International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey on Online Social Networks for Privacy-Preserving Friend Recommendation Scheme

Aneesha P A

M.Tech, KMEA, Computer Science and Engineering, Mahatma Gandhi University, Kerala, India

Abstract: ***In our daily life, Online Social Networks (OSNs) become an important part. Thousands of million people that use OSN every day by friend recommendations, so OSN users social circle extend greatly. OSNs put forward attractive means for information sharing and digital social interactions, therefore increase a number of security and privacy issues. For privacy protecting scheme it prevents the revelation of identity of users but also the revelation of preferred features in users profile. An individual user can select features of his/her profiles that should not be disclosed to others. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. Usually social networking is represented as graphs, users are nodes and features are labels.***

Keywords: Online Social Network, Privacy, Trust, Social Relationship.

1. Introduction

Now a days we seen significant growth and receiving much more awareness in Online Social Networks(OSNs). More people are allied to the internet and social networks are vital part of our daily life.OSN users communicate in various ways and share many aspects of their lives via OSNs. OSN is a web-based service that allows individuals to :

- Within the service construct a public or semipublic profile,
- Articulate a list of other users with they share a connection,
- Within the service view and traverse their list of connections and those made by others

Two types of linked data that operate on OSNs, they are : Profiles and Connections. Profile is tied to a user and representation to the outside world. A Connection that exist between two users and of several types, like friend, colleague, fan etc. A collection of connections that are represented by graphs. OSN offers other forms of information related to users, depending on the additional services they are messages, multimedia, tags, preferences, groups etc.

2. Literature Survey

Now a days there are several Online Social Networks (OSNs) such as face book, Twitter, LinkedIn etc. Trust and Privacy are the important issues in OSNs. Based on three criteria trust can be categorized, they are: Trust information collection, Trust value assessment, Trust value dissemination shown in Fig 1. [1]Trust information collections are based on three sources, attitudes, behaviors, experiences; According to the data model trust value assessment are namely graph, interaction, and hybrid; trust value dissemination are namely trust-based recommendation and visualization models. Privacy settings based on profile information. Based on statistical data, to predict expected user preferences profile information is used. In this section we include a survey of privacy and trust in Online Social Networks(OSNs).

Thapa A,Salinas [2] proposes a paper called Asymmetric Social Proximity Based Matching Protocols for Online Social Networks. To redefine the OSN model they contain the community structures and between two users they propose a realistic asymmetric social proximity measure. In proposed asymmetric social proximity, it contains three primitive matching protocols, better than the previous works users can protect privacy and provide different privacy levels. The communication and computation cost of these protocols are analyzes. Using real social network data it validates asymmetric proximity measure. To evaluate the performance communication cost, computation cost, total running time and energy consumption they conduct an broad simulations.

C.Zhang, J.Sun, X.Zhu, Y.Fang [3] proposes challenges and opportunities in OSN. They proposes a privacy and security challenges in OSN. Now a day's several exponential growth in Online Social Networks Such as Facebook, Myspace, Twitter etc. When creating a profile by joining peoples on social networking sites. profile is a list of identifying information. Here friends are connecting to other friends or members by sending a friend message. Different types of OSNs the visibility of a users profile varies. OSNs are centralized and web- server based. Commercial OSN providers like Facebook Inc., LinkedIn Corp., XING AG provide all functionalities like storage, maintenance and access to OSN. The given figure 2 shows the client server architecture of OSN.

To communicate Via the client-server architecture, it requires the internet connectivity to users via the remote central server.

