© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Credence Based Sollitude Companion for Online Social Network

Sundar R, Dr. N. Jayalakshmi,
Department of Computer Science and Engineering, Saveetha Engineering College, Chennai, Tamilnadu, India

ABSTRACT

Online social networks encourage associations between individuals based on attributes (i.e., friends, professional colleagues), etc. They make it simpler for people to discover and communicate with individuals who are in their networks using the Web as the interface. For example Facebook is solid in Relationships, furthermore bolsters Presence, Identity, Conversations, and Reputation in Groups, further more underpins Sharing and Conversations. Facebook consolidates the personal and the professional. *Privacy Controls*–In most networks, the ability to access more detailed information about a person is based on their attributes as one of your connections; “friends” see a great deal more data than the individuals who are not your “friends.” You can control who is actually in your personal network by effectively managing who you invite into your network and whose invitations you accept. Sadly, privacy concerns raised in the recommendation process impede the Expansion of OSN users’ friend circle. To overcome this issue we have approach the practice known as Credence Based solitude Companion for OSN to expand the friend circle or getting the help from the Friends of Friend without disturbing the privacy by using the Attested mechanism.

Keywords: Attested Mechanism, Privacy, OSN, Trust level

I. INTRODUCTION

Online social Networks furnish individuals with a simple approach to share or exchange information with each other and make new companion in cyberspace. Miserably, security concerns raised in the recommendation process to obstructs the broadening the friends circle in online social networks. Earlier [1], friend recommendation process was carried out based on their attributes and recommending the friends of friends. Trust calculation is made based on the attributes[11]. In the above approach trust level calculation is achieved partially. The main motive of this paper is to widen the friends circle with accurate privacy. The privacy can be achieved by increasing the level of trust calculation by computing the conversation list etc., and the images which are shared by the senders can only be viewed by the other companions and it can’t be downloaded or shared by the others without a appropriate permission from the sender[10]. By implementing this design, the crimes which are done by the malicious users can be reduced. The below example will clearly state the proposed work. Let us consider an example of three friends such as Bob, Alice and Annie. The Bob and Alice, Alice and Annie are 1-hop friends and by profession they are Lawyer, Civil Engineer and Architect respectively. The Bob want to remodel his house so he needs the help from Annie. Annie was unknown to Bob without Alice. So Alice recommends Annie to Bob. After recommendation now Bob and Alice are friends after accepting the friend request from the Bob to Alice Multi-hop chain is also achieved and the trust level will also be calculated Trust level between Bob and Alice will be comparatively higher than Bob and than that of Annie vice-versa for Annie and Alice By calculating the trust level based on attributes and conversation list, the security level will also be increased[15]. On the other hand Bob needs to share his images through online social network which will be viewed by all and the images can’t be downloaded by other companions like Alice, Annie etc without appropriate permissions from the Bob. By trace-driven experimental results, we demonstrate both the security and efficiency of our proposed scheme.

II. LITERATURE SURVEY

FRIEND RECOMMENDATION PROCESS

The friend recommendation process will be carried out based on the attributes such as Location, Education details, Area of Interests etc. The trust calculation will be achieved partially. The trust calculation is computed based on the attributes. Hence the privacy is assured while recommending the friends are achieved partially.

IMAGE SHARING

In current methods the images can be downloaded/shared by other companions without knowledge of image uploaded. Hence it causes the malicious users to misuse the images/documents. The privacy will also be impeded.

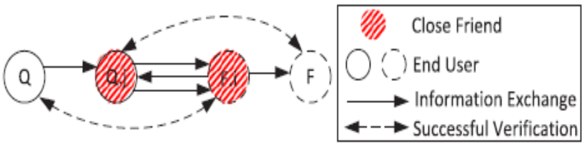


Figure 1: Image Sharing Techniques

In Figure 1. shows the image sharing verification technique of the existing system.

NEW SYSTEM DESIGN

To overcome this issue we proposed the mechanism known as the attested mechanism. By using this mechanism the friend recommendation process and image sharing process will be carried out in more privacy by using the weight-age method.

In the proposed system we have weight-age methodology to compute the trust level of the existing. There are three types of weight-age classification namely high, medium and low are implemented in :

1. Friend Recommendation with Attested Mechanism
2. Image Sharing Process with Attested Mechanism

FRIEND RECOMMENDATION USING ATTESTED MECHANISM:

As mentioned in introduction segment friend recommendation will be carried out by using the attested mechanism. The friend recommender will create code which is in alpha or numeric formats by using attested mechanism [3][9]. By using this mechanism trust level will also be improved. The below diagram will clearly states the working mechanism.

