1] rose in the recommendation procedure block the extension of OSN clients' friend circle. Some OSN clients decline to disclose their identities and their friends' data to the public domain. In this paper, they propose a trust-based privacy-preserving friend recommendation scheme for OSNs, where OSN clients apply their attributes to find matched friends, and build up social relationships with outsiders through a multi-hop trust chain. Based on trace-driven experimental results and security analysis, we have shown the feasibility and privacy preservation of their proposed scheme.

This paper [2] propose a Global Relationship Model (GRM) to catch the relationship strength amongst clients and then develop a searching mechanism, in particular i-Search, to locate the optimal social path between any two clients who are seriously associated in heterogeneous SNSs. They assess the execution of P2P-iSN and demonstrate that their P2P-iSN can effectively support numerous future applications, for example, enhanced trust/reputation metrics and integrated content-sharing. With the proposed P2P-iSN, SNS developers can design more effective user-centric SNS applications.

Authors [3] perform a large-scale study to evaluate exactly how severe the privacy leakage issue is in Facebook. As a case study, authors concentrate on evaluating birth year, which is a crucial human attribute and, for many people, a private one. To assess Facebook clients' ages, they abuse the basic social network structure to outline an iterative algorithm, which determines age estimates based on friends' ages, friends of friends' ages, etc. They find that for most clients, including highly private clients who hide their friend lists, it is possible to assess ages with an error of only a few of years, additionally make a particular proposal to Facebook which, if implemented, would greatly reduce privacy leakages in its service.

Authors [4] devise a model for the Federated Network centered on a User and use it to characterize the issue of Friend Finding. The solution utilizes two stages, first known as Quick Connect which tries to discover old acquaintances. The second stage, Delayed Connect utilizes the Social Graph of Users to find prospective friends. They indicate how the FSN data revolved around a User can be extricated from FOAF entries and create new recommendations. We should show the working of Talash as a part of StatusNet.

The paper [5] considers the particular issue of how clients can securely authenticate online identities (e.g., associate a Facebook ID with its owner). Based on prior social science research showing that the social tie quality is a helpful indicator of trust in many real-world relationships, they investigate how strength can be visualized utilizing well defined and measurable parameters. They then apply the visualization in the context of online friend invitations and propose a protocol for secure online identity authentication. They likewise introduce an implementation on a prevalent online social network.

In this paper [6], authors propose PriMa (Privacy Manager), a privacy protection mechanism that supports semi automated generation of access rules for clients' profile data, filling the gap between the privacy management needs of SN clients and the existing SNs' privacy protection mechanisms. PriMa access rules are generated utilizing a multicriteria algorithm, so as to account for an extensive set of criteria to be considered when dealing with access control in SN sites.

This paper [7] propose a novel reputation framework which permits clients to discover potential associations between new people based on the most updated friend list of every client in OSNs. To some extent, this plan gives an approach to judge people in OSNs without real interactions, but based on the existing overall attitudes on particular people. Additionally, this plan can ensure the confidentiality of the potential relationships in which nobody can able to acquire the detailed connections between two end nodes. In opposition to those which distribute every individual's reputation online, we treat the notoriety esteem in our framework as a private issue that has been deliberately ensured.

In this paper [8], authors propose FindU, the first privacy-preserving personal profile matching schemes for mobile social networks. In FindU, a starting client can discover from a group of clients the one whose profile best matches



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

with his/her; to confine the risk of privacy exposure, only important and, insignificant data about the private attributes of the participating users is exchanged. Several expanding levels of client privacy are defined, with diminishing amounts of exchanged profile data. Utilizing secure multi-party computation (SMC) systems, they propose novel protocols that acknowledge two of the client privacy levels, which can also be personalized by the users.

