Research Article

Literati Journals
Empowering Researchers

A Survey on Defined Circle Friend Recommendation Policy for Growing Social Media

Shamily Varghese E,[1*] Sushma Ravindra Y[1]

Abstract: Today social media has grown with a fast and has spread wide across the globe with a unique user profile as nodes under an Online Social Network (OSN). This paper focus on the current trends on Social Media and a brief survey on OSN with Friend recommendation Scheme. The OSN users under various social domains such as Facebook, Twitter, and Google have been assigned a unique identification as to establish under the network and communicate under single and multi-hop communication. Today the individual share they daily life affairs on social media and a concern is created on preserving the policies of privacy. In this survey paper a summary on various schemes and its applications are discussed for my concern of work.

Asian Journal of Management Sciences,
Volume 4, Issue 7
Published on: 20/08/2015

Cite this article as: Shamily Varghese E, Sushma Ravindra Y. A Survey on Defined Circle Friend Recommendation Policy for Growing Social Media. Asian Journal of Management Sciences, Vol4(7): 58-60, 2016.

INTRODUCTION

Social media and OSN creates a platform for the users from different walks of life to get connected on a single platform to share they views, comments and social life such as feelings and updates. This platform connects the people on friend list via friend recommendations for the profile. The profile of an individual shall consist of private and public information's such as posts and personal information. Currently OSN insist the existing members to recommend the new members the friends under the scheme of friends of friend (FoF). A several social media related work has been proposed [1, 2] which spot lights on the appeal of social relationships and status on the upcoming post under sentimental analysis and emotional analysis. A huge bigdata approach has been highlighted for the OSN data, as the data collected per hour roughly various from 2.3 TeraBytes to 2.5 TeraBytes. Hence we can easily append Big Data techniques on data analysis and mining. This approach makes the network unprotected and slow.

The major threat to OSN is identity misusing and Spoofing of one's personal data under cyber malfunction. Today we use OSN for more than buzzing out updates and post. These include personal message sharing under friend circle, group chat for a team of client and a common likes on similar page of an untrusted profile.

Considerably, the social media has covered the entire urban and metropolitan areas with its network for large data and user connectivity. In general a network of a small area consists of 1500 and more profiles with unique ids. This research has made the entire research community understand the importance of OSN and its data mining asset.

The motivation of this paper is to achieve a better performing scheme on OSN under a untrusted private Big Data environment for initial friend recommendations to hyper active and false friend profile bonding.

This paper is organized with an Introduction on an OSN in section I and followed by a comparative review research in Section II and is concluded with a summary in Section III. This review is solely for M.Tech thesis and claims no right on data and statistics neither shared under the subject nor claim any copyrights for the same.

LITERATURE REVIEWS

As discussed from the section I, the OSN has a wide user network with multiplying big data. This has made the researches propose many schemes for data hiding, privacy preserving and cybercrime reduction. Hence to start with we shall discuss privacy issues in the OSN.

1. OSN v/s Privacy

Many approaches has been claimed to showcase the privacy preserving issues on an OSN as it is forging the user attributes and ID's for fake profile creation. In this Fog et al [3][4] has disused a remedy under a game theory terminology. This is to model the privacy management of a shared data which has single hop connection under FoF scheme. This acts as a thread

[1]Reva Institute of Technology and Management, Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Near Border Security Bustop, Bengaluru, Karnataka-560064, India.
Email: shamilyvarghese@gmail.com
*Corresponding author

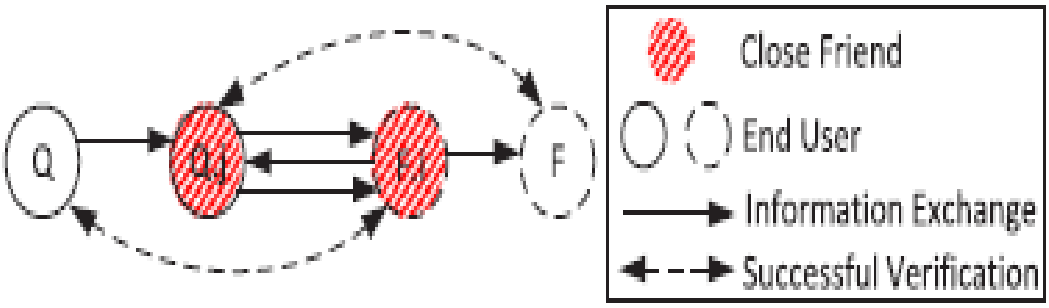

Figure 1: PPAC Scheme

under the interference of user profile based on social relationships, which is considered a very intense attack on identifying a real identity of a user under a positive attribute set. Apart from this, a thread on malfunctioning of an individual account shall also be considered.

