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

Technique for Preserving Privacy and Security to the Online Social Network

Swati Pulkurte[1], V. V. Dakhode[2]

[1]Department of Computer Engineering, Sinhgad College of Engineering, Pune, India

[2]Professor, Department of Comp. Engineering, Sinhgad College of Engineering, Pune, India

Abstract: ***Social networking has started a new era on the internet. Social networking provides lots benefits to its users like sharing of data, chatting with different users, for sharing of images and so on. But social media also has some issues such as security and privacy of the shared data on it. Some of the users of online social network will not permit their identities and also friends information with the public domain. While sharing personal data in the network user demands some privacy. Currently available systems provide privacy to the online social network. But those systems are not able to provide accuracy to the social network. So to improve the accuracy and privacy of social network we are proposing a system. System evaluates trust score for maximizing the accuracy of the online social networking system. By making use of this system trust friendship is introduced in two friends.***

Keywords: OSN, Trust score, 1- hop friendship, multi-hop friendship

1. Introduction

For sharing of data there are number of systems are created by the internet for example Web. From those entire systems Online Social Network (OSN) is most widely used on internet by large number of users. OSN has become very much popular and 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 generated very large amount of data social data having personal and private data about every individual user.

An application on online social network has different problems such as security and 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 cyberspace.

Shockingly, restricting the development of OSN users friend circle, security issues brought up in the suggestion procedure. Some OSN user not allow to uncover their identities and their friends data to general society domain. To solve this issue, for OSNs utilize a privacy-preserving trust based friend recommendation system, which permit two unknown persons build up trust relationships depending on 1-hop friendships. Proposed system includes:

- System use trust relationship and OSN clients social attributes to build up the friend suggestion system logically while saving the security of OSN client's identities and attributes. System employ OSN users close friends to create anonymous communication channels.
- We extend existing friendships to multi-hop trust chains without trading off recommender's identity privacy depending on the 1-hop trust relationships.
- This trust level derivation scheme enables strangers to obtain an objective trust level on a particular trust chain.
- To verify the performance of our system in terms of security, effectiveness, and viability extensive trace-driven experiments are deployed.
- Use trust score Calculation for estimate the trust between users.

This paper focus on related work in Section II, Section III studied the implementation details, problem definitions and proposed system. Section IV shows result analysis of a system and at last conclusions and future work provided in Section V.

2. Literature Review

This section discusses related work done by the researchers and publishers for text mining process. In [2], author introduces new method called VENETA, a mobile social networking system to execute friend of friend detection algorithm. This paper is centered on number of problems by introducing a decentralized system and displayed a method that consistently coordinates the friendship study of conventional social networking websites into communication sites into only decentralized environments. Small security issues are there in proposed approach yet considering popularity in server based frameworks proposed system may turn into a important component in upcoming mobile social applications.

In [3], FindU, it's a first security guarantying personal profile co-coordinating plan for mobile informal groups. In FindU, a starting user can search from a social affair of users the one whose profile best matches with his/her; to constrain the risk of contact simply basic and insignificant information related to the private qualities of the taking an interest users is traded. A few extending levels of clients security are explained, with minimizing measures of exchanged profile information.

In [4], explain a sensible method with anonymize an informal group to gratify the kanonymity need. The method is in two stages. At initial, separate the areas of all vertices in the system. To encourage the connections in neighborhoods of particular vertices having the isomorphism tests which will be driven continually in anonymization, likewise propose a direct yet effectual neighborhood component coding methodology to signify to the areas concise. In the next step, they meanly form vertices into gathering events additionally, anonymize the ranges of vertices in the same bunch. Due to the inside and out saw power law scattering of the degrees of vertices in extensive interpersonal organizations, they start with those vertices of high degrees.

In [5], system processes trust considering EX, CI and I as the three rule qualities that helps in computing the trust. Similarly, out of these three, CI and I are determined by the structure and EX is the information from the user. The user adds the security level with all data which they exchanges. As the security level is same as the limit trust score, the choice is made to allow the entrance or deny the access dependent upon the characterized Trust Rule which contains the comparison among the trust score of each friend in the friend list and the edge trust score given as the data from the client. The decision that is delivered by applying the Trust Rule helps in access control of the data which is exchanged by the proprietor shape the reputation way to each node and in addition kept secret of detail routing data from the middle nodes.

3. Implementation Details

In this section we will go through system overview in detail, proposed algorithm, and mathematical model of the proposed system.

A. System Overview

The following figure 1 shows the architectural view of the proposed system.

Proposed system computes the trust score of the friends in the process of recommendation which will be in range of 0 to 1.
For selecting the single user from number of recommendations trust higher score is used.

System makes use of live OSN data instead of using the previously generated dataset, i.e. it retires social coordinates from Facebook by accessing Facebook API or a RestFB API is used to extract user's social coordinates and use it as dataset. RestFB is a simple and flexible Facebook Graph API and Old REST API client which is written in Java. The basic assumption of our network model is that there exist secure communication channels among CA and each OSN [1] user. In system central authority is responsible for parameter distribution. By some authentication and key exchange system or by physically making use of encrypted phone or email the secure channels may set up.These assumptions assurance the privacy of the data sharing from CA.

