Survey on Preserving Privacy using Encrypted Communication in Online Social Networks

Swati Pulkurte
Dept. of Computer Engineering SKNCOE, Savitribai Phule Pune University, Pune, India.

V. V. Dakhode
Assistant Professor, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, India.

ABSTRACT
The popularity of online social networks is constantly increasing due to various advantages such as online communication and sharing information among friends. Online social network applications severely suffer from various issues such as security, privacy. However, users want to make new friends to enlarge their social connections as well as to obtain information from thousands of people. Extensively in the recent past Friend recommendation is a very important application in many online social networks (OSNs). There is a strong need to develop privacy-preserving friend recommendation methods for social networks as user privacy is main concern nowadays. Online Social Networks (OSNs), not only attract millions people to use every day but also greatly extend OSN users social circles by using friend recommendations. This paper is motivated by need of friend recommendation without revealing privacy and security while using social networks.

Keywords
Online social networks, data privacy, trust, privacy protection algorithms.

1. INTRODUCTION
The Internet has produced different types of information sharing systems, including the Web. Online sharing network (OSNs) have experienced tremendous growth in recent years such as Facebook, YouTube, twitter, and LinkedIn, has produces large amount of social data containing personal and private data about each individual users. Online social networks (OSNs) provide people with an easy way to connect with each other and make new friends in the cyberspace. Similar to what people commonly do in real life, OSN users always try to expand their social circles in order to satisfy various social demands, e.g., business, freedom, 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 we consider the possibility of establishing a multi-hop trust chain two strangers by using existing 1-hop trust of existing friends on the OSNs. Online social network applications severely suffer from various issues such as security, privacy. Online social networks are organized around users not like the Web, which is largely organized around content. Social network analyses have enhance the research in developing various recommendation algorithms. Researchers from different computer science disciplines have undertaken some of the problems that arise in OSNs and propose a diverse range of privacy solutions, including software tools and design principles.

2. MOTIVATION
OSN user profiles represent a rich source of personal information, including demographic information, users’ interests and their social relations. Privacy threats resulting from this direct exposure of personal information have been widely publicized and researched. Online social networks have experienced a surge in popularity recently, particularly because they allow users to share music, photographs, home cinemas, and blogs with friends and family rapidly and easily. Two of the most popular social networks today, myspace.com and facebook.com, permit users to effortlessly share their data with their family, friends, coworkers, and classmates. Hence there is a need to preserve confidentiality of data in OSN. Some are the terms related to preserving data.

2.1 Data Privacy
The word privacy has many subtly different meanings, each with their own definition. This ranges from "personal privacy" to “Information Privacy”, around which privacy on the Internet in general revolves. Information Privacy is "an individual’s claim to control the terms under which personal information, identifiable to the individual – is acquired, disclosed or used."

2.2 Trust
Trust can be seen as a “mental short-cut” that enables users to promptly engage in trust-related behaviors”, e.g. the provision of personal information. In the organizational trust literature, trust is mostly defined as a belief or expectation about the other (trusted) party, or as a communication intention or willingness to depend or rely on another party, united with a sense of vulnerability or risk if trust is disrupted.

3. LITERATURE SURVEY

A mobile social networking platform to implement friend of friend detection algorithm is introduced in [5]. This paper concentrated on different issue by introducing a decentralized method and also presented a technique that seamlessly integrates the friendship study of traditional social networking websites into purely decentralized environments. Some privacy issues arises in proposed approach but considering popularity in server based systems proposed mechanism might become an important feature in upcoming mobile social applications

[2] FindU Technique
In this technique first security protecting individual profile coordinating plans for mobile informal communities referred in [12]. In FindU, an initiating client can discover from
3.1 Trust Level
The trust level in the existing system is defined as the reliability trust [1] with propagative property, and it is a numeric value $T \in [0,1]$ between pair-wise OSN users, where 0 denotes lowest trust level and 1 represents the highest level with full trust, respectively. In [1] paper , Pederson commitment scheme to preserve the trust level between pair-wise OSN users. But trust level approach is not very precise to define trust. It defines either “yes” or “no” statement.

3.2 Trust Score
Another approach which states trust approximately is by calculating trust score. Trust Score will be in the range of 0 and 1. The framework computes trust considering EX, CI and I as the three principle qualities that helps in calculating the trust in [11]. Likewise, out of these three, CI and I are determined by the framework and EX is the information from the client. The client appends the security level with every information that she transfers. As the security level is same as the limit trust score, the decision is made to permit the entrance or deny the access contingent on the characterized Trust Rule which contains the comparison between the trust score of each friend in the friend list and the edge trust score given as the information from the client.

3.3 Trust-Based Friend Recommendation
The trust-based friend recommendation includes two major sub protocols, secure social coordinate matching and friend recommendation process. Based on the matching results (inner product) of social coordinates and established trust relationships, recommenders determine their recommendation decision on whether continues to query their friends or not.

4. GAP ANALYSIS

<table>
<thead>
<tr>
<th>Sr.no</th>
<th>Paper</th>
<th>Technique used for</th>
<th>Achieved</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Preserving Privacy in Social Networks Against Neighborhood Attacks [3]</td>
<td>Identify privacy attacks such as neighborhood attacks.</td>
<td>High feasibility.</td>
<td>Handles only 1-neighborhoods attack</td>
</tr>
<tr>
<td>3</td>
<td>Estimating Age Privacy Leakage in Online Social Networks [4]</td>
<td>estimating birth year, which is a fundamental human attribute</td>
<td>High accuracy for several classes.</td>
<td>many older users, age is difficult to estimate accurately</td>
</tr>
<tr>
<td>5</td>
<td>Enforcing Access Control in Web-based Social Networks [7]</td>
<td>access control model using semi decentralized architecture</td>
<td>Access control on client side</td>
<td>Access control enforcement is carried out at client-side not at server side.</td>
</tr>
</tbody>
</table>
5. PROPOSED WORK

The proposed system establishes trust based relationship between the users with preserving privacy of the users. The input here is the social attributes of the OSN users.

First, the privacy preservation friendship is established by encrypting the social attributes of the users. It is done by the central authority (CA). CA takes attributes from OSN users and encrypts it.

Secondly, the trust based friend recommendation is done by securing communication of users. It is done by checking whether the request for communication is from trusted user or not.

The contribution lies in calculating trust score (refer fig 5.1) by which the user who wants recommendation will able to check how much the recommender trust worthy.

6. CONCLUSION

This paper presented an all-inclusive survey of recommendation with concern to privacy. The main features, the advantages and disadvantages of each recommendation algorithm are described. As per survey, a strong need to develop privacy-preserving friend recommendation methods for social networks because user privacy is challenging issues nowadays. Paper proposed trust based privacy preserving for friend recommendation. The future scope of this proposed work is trust score calculation between various friends and establishing a secured communication link between strangers via a secured trust based privacy preserving friend recommendation system.

7. REFERENCES

[1] Linke Guo, Member, IEEE, Chi Zhang, Member, IEEE, and Yuguang Fang, Fellow, IEEE, "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.


[12] Ming Li, Ning Cao, Shucheng Yu and Wenjing Lou, “FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks”.