

Survey on Trust Based Secure Friend Recommendation System for OSN Using C4.5

Pooja Jadhav¹, V.M.Barkade²

¹Department of Computer Engineering, Rajashri Shahu College of engineering , Pune, Savitribai Phule, Pune University, Pune, Maharashtra, India

²Department of Computer Engineering, Rajashri Shahu College of Engineering, Pune, Savitribai Phule, Pune University, Pune, Maharashtra, India

ABSTRACT

To connected with world online communication and sharing information using the social network sites become a very famous in recent days. But it's very challenging job for social network site to provide the privacy and security. Active OSN user privacy protection by using proposed method which is allowing them to enhanced their social networks. To carry out the secured social directed coordinating, existing framework use the secure kNN plan. Yet, with the help of KNN, distance based learning is not clear which sort of distance to use and their component to use to give the best results and calculation expense is very high. This paper overcome this limitation and increased the outcomes precision, using framework utilizes C4.5 classifier for secure social coordinate matching. Through security analysis and trial outcomes, and demonstrate that the security, feasibility and precision.

Keywords : Online, Social Network, Multi Hop Relationship, Trust Value, Privacy, C4.5Classifier.

I. INTRODUCTION

For sharing of data there are several of systems are created by the internet such as Web. From those entire systems Online Social Network (OSN) is most popularly utilized on internet by large number of users. OSN has become very much popular as well as now days have become standout from the most common destinations on the Web. Due to OSNs large group of development are encountered such as Facebook, YouTube, twitter, Linked In has created very huge amount of data social data having personal and also private data about every individual user.

An application on online social network has various issues like security as well as protection. But the users want to create new friend to increase their social associations and also for getting information from multiple individuals. Comprehensively in the later past Friend proposition is an essential in various

online casual associations. Online social network are sorted out around users not care the Web, which is, all things considered, created around substance. OSNs give simple procedure for communication and make new friends in web. Shockingly, restricting the development of OSN user's friend circle, security issues brought up in the suggestion procedure. Some OSN user not allows to uncover their identities and their friends data to general society domain. To solve this issue, for OSNsutilize a privacy-preserving trust based friend recommendation system, which permittwo unknown persons build up trust relationships depending on 1-hop friendships.

II. LITERATURE REVIEW

In this paper [1], author tries to address this issue by presenting a decentralized approach that can checks that social neighborhood of a client for discover

friends of friends. Alternatively, just apply data about the clients of the framework, this techniques are depends on real friends. Satisfactorily addresses the privacy issues. . Similarly, author show VENETA, author proposed a new friend to friend detection algorithm in a mobile platform which contains different features.

In this paper [2] author firstly acknowledges a extraordinary substance of trust measurement and Quality –of- Service (QoS) based directing measurement. They shows the difference between trust measurement and trust-based distinguishing, the important logarithmic properties are used for trust metric that must have keep in mind the final motive to work effectively and preferably with particular summed up division vector on the other hand connection state directing conventions in WANETs.

In paper [3] author proposed the potential of social network by filtering the information. Collaborative Filtering (CF) is a suitable technique for systems on social networking websites, because Collaborative Filtering gathers tastes of identical users. On running CF on social networking websites is quantitative estimation of trust between friends. In this paper a framework of collaborative filtering on social network is proposed, on measuring trust factors by data-mining over a survey dataset provided by the Facebook Project. A trust factors can be used as input parameters in the CF algorithm. Facebook is taken as a case study.

In this paper [4], author indicates that it is not really knew how protection concern and trust impact social collaborations within an individual to individual communication destinations. By surly understanding an online diagram between individual to individual communication destinations, Facebook and MySpace, looked at impression of trust and protection concern, along with by capability to share data and develop new connections. Peoples from both local area networks reported a comparative level of security.

Peoples using facebook to communicate altogether more unmistakable trust and peoples are using it and were more active to share identifying information. The results of on communication on social networking sites, trust is not necessary in the creating of new connections as it is in eye to eye encounters. This study illustrate online connections can make in locals and seen the trust and security assurances are weak.