Table 1: Survey Table

Sr. No.	Title	Problem Discussed	Method Used	Advantages	Disadvantages
1.	A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks, ieee transactions on dependable and secure computing, vol. 12, no. 4, july/august 2015	Propose a trust-based privacy-preserving friend recommendation scheme for OSNs, where OSN users apply their attributes to find matched friends, and establish social relationships with strangers via a multi-hop trust chain.	Trust-based privacy-preserving friend recommendation scheme	Improve security and feasibility of the proposed scheme.	It is limited for only Online Social Networks applications
2.	P2P-iSN: A peer-to-peer architecture For heterogeneous social networks, in IEEE Netw., vol. 28, no. 1, pp. 56–64, Jan./Feb. 2014	Propose a Global Relationship Model (GRM) to capture the relationship strength between users and then develop a searching mechanism, namely i-Search, to find the optimal social path between any two users who are meaningfully connected in heterogeneous SNSs.	peer-to-peer architecture, namely P2P-iSN	Find the optimal social path between any two users who are meaningfully connected in heterogeneous SNSs	Need appropriate privacy protection and incentive mechanisms must be in place.
3.	Estimating Age Privacy Leakage in Online Social Networks, in Proc. IEEE Conf. Comput. Commun., 2012, pp. 2836–2840	Perform a large-scale study to quantify just how severe the privacy leakage problem is in Facebook.	Privacy leakage & Iterative method	Greatly reduce Privacy leakages in its service.	It found that for most users, including private users who hide their friend lists, it is possible to Estimate ages within a few years.
4.	Talash : Friend Finding In Federated Social Networks, in Proc. Linked Data Web, 2011, pp. 1–8	Try to find known acquaintances and new interesting friends on a Federated Social Network (FSN) , using StatusNet as their platform	Friend Finding Algorithm	Each User controls his presence on the internet and can interact with other Users using a set of protocols such as the O Status Suite.	This fail to consider users' privacy concerns on both identity and their social attributes.
5.	RelationGram: Tie-strength visualization for user-controlled online identity authentication, in Proc. 17th Int. Conf. Financial Cryptography Data Security, 2013, pp. 69–77	Consider the specific problem of how users can securely authenticate online identities.	RelationGram: a tie strength visualization from a trust graph	tie-strength visualization is a useful primitive for online identity authentication	Studies required because people's inherent altruism that explains Internet phenomenon's such as Wikipedia would also encourage users to share their tie strength visualizations, because little burden is required on their part, and they can help their friends to befriend each other with more safety.
6.	PriMa: A comprehensive approach to privacy protection in social network sites, Ann. Telecommun., vol. 69, nos. 1/2, pp. 21–36, 2014	Propose PriMa (Privacy Manager), a privacy protection mechanism that supports semi automated generation of access rules for users' profile information.	PriMa privacy policy generation	Enhance the precision of the privacy preference propagation process by leveraging machine-learning techniques.	Lack of mutual content
7.	A multi-hop privacy-preserving	Propose a novel reputation system which allows users to find potential	privacy-preserving reputation scheme	Perfectly hide the detail routing information from	Derivation of the reputation value on the designated reputation path



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

	reputation scheme in online social networks, in Proc. IEEE Global Telecommun. Conf., Dec. 2011, pp. 1–5	connections between unfamiliar people based on the most updated friend list of each user in OSNs		the intermediate nodes along one path.	as an open problem
8.	FindU: Privacy-preserving personal profile matching in mobile social networks, in Proc. IEEE 30th Conf. Comput. Commun., Apr. 2011, pp. 2435–2443	Propose FindU, the first privacy-preserving personal profile matching schemes for mobile social networks.	Fully distributed privacy-preserving profile matching protocols	This schemes are not only secure under the HBC model, but also prevents certain active attacks	Time Consuming Process.

