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 6, June 2016

Friend Recommendation in KNN Classification

Nisha S Sarma, Anna Prathibha Shobak

M. Tech Student, Dept. of CSE, Mahatma Gandhi University, Mangalam College of Engineering, Kottayam, India.

Assistant Professor, Dept. of CSE, Mahatma Gandhi University, Mangalam College of Engineering, Kottayam, India.

ABSTRACT:OSN is an online service that facilitating the building of social relations among people.OSNs attracted by thousands of million people.OSN users extending their social circles by friend recommendations.During this recommendation process they establish multihop trust chain relationship followed by 1 hop trust relationship.But different privacy issues are raised in the recommendation process.This is happen when some OSN users will disclose their identities and their friends information to the public.For providing a privacy,a new technique called trust based privacy preserving friend recommendation using KNN classification(FRKC) where OSN users can find their matched friends by applying their attributes using multi hop trust chain.

KEYWORDS: Privacy, trust, OSN

I. Introduction

Social network is a platform to build social network or relations among people,where people can share similar interests,backgrounds,activities etc.OSN's helps people with an easy way of communication with others and can extend their friends circle.Social network is a set of people connected by a set of social relationship like friendship,coworking or information exchange.Different social networking sites are exist like facebook,twitter etc. shows how people are connected with one another and their communications.Friend recommendations are done based on the previous existing relationship.By satisfying various social demands OSN users can extend their social circles.But current approaches cannot achieve a good results.In the new technique trust relationships are formed by shared social attributes.For finding a particular user,new technique use the existing trust based friendships during friend recommendations.Traditional recommendations approaches commonly uses yes or no answers for recommend a friend.But it shows the lower possibility for finding matched friends.So that this type of schemes fail to extend friendship more than two hops commonly.By using multihop chain for recommendation will increase the possibility of reaching more FOFs.New scheme consider the privacy preservation and leakage related to identity and social attributes.

II. Related work

Different works point out the different security breaches on the OSNs.B.Zhou.et al. consider privacy preservation in social network data[3].In this technique ,they identify neighbourhood attacks and also they consider attack to the identities,attributes and relationships of OSN users[18][19][3].C Zhan.et al. article[1] gives a starting point for developing effective secure and privacy preserving OSNs.Also their work can motivate OSN developers to create OSNs without compromising user's security and privacy. access control mechanisms are existed in OSNs like facebook [4].It shows that how a model can express access control policies having rich and natural social significance.

An article by Carninati.et al. propose a different access control mechanism for information sharing sites[5].That considers different information's in the policy design.A game theory model for privacy management was also done [5][6].This is for content sharing and can provide privacy for social profiles and attributes.

Different surveys describes[8][9][10] trust and reputation for online service provision and mobile adhoc network.These service are based on current trends.Along with that Sherchan et al. describes trust management in social networks[11].A peer to peer architecture for hectrogenious social network was proposed by Lin et al. [12].Establishment of friend ships chains in social network are discussed in [13][14][15].Game theory related models

DOI: 10.15680/IJIRCCE.2016. 0406294

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 6, June 2016

are used for privacy management in content sharing[6],[7].Which is similar to the new schemes of providing privacy in social attributes and profiles.This game theory related models [14] also provide automatic access policy generation for users.Based on the existing friend relationships Mislove et al. in [20] discuss the inference of user profiles.

In the new scheme the concept of propagative trust is same as in [19].Along with that new technique discussed in [24],where the scheme analyze similarity based on user's interests and attributes.In [25] paper uses the same idea but data mining approaches are used for input to CF algorithm to gather uses information.Using homomorphic encryption a secure friend discovery scheme is discussed in [21].Also private matching schemes are discussed in [22],[23] papers.