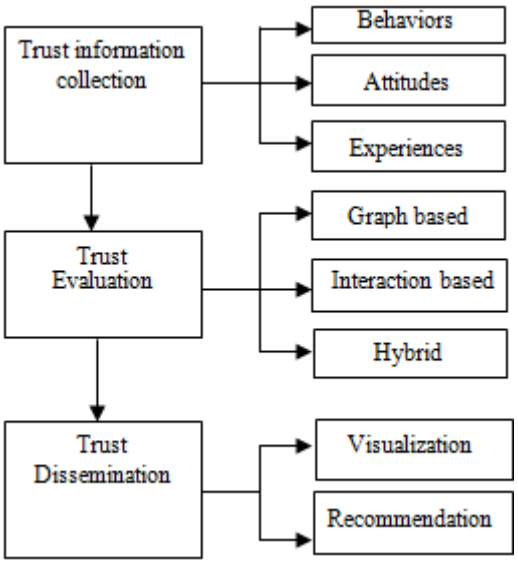

Figure 1: Social trust system classification

In online social graph model contain a new entity called OSN provider is added OSN user has a social relationship with her. OSN has contain several wide categories: Users identity anonymity, Users personal space privacy, users communication privacy.

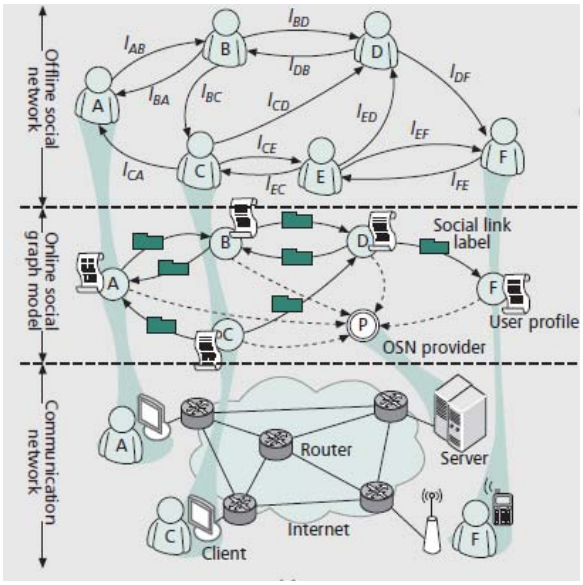

Figure 2: Client-server Architecture

- Users identity anonymity - In different types of OSNs protection of a users identity changes accordingly. The Dating sites like friendster, a weak pseudonymity is created, the first name of the member is visible to others, and not her last name.
- Users personal space privacy - Across different types of OSNs visibility of a users profile also varies. OSNs like MySpace allow users to choose their profile to be public or friends only. To hide thier friend lists, MySpace users hacked their profiles and LinkedIn allows users to select thrashing their friend lists.
- Users communication privacy - To the network operator OSN users disclose their personal information or OSN provider the using the network itself, that is data such as time, location of connection.

L.Guo, X.Zhu, C.Zhang and Y.Fang[4] proposed that People to communicate with other people or share their own profiles on their web pages through Online Social Networks such as Facebook, Twitter etc. Reputation system is the main functionality of OSNs. Reputation is generally means of collective measure of trustworthiness. It is based on the referrals or ratings from other members in a community. An individual's trust can be derived from a mixture of received referrals and personal experience. The below figure 3 shows the trust transitivity principle.

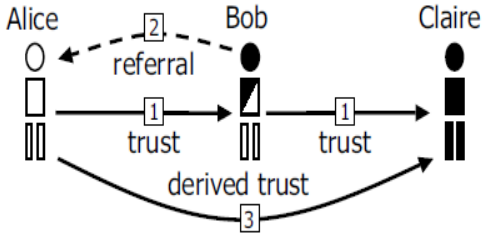

Figure 3: Trust transitivity principle

Here they propose a privacy-preserving reputation scheme for Online Social Networks, a pair of unknown nodes which securely find a reputation path and by implementing anonymous reputation value transmission procedure, telling globally one reputation value to another. To form the reputation path to each node here implements a structured encryption with data update. Detail routing information is perfectly hide from the intermediate nodes along one path. Without disclosing each hop's values pass the intermediate nodes reputation value.