- The Central Authority (CA) is a fully-trusted communications which stores users' social coordinates in its storage. It is also responsible for system setup and generating public/ private key pairs to OSN users in the system. In our system, we need an always-online CA to give the recommendation service.
- Roles of OSN Users For the ease of description, OSN users are given dissimilar roles in our scheme.

Querier (Q): users who start the friend recommendation process.
Friend (F): users who is 1-hop away from each other with recognized friendships.
Recommender(R): users who are strangers to the querier and eager to help the querier discover anonymous trust chain.
Destination user (D): the one that the querier is appears for.

Social coordinates : In our system, each user has a unique vector to represent his/her social attributes, e.g., affiliation, age, gender, etc, where we name it as social coordinate, and n is the length of the vector.

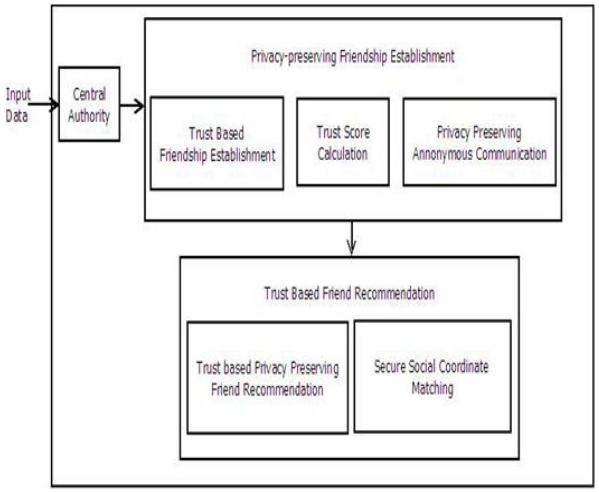

Figure 1: System Architecture

B. Algorithm

This section discusses the proposed system algorithm and algorithm for the adding graphical element into slide.

Algorithm 1: Proposed Algorithm

Step 1: Here Input is to use the RestFB API to extract user's social coordinates and use it as dataset.
(RestFB is a simple and flexible Facebook Graph API and Old REST API client written in Java)

Step 2: Insert user query

Step 3: Search in 1-hop friendship of current user.

Step 4: If found Calculate the trust score by the following equation: Trust (ego user, $friend_x$)

$$Trust = 0.614 \times Existing\ Trust + 0.277 \times \frac{n}{m}$$

Where,

$$Existing\ Trust = \begin{cases} 1, & for\ close\ friends \\ 0.75, & for\ friends \\ 0.25, & for\ less\ known \end{cases}$$

n = number of time user login to system
m = activeness

Step 5: Evaluate trust hashed communication

Step 6: If not found take the next hop and continue the procedure with step 4.

Step 7: Final Output: recommended friend.

Algorithm 2: Secure KNN algorithm
Step 1: CA selects a secret parameter S and two invertible matrices B1 and B2 for each user.

Step 2: CA creates the extended vectors A and Q for the user's social attributes and the queried vector and embeds a random number r to secure the confidentiality of the matching results P

Step 3: Based on S, B1 , and B2 , CA encrypts extended vectors .

Step 4: The final matching result can be derived as

$$\left\{B_1^T \bar{A}^{[1]}, B_2^T \bar{A}^{[2]}\right\}.\left\{B_1^{-1}\overline{Q}^{[1]}, B_2^{-1}\overline{Q}^{[2]}\right\} = \gamma AQ - 0.5\gamma \| A$$

C. Mathematical Model
System S is represented as S= {U, P, R, PP, SP}

Input:
Browse Dataset
U= {u1, u2, u3,…., un}
Where, U is a set of number of related papers and u1, u2, u3,..un are the number of papers.

Process:
1. Central Authority
P = { P1, P2, P3,, Pn }
Where, P is represented as a set of Central Process P1, P2, P3, , Pn are the number of central authority process.

2. Privacy Preserving Friendship Establishment
R= {R0, R1, R2}
Where, R is represent as a set of steps performed in this module.

R0= System set up
In this step, CA assigns the ID-based public/private key pairs to each user in the system so that secret information of a user will not reveal.
ID= {ID1, ID2, ...IDn}

– R1= Trust based friendship establishment
In this step, we perform trust score calculation. Different from close friends, we require
OSN users assign different trust levels T 2 [0; 1]; to each one of their 1-hop friends.
T= {T1, T2, T3,, Tn}
Where, T is represents as a set of trust value assigns to multiple users.