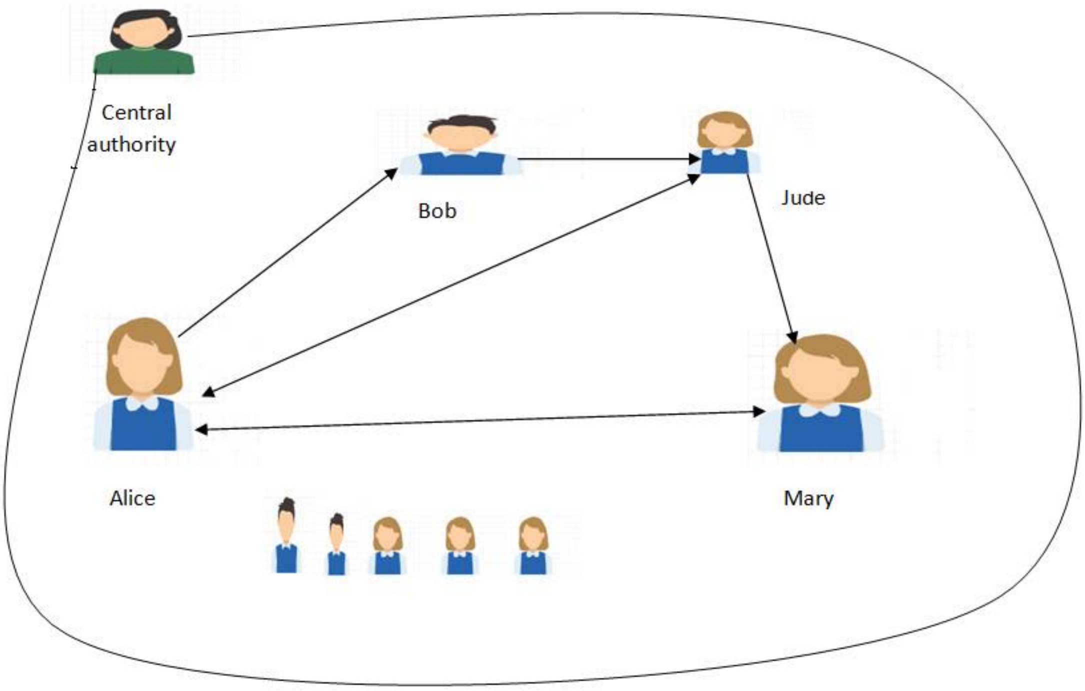
III. Proposed System

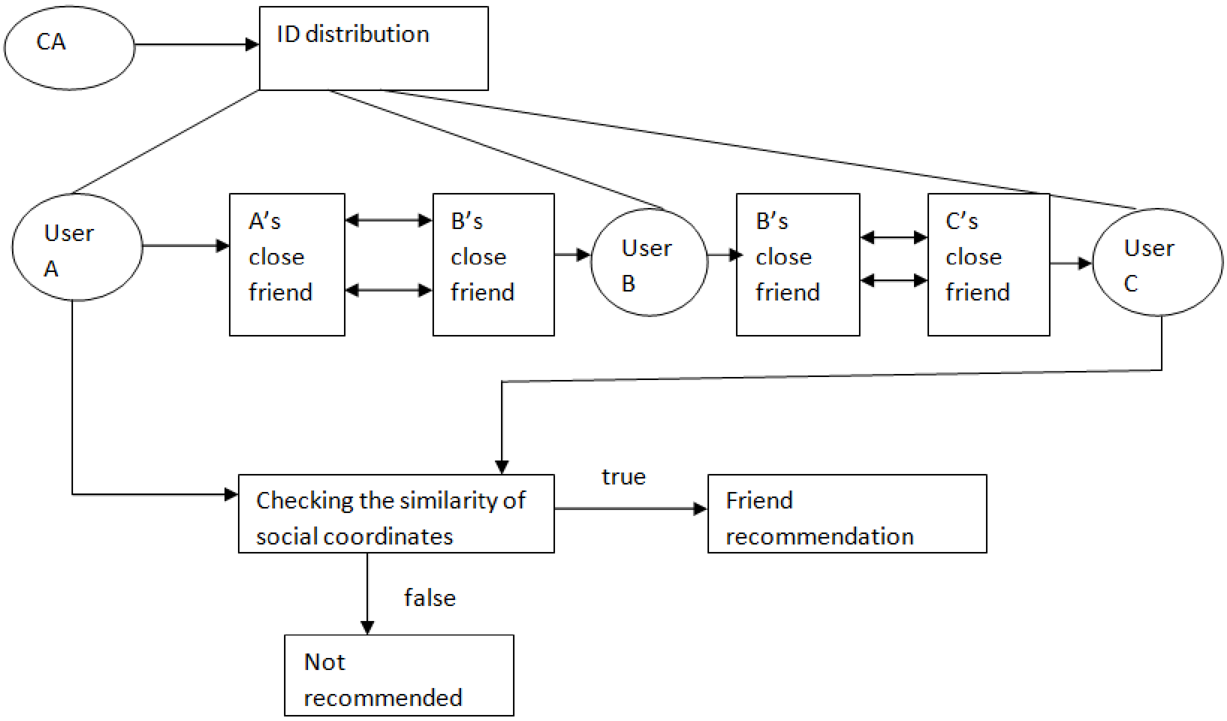
Main design goal of the scheme is to help OSN users securely establish trust relationships with strangers via multi-hop recommendation process. By using the existing 1-hop trust relationships, the new scheme enables OSN users to extend their social circles along with maintaining their identity privacy.