2. Friend Recommendation Scheme

Consider AA and BB are two independent users sharing a common bond of friendship with CC. accordingly the attributes of each user matches with an personal relationship status such as joining same intermediate school or an graduated fellows from a YY university.[6, 5]

Apparently, in a modern era intelligent OSN, an auto recommendation is been given to AA and CC to add BB among they friend circle as the attributes matches with the user. This FoF scheme is appended as it generally specifies the ratio of connectivity instead of trust and privacy management. [5]

3. Trust Based Friendship Recommendation Scheme

A TBFR Scheme deals with assigning a higher priority values for a close friend circle to make the communication proactive and protected. This scheme involves in assigning Multi Hop function on a level L= [H, €] where H is the Hop ratio of trust and € denotes the friend domain of trusted attribute sets. This scheme is preferred with a comparative of other scheme under an unprotected network from [8][9] as to achieve a higher reacting performance rate.

4. Privacy Preserving Anonymous Communication Scheme

Under OSN an occasional chat is preferred among the users sharing a particular attributes but no bond of friendship. In such an occasion an area confidently is been assigned on the trust connection of a recommended or a mutual friend as shown in Figure 1. This includes bonding ratio of OSN with PPAC Scheme.

Trust Based Friend Recommendation Scheme

As discussed in the previous sections of this paper, five various schemes and its attributes for OSN has been discussed. In this section, TBFR Scheme is discussed from the concern of future enhancement and development.

This scheme consists of two protocols, Secure Social Coordinates matching and trusted friend recommendation process. Under SSC matching we append KNN algorithm to assign the trusted and safe coordinates in the system for secure connection establishment and management. With this a generic non-isolated and a mutually depended quadrants has been identified. The second protocol, i.e., fetching friend recommendation has to be initiated as to achieve a mutual coordinates upon whom a trusted algorithm can be supported.

CONCLUSION

From the brief survey on Online Friend Recommendation Schemes and the affecting parameters here I perform a comparative analysis on how TBFR scheme has a positive impact upon the FoF and PPAC scheme. The major objective of this paper was to perform a brief survey on these techniques to highlight the agenda of work progress and move ahead on the major thesis contribution of M.Tech.

According to my survey, TBFR scheme has a higher reliability factor with an increased trusted margin in OSN. From the initial parameters of fetching an attribute to the extreme parameter of analyzing a mutual and trusted bounded friend to establish a secure communication between two unbounded users makes TBFR a remarkable and potential scheme in social media and data management under trusted domain.

REFERENCES AND NOTES

1. B.Carminati, E. Ferrari, and A. Perego, “Enforcing access controlin web-based social networks,” ACM Trans. Inf. Syst. Security, vol. 13, no. 1, pp. 6:1–6:38, Nov. 2009.
2. C. Squicciarini, M. Shehab, and F. Paci, “Collective privacymanagement in social networks,” in Proc. 18th Int. Conf. WorldWide Web, 2009, pp. 521–530.
3. 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.

4. Mislove, B. Viswanath, K. P.Gummadi, and P. Druschel, “You are who you know: Inferring user profiles in online social networks,” in Proc. 3rd ACM Int. Conf. Web Search Data Mining, 2010, pp. 251–260.
5. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, “Measurement and analysis of online social networks,” in Proc. 7th ACM SIGCOMM Conf. Internet Meas., 2007, pp. 29–42.
6. Zhang, X. Zhu, Y. Song, and Y. Fang, “A formal study of trustbased routing in wirelessad hoc networks,” in Proc. IEEE 29th Int. Conf. Comput. Commun., Mar. 2010, pp. 1–9.
7. 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. T. H.-J. Kim, A. Yamada, V. Gligor, J. Hong, and A. Perrig, “Relation Gram: Tie-strength visualization for user-controlled online identity authentication,” in Proc. 17th Int. Conf. Financial Cryptography Data Security, 2013, pp. 69–77.
9. L. Backstrom, E. Sun, and C. Marlow, “Find me if you can: Improving geographical prediction with social and spatial proximity,” in Proc. 19th Int. Conf. World Wide Web, 2010, pp. 61–70.
10. 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.
11. M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, “Veneta: Serverless friend-of-friend detection in mobile social networking,” in Proc. IEEE Int. Conf. Wireless Mobile Comput. Netw. Commun., Oct. 2008, pp. 184–189.