– R2= Privacy preserving anonymous communication
After R0 and R1, OSN users within 1-hop can initiate the anonymous communication.
The process is as follows:

$$Q \rightarrow Q.j : E_{pkQ.j}\,(PS^{\alpha}_{F.q} \,||\, sk_{PS}{}^{\alpha}_{F.Q}), exp, \sigma Q$$

$$Q.j \rightarrow PS^{\beta}_{F.i} : PS^{\alpha}_{F.q},\ n1,\ \sigma Q.j$$

$$PS^{\beta}_{F.i} \rightarrow Q.j :\ PS^{\beta}_{F.i},\ n2,\ \varphi_{\beta,\alpha}$$

$$Q.j \rightarrow PS^{\beta}_{F.i} : \varphi_{\alpha,\beta}$$

3. Trust Based Friend Recommendation
PP= { pp1, pp2 }
The trust-based friend recommendation includes two major subprotocols, secure social coordinate matching and friend recommendation process.

– PP1= Secure social coordinate matching
To achieve this step, we apply the modified secure kNN scheme, in which users social coordinates can be formed into a set of binary vector A.

– PP2= Friend recommendation process
The trust-based recommendation process should satisfy, the trust chain could be set up according to the matching results

Output:
Final Output
SP= { sp1, sp2, sp3,, spn }
Where, SP is represent as a set of Final Output and sp1, sp2, sp3,, spn are number of final output.

D. Flow Diagram

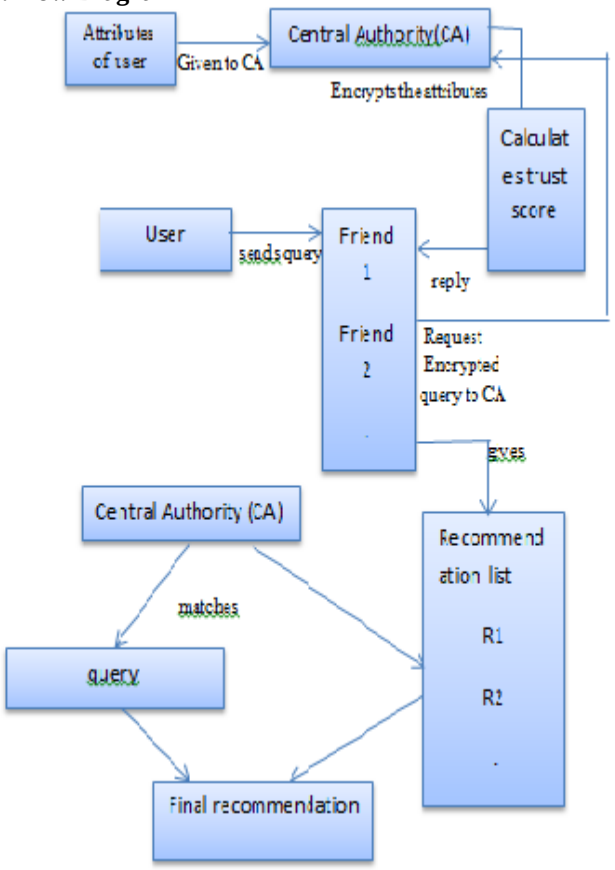

Figure 2: Workflow of Proposed Work

E. Experimental Setup

The system is built using Java framework (version jdk 8) on Windows platform. The Netbeans (version 8.1) is used as a development tool. The system doesn't require any specific hardware to run, any standard machine is capable of running the application.

4. Result and Discussion

A. DataSet Discussion

For evaluating the performance of the system used the Facebook dataset.

B. Results

In this section we will see the experimental result of the proposed system. In table 1 shows the time required for the proposed system and existing system. The following table shows that the time required for 1-hop friendship is less than the time required for the multi-hop friendship system.

Table 1: Time Comparison

System	Time Required
1-hop friendship	6 min
Multi-hop friendship	8 min

In table 2 shows the reachability comparison of the existing system and proposed system.

Table 2: Reachability Comparison

	Existing System (%)	Proposed System (%)
Facebook Dataset	20	80

5. Conclusion

For online social networks this system utilize a privacy-preserving trust-based friend recommendation scheme, which permit two unknown users to create trust relationships in view of the current 1-hop friendships (see figure 2). We essential design the unknown close friend verification method to secure the communication between OSN clients for privacy concerns. At that point, apply the secure KNN algorithm as the running protocol to get the encrypted social coordinate matching outcomes. To get the target trust score, framework propose an solution for calculate the average trust score as the transitive overall value without trading off every personals trust level. All through security analysis and experimental evaluation demonstrates the feasibility and security of the proposed framework.

References

[1] LinkeGuo, 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.
[2] 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. 184189.
[3] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: Privacypreserving personal profile matching in mobile social networks," in Proc. IEEE 30th Conf. Comput. Commun., Apr. 2011, pp. 2435-2443.
[4] Bin Zhou, Jian Pei, "Preserving Privacy in Social Networks Against Neighborhood Attacks"
[5] Vedashree K.Takalkar, Parikshit N.Mahalle, "Trust Based Confidentiality Approach in Online Social Network".
[6] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust based routing in wireless adhoc networks," in Proc. IEEE 29th Int. Conf. Comput.Commun. Mar. 2010, pp. 1-9.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in Proc. 13th Amer. Conf. Inf. Syst., 2007, p. 339.
[13] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," ACM Trans. Inf. Syst. Security, vol. 13, no. 1, pp. 6:1-6:38, Nov. 2009