A.Cutillo, R.Molva and T. Strufe[5] proposes another concept called Safebook. Online Social Network applications rigorously suffer from Various security and privacy exposures. This method propose a new approach to tackle privacy and security problems. Safebook is adopt a decentralized approach and privacy preserving Online Social Network application. Decentralization and exploiting real-life trust are the two design principle in safebook. For privacy and security various mechanisms are integrated into Safebook, to preserve user's privacy, data integrity and availability they provide data storage and data management functions. Figure 4 shows three different levels of Social Networking Services.

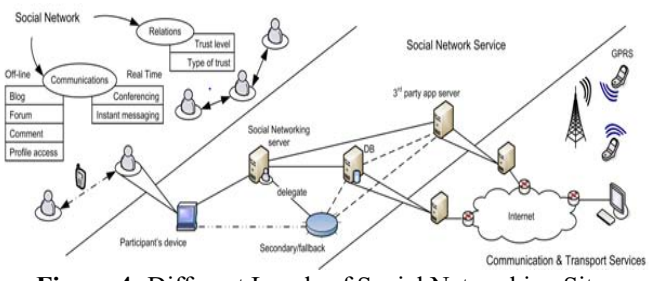

Figure 4: Different Levels of Social Networking Sites

They are Social Network (SN), Social Networking Service (SNS), Communication and Transport(CT) levels.

- Social Network level - the digital representation of members and their relationships
- Social Networking Service - the application infrastructure, managed by the SNS provider
- Communication and Transport - Communication and transport services as provided by the network.

Safebook consist of three-tier architecture, They contain
- SN level of the OSN implementing the user-centered Social Network layer;
- SNS services implementing a Peer-to-peer substrate;
- the internet, representing the CT level.

Safebook, a decentralized and privacy preserving SNS.

W.Chen and S.Fong [6]proposes a frame work, Collaborative filtering framework. Social network has grown in tremendous popularity. In recommender system, recommendation to a user are by gathering similar users and filtering their information over a network. Over a social network Collaborative filtering CF gathers tastes of similar users; social network provides a collaborative social environment. In Social networking environment CF is believed worked well, due to decentralized and virtual nature of social network, measuring trust is a challenging task. For example, in Facebook users can be categorized their friends as family, friends, and friends-of-friends. colleagues, members of same group etc these are the other relations that have done in the facebook. Figure 5 shows an example of clustering friends on facebook, by relations via a visualization program.

Two types of filtering techniques that are used in recommender system:
- item based recommender system
- collaborative-based recommender system

In item based filtering, attributes of items that a user purchased favored before and attempts to find other items that have similar attributes and recommend them to the user. Collaborative filtering that focuses on the user data. That makes automatic predictions about the interests of a user by collecting information from many users who shared similar background and preparation.

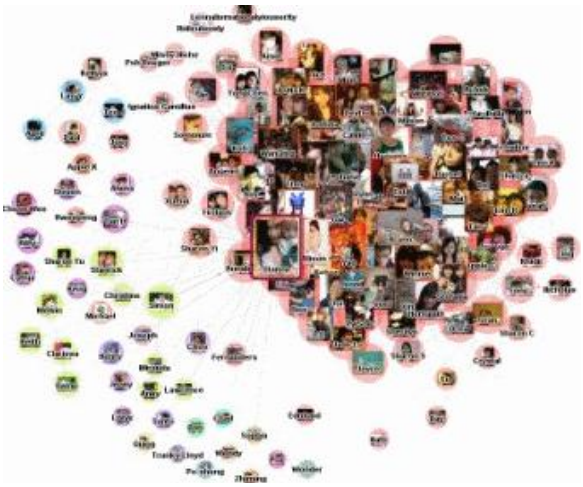

Figure 5: Visualization of friends on facebook

Panda et al. [7] used a new efficient definition of privacy called 1-diversity on preserving privacy in collaborative social network data. it has been identified that 1-diversity social network still may leak privacy as an adversary may have prior knowledge about the sensitive attribute value of an individual. Li et al. [8] propose dto preserve relationship privacy between two users one of whom can be identified in the released social network data. 1-diversity anonymization model has been defined to preserve users relationship privacy. Two graph manipulation algorithms, MaxSub and MinSuper, have been proposed to achieve 1-diversity anonymization.