IV. Architecture

A. *Architecture*

The architecture consist of central authority that stores social coordinates of users. It also provides public /private key pairs in the system.System maintaining a trust level of users.It is a numeric value.Lowest trust level is defined as 0 and highest trust level is defined as 1.Considering the example shown below,imagin Alice is looking for an eye specialist on medial OSN.Then one of their close friend Bob,who worked in a hospital recently,recommends to Alice his best friend Jude for further information.Then Alice not known Jude directly,helps her recommend an eye specialist Mary,who is an acquaintance of Jude.That is Alice and Jude are strangers before the multihop recommendation process,then form a trust relationship using 1 hop friends.





B. *Friendship establishment*

Assuming that each OSN user's have a certain number of trusted friends which does not reveal any secret information.So that users can route their packet to destination via their trusted friends.Friendship establishment leads to sharing of key between trusted users. Which help secure communication by sending messages.Based on the message similarity,establishment process is carried out.Entire communication details held is secure.The result is given to the server side for recommendation.All information passing to the server is in encrypted form.So that server cannot identify the personal details and information about each user.Homomorphic encryption [16] is used for this secure communication.

C. *Friend Recommendation*

Friend recommendation can be done using KNN classification[17].Which helps to maintain a trust relationship between OSN users during recommendation process .For the working of KNN,two data set are used.One is training data and other is test data.The algorithm tries to find that the test data belonging to which of the training data.Instead of feature here the system considers words similarity.Checksum calculations are done using a hashing function.At the server side checksum values are used for friend recommendation process. Based on the matching results of social coordinates and established trust relationships, recommenders determine their recommendation decision on whether continue to query their friends or not.

V. Results

To evaluate the performance of the new scheme,facebook dataset is consider.By comparing the time and accuracy gives the performance of the new scheme.In fig.1shows along x axis the message dataset size and along the y axis the time required to perform the friend recommendation are plotted.Below figure shows that the time required for the new methods is very much smaller than the old method.

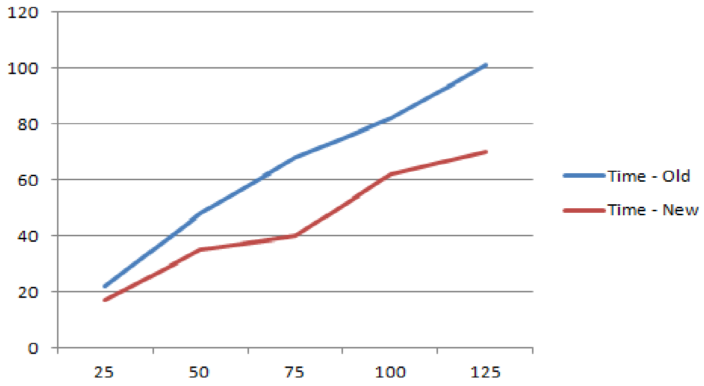


Figure:1

In fig.2 shows that, along x axis message dataset size and in y axis accuracy of friend recommendation in percentage. The below fig. shows that as message size increases accuracy is increased in both method.But new method accuracy is more than old method.