In paper [5] author used a FindU, FindU is a first security ensuring individual profile, FindU is co-coordinating plans for mobile informal groups. In FindU, an initial customer can find from a social affair of clients, whose profile best matches with his/her, the risk of contact simply fundamental and insignificant data about the private qualities of the taking an interest clients is traded. A few extending levels of clients security are described, with reducing measures of exchanged profile information.

In paper [6] author proposed, now a days, communicating and sharing information on social networking is famous but to provide privacy and security is more difficult. Due to this new friends are increased online. In this paper by using OSN's need of friend proposal not showing privacy and security. Existing KNN plan is used for to carry out the secured social directed coordinating. By using KNN, distance based learning is not clear which sort of distance to use and gives the best results and calculation expense is very high. The proposed framework use SVM classifier for secure social coordinate matching. Security analysis and trial outcomes, we demonstrate that the security, feasibility and precision of the proposed method and it is to anything existing one.

In this paper [7], author proposed Online social network like Orkut , YouTube, and Flickr are among the most standard locals on the Internet. A client gives a suitable technique for sharing, organizing and finding substance in LAN(Local Area Network). The major areas allow as recalling the features of social online features graph all over the scale. Considering

those charts is essential and modifying current systems. Layouts the new uses of online social community. This paper suggest a large-scale measurement analysis of the structure of various online social websites. From Flickr, YouTube, Live Journal, and Orkut online social networks author gathered information. In this paper author crawled the freely available client links one very website and getting a vast portion of each social community's graph. Author focused on different online social networks at scale.

In paper [8] author shows that OSNs is online service which is used to maintain social relationships, for this purpose multihop trust chain relationship followed by 1 hop trust relationship is used. A new technique KNN is used to maintain privacy. Where OSN users can find their matched friends by applying their attributes using multi hop trust chain.

III. SYSTEM ARCHITECTURE

To perfectly hide the identity and network address (IP or MAC address) of an OSN user, we assume each OSN user has a certain number of fully trusted friends, which will not reveal any secret information of a user with the particular ID. The assumption satisfies the circumstance in the real life or OSNs with secure channels. For example, people may have several closest friends whom they fully trust. In order to hide the network address and identity, users can route their packets to the destination via a specific trusted friend, and thereby hide their identities with the help of their close friends. Similarly, as a friend of Bob, Alice also obtains a set of pseudonyms to ensure anonymous communication during the recommendation process. However, different from close friends, we require OSN users assign different trust levels to each one of their 1-hop friends and define a map that maps the reliability trust level to an integer.