### III. PROPOSED ALGORITHM

#### A SYSTEM ARCHITECTURE

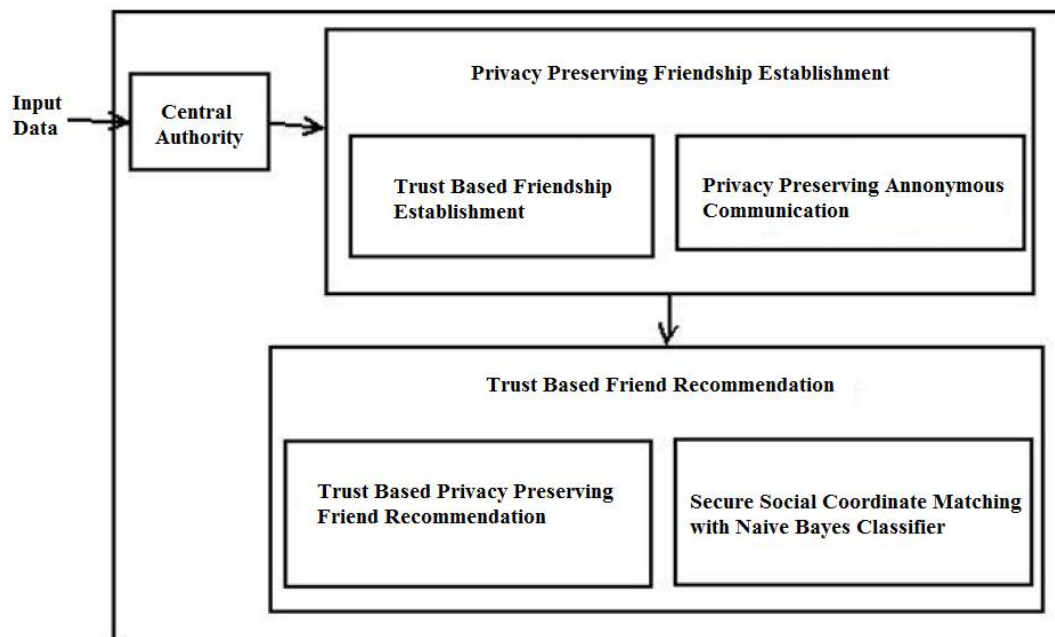


Fig.1. System Architecture

Online social networks (OSNs) provide people with an easy way to communicate with each other and make new friends in the cyberspace. Unfortunately, privacy concerns raised in the recommendation process impede the expansion of OSN user's friend circle. Some OSN users refuse to disclose their identities and their friend's information to the public domain. To overcome this problem, use a privacy-preserving trust-based friend recommendation scheme for online social networks, which enable two strangers establish trust relationships based on the existing 1-hop friendships. Proposed system includes:

1. We utilize OSN user's social attributes and trust relationship to develop the friend recommendation scheme in a progressive way while preserving the privacy of OSN user's identities and attributes.



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

2. We use OSN users close friends to establish anonymous communication channels. On the 1-hop trust relationships, we extend existing friendships to multi-hop trust chains without compromising recommender's identity privacy.

3. Our trust level derivation scheme enables strangers to obtain an objective trust level on a particular trust chain.

4. Extensive trace-driven experiment is deployed to verify the performance of our scheme in terms of security, efficiency, and feasibility.

5. Use trust score Calculation for estimate the trust between users.

## IV. CONCLUSION

From this survey we conclude that the privacy becomes major concern issue in friend recommendation system. Because in such system, for recommendation, users personal information is utilized, like users friend list, name, email id etc. This will utilized by unauthorized entities. Therefore the privacy preserving friend recommendation becomes essential feature in online social networking sites. This paper studies some recent methods for recommendation. We also make the comparative analysis of these systems on the basic of technique used, advantages and their disadvantages. These limitations become features challenges in this field.

## REFERENCES

- [1]Chi Zhang, "A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks", *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, July/August 2015.
- [2] P. Lin, P.-C. Chung, and Y. Fang, "P2P-iSN: A peer-to-peer architecture for heterogeneous social networks," *IEEE Netw.*, vol. 28, no. 1, pp. 56–64, Jan./Feb. 2014.
- [3]R. Dey, C. Tang, K. Ross, and N. Saxena, Estimating age privacy leakage in online social networks, in *Proc. IEEE Conf. Comput. Commun.*, 2012, pp. 2836-2840.
- [4] Raturaj Dhekane, Brion Vibber, Talash: Friend Finding In Federated Social Networks Hyderabad, India, 2011.
- [5]T. H.-J. Kim, A. Yamada, V. Gligor, J. Hong, and A. Perrig, "RelationGram: Tie-strength visualization for user-controlled online identity authentication," in *Proc. 17th Int. Conf. Financial Cryptography Data Security*, 2013, pp. 69–77.
- [6]A. Squicciarini, F. Paci, and S. Sundareswaran, "PriMa: A comprehensive approach to privacy protection in social network sites," *Ann. Telecommun.*, vol. 69, nos. 1/2, pp. 21–36, 2014.
- [7]L. Guo, X. Zhu, C. Zhang, and Y. Fang, "A multi-hop privacy-preserving reputation scheme in online social networks," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2011, pp. 1–5.
- [8]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.