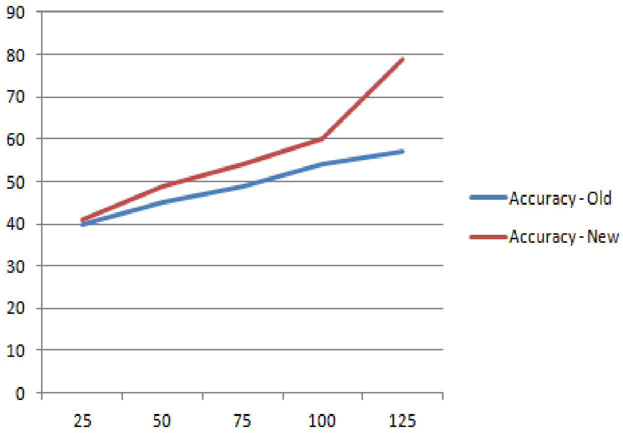


Figure:2

VI. Conclusion and Future Work

The new technique produce 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. Giving reliability to the system is considered for future enhancement.

References

1. 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.
2. 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.
3. B. Zhou and J. Pei, “Preserving privacy in social networks against neighborhood attacks,” in Proc. IEEE 24th Int. Conf. Data Eng.,2008, pp. 506–515.
4. P. W. L. Fong, M. Anwar, and Z. Zhao, “A privacy preservation model for facebook-style social network systems,” in Proc. 14th Eur. Conf. Res.Comput.Security,2009,pp.303-320.

5. B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," ACM Trans. Inf. Syst. Security,vol. 13, Nov.2012.
6. A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks ," in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 521–530.
7. 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.
8. A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Syst.,vol. 43, pp. 618–644, Mar. 2007.
9. J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Survey Tutorials, vol. 13, no. 4, pp. 562–583, Dec. 2011. .
10. K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," IEEE Commun. Survey Tutorials, vol. 14, no. 2, pp. 279–298, Dec. 2012.
11. W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," ACM Comput. Survey, vol. 45, no. 4, pp. 47:1–47:33, Aug. 2013.
12. 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.
13. E. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant manets," IEEE Trans. Mobile Comput., vol. 8, no. 5, pp. 606–621, May 2009.
14. 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.
15. C. Wei, R. Khoury, and S. Fong, "Web 2.0 recommendation service by multi-collaborative filtering trust network algorithm," ," Inf. Syst. Frontiers, vol. 15, no. 4, pp. 533–551, Sep. 2013.
16. Ron Rothblum. "Homomorphic Encryption:from Private-Key to Public-K Electronic Colloquium on Computational Complexity,"Report No.146 (2010)September 21,2010.
17. Tom DuBois. Computer Science Department University of Maryland,College Park,College Park MD 20741.
18. A. 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.
19. C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trustbased routing in wireless ad hoc networks," in Proc. IEEE 29th Int. Conf. Comput. Commun., Mar. 2010, pp. 1–9.
20. A. 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.
21. W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proc. IEEE 30th Conf. Comput. Commun.,Apr. 2011, pp. 1647–1655.
22. L. Guo, X. Liu, Y. Fang, and X. Li, "User-centric private matchingfor ehealth networks—A social perspective," in Proc. IEEE Global Commun. Conf.., 2012, pp. 732–737.
23. L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for ehealth networks," in Proc. IEEE 32nd Int. Conf. . Distrib. Comput. Syst., Macau, China, 2012, pp. 224–233.

BIOGRAPHY

Nisha S Sarma doing M Tech in Computer science And Engineering at Mangalam College of Engineering. She receives B Tech degree in 2013 at Saintgits college of engineering.Area of interest are data mining and security.

Anna Prathibha Shobak,Assistant professor in Mangalam college of engineering,M E ,CSE from Anna university.Secure multimatch packet classification based on signature toe (IJCSIT).International Journal of computer Science and Information Technology,vol-6(2),2015,1677-1679.