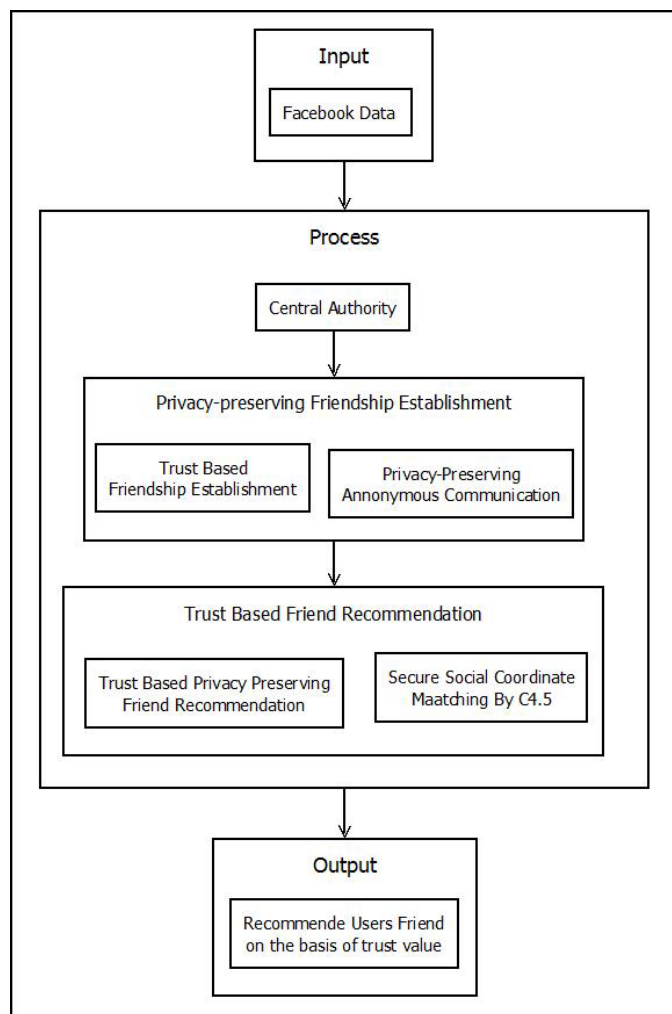


Figure 1 : System Architecture

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 continue to query their friends or not. To achieve the secure social coordinate matching, we apply these cure kNN scheme and modify it. In our scheme, users' social coordinates can be formed into a set of binary vector A. Binary vector Q is the social coordinate vector that contains query information, which can be any possible user's unique social coordinate in the OSN. The trust-based recommendation process should satisfy the above requirements, such that the trust chain could be set up according to the matching results and the trust requirement. The basic requirement of trust level

derivation process is securely collect the overall trust level based on each individual's value on the trust chain. According to the assumptions in the previous section, OSN users treat their trust levels on the friends as privacy and do not want to disclose.

IV. CONCLUSION

In this study, for online social networks this system use a privacy-preserving trust-based friend recommendation scheme. To carry out the secured social directed coordinating, existing framework use the secure kNN plan. Yet, with the help of KNN, distance based learning is not clear which sort of distance to use and their component to use to give the best results and calculation expense is very high. To overcome on this limitation and increased the outcomes precision, proposed framework utilizes C4.5 classifier for secure social coordinate matching. Through security analysis and trial outcomes, we demonstrate that the security, feasibility and precision of the proposed method are to have superior to anything existing one. Experimental results prove that the proposed system is more secure than the existing system, it perform better than the existing system.

V. REFERENCES

1. M von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, "Veneta: Serverless friend-of-friend detection in mobile socialnetworking," in Proc. IEEE Int. Conf. Wireless MobileComput. Netw.Commun., Oct. 2008, pp. 184-189.
2. C Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study oftrust based routing inwireless ad hoc networks," in Proc. IEEE 29th Int. Conf. Comput. Commun ., Mar.2010, pp.1-9.
3. W Chen and S. Fong, "Social network collaborative filtering framework and onlinetrust factors: A case study on Facebook," in Proc. 5th Int. Conf. Digital Inf. Manage.,Jul. 2010, pp. 266-273.
4. C Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacyconcern within social networking sites: A comparison offacebook and myspace," in Proc. 13th Amer. Conf. Inf.Syst., 2007, p. 339
5. M Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacypreservingpersonal profile matching in mobile social networks,"in Proc. IEEE 30th Conf. Comput. Commun., Apr.2011, pp. 2435-2443.
6. SandeepKonjere and V.N.Dhawas "Online Social Network for Recommendation System usingSVM " International Journal of Computer Applications (0975-8887)Volume 147 No.14, August 2016
7. A Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B.Bhattacharjee, "Measurement and analysis of online socialnetworks," in Proc. 7th ACM SIGCOMM Conf. InternetMeas., 2007, pp. 2942.
8. Nisha S Sarma, Anna PrathibhaShobak "Friend Recommendation inKNN Classification" international Journal of Innovative Research in Computerand Communication EngineeringVol. 4, Issue 6, June 2016
9. Bharat K Samanthula, Lei Ken "Privacy Preserving and Efficient Friend Recommandation in Online Social Networks", Transactions on Data Privacy Volume 8 Issue 2, August 2015 ISSN: 1888-5063 EISSN: 2013-1631