Ford et al [9] proposed a new algorithm for enforcing p-sensitive k-anonymity on social network daat based on a greedy clustering approach. Narayanan et al. [10] proposed a developed Re-identification algorithm for anonymized graphs. it is validated for Flicker and Twitter. Lijie et al [11] studied link identification attack in which the adversary attacks using liking probability, here t-confidence has been proposed.

Lan et al. [12] proposed an approach for preserving privacy of social networks which can be represented as bipartite graphs. Sun et al. [13] proposed a privacy-preserving method for sharing data in social networks, with efficient revocation for preventing a contacts access right to the private data once the contact is removed from the social group and can be used as a plug-in for Facebook.

3. Conclusion

Now a days there are several Online Social Networks(OSNs) such as Facebook, Twitter, MySpace etc. They have tremendous growth in social networks. Privacy and security are the important issues in the OSN. Trust in OSN is the important fact in it. Trust can be categorized into three criteria: trust information collection, trust value assement, trust value dissemination. Privacy are the most important fact in OSN. Friend recommendation is the most application in many OSN.

References

[1] Sherchan, W., Nepal S and Paris C,"A Survey of trust in social networks" ACM Comput. Sury. 45,4 Article 47 (August 2013), 33 pages.
[2] Thapa, A.; Li, M.; Salinas, S.; Li, P. "Social Proximity Based Private Matching Protocols for Online Social Networks" Publication Year: 2014.
[3] C. Zhang, J. Sun, X. Zhu, and Y. Fang “Privacy and security for online social networks: Challenges and opportunities” IEEE Netw., vol. 24, no. 4, pp. 13–18, Jul./Aug. 2010
[4] 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.
[5] A. Cutillo, R. Molva, and T. Strufe, "Safebook: A PrivacyPreserving Online Social Network Leveraging

on RealLife Trust",‖ Communications Magazine, vol. 47, no. 12, 2009, pp. 94–101.
[6] W. Chen and S. Fong, "Social network collaborative filtering framework and online trust factors: A case study on facebook" in Proc. 5th Int. Conf. Digital Inf. Manage., Jul. 2010, pp. 266–273.
[7] G.K.Panda, A. Mitra, Ajay Prasad, Arjun Singh, Deepak Gour, "Applying l-Diversity in anonymizing collaborative social network" In: International Journal of Computer Science and Information Security, Vol 8, Issue 2, pp 324 - 329, 2010.
[8] Na Li, Nan Zhang, Sajal K. Das, "Relationship Privacy Preservation in Publishing Online Social Networks", In Proc. of IEEE International Conference on Privacy, Security, Risk, and Trust, Boston, MA, pp 443-450, 2011.
[9] Roy Ford, Traian Marius Truta, and Alina Campan, "P-Sensitive K-Anonymity for Social Networks".
[10] A. Narayanan, V. Shmatikov, "De-anonymizing social networks", In Proc of 30th IEEE Symposium on Security and Privacy, Berkeley, CA, pp 173-187, 2009.
[11] Z. Lijie and Z. Weining, "Edge Anonymity in Social Network Graphs," in Proc. of International Conference on Computational Science and Engineering CSE '09, pp 1-8, 2009.
[12] Lihui Lan, Shiguang Ju Hua Jin, "Anonymizing Social Network using Bipartite Graph", In Proc. of International Conference on Computational and Information Sciences (ICCIS), Chengdu, pp 993 - 996, 2010.
[13] Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang, "A Privacy-Preserving Scheme for Online Social Networks with Efficient Revocation", In Proc. of INFOCOM, IEEE, San Diego, CA, pp 1-9, 2010.

Author Profile

Aneesha P A received the Bachelor of Technology degree in Computer Science and Engineering from Mahatma Gandhi University of Science and Technology in 2013 and currently doing Master of Technology in Computer Science and Engineering from Mahatma Gandhi University.