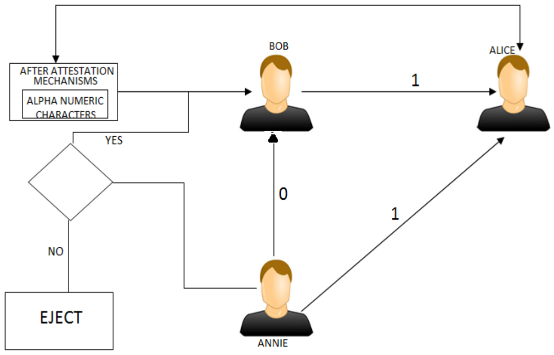


Figure 2: Friend Recommendation with attested Mechanism

1’s indicates friend

0’s indicates friends after recommendation

IMAGE SHARING USING ATTESTED MECHANISM:

The image can be shared to others but images can’t be downloaded by others. By using the weight-age technique the friends trust levels are classified into three types namely high, medium and low. The Notifications can be shown to image up loader if the trust level is high, for medium and low The Attested mechanism will be used without the appropriate permission the image can’t be downloaded by other users[4][5].

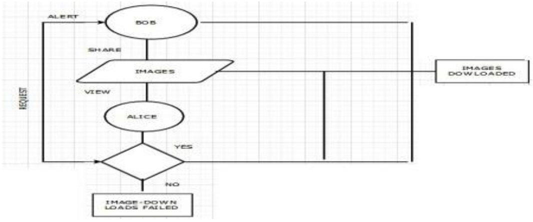


Figure 3: Image sharing techniques with Attested Mechanism

In the above Figure it clearly states that the companion can able to download the images with appropriate permission from the image uploader. The uploader can able to give access to download the image or deny the permission to download the image.

ALGORITHM IMPLEMENTATION:

The below cryptographic equation is used to calculate the trust level that are based on certain attribute’s include frequently contacted.

$$I(f_{u,}f_u^c) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(f_{ui}, f_{uj}^c), I(f_{ui}, f_{uj}^c)$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{m} P\left(f_{ui}, f_{uj}^{c}\right) \log \frac{P(f_{ui}, f_{uj}^{c})}{P(f_{ui}), P(f_{uj}^{c})}$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{m} P(f_{ui}), P(f_{uj}^{c} | f_{ui}) \log \frac{P(f_{uj}^{c} | (f_{ui})}{P(f_{uj}^{c})}$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{m} P\left(f_{uj}^{c}\right), P\left(f_{ui} \middle| f_{uj}^{c}\right), \log \frac{f_{ui} | f_{uj}^{c}}{P(f_{ui})}$$

For case When f_u and f_u^c are statistically independent, I(f_u : f_u^c)=0 ie No Average Mutual Information.

a) Average Self Information

The below equation shows that the system gathers the communication information between two users

H(f_u) $= \sum_{i=1}^{n} P(S_{ui}) I(S_{ui})$
$= -\sum_{i=1}^{n} P(S_{ui}) \log P(S_{ui})$

$H(f_u)$represents the average information as per source attribute and is also called entropy.
The Entropy can be interpreted as expected value of $\log \frac{1}{PS_{ui}}$

Chinese Character for Entropy looks like
0< P($S_{ui\leq 1,}$ $\log \frac{1}{P(S_{u)}} \geq 0, H(S_{ui})$≥0

The below equation states that attested Mechanisms:
$H(f_u ; f_u^c)$= -$\sum_{i=1}^{n} \sum_{j=1}^{m} P(f_{ui,} f_{uj}^{c}) \log P(S_{ui,} f_{uj})$

H(f_u,f_{uc})= H(f_u)+H($f_u^c | f_u$)
=H(f_u^c) + H(f_u) + H(f_u^c)- H($f_u s_u$)

b) Information Calculation:

The attributes can be calculates The friend set will be maximum priority. The trust level computation will also be made based on attributes and contacted list. The contacted list will give huge priority along with attributes[2].

I(f_u,s_u)= H(f_u)-H($f_u | s_u$)=H(f_u)

c) ***Symmetric Equation:***

The below equation states the conditional statement for the introduced attested mechanism for image sharing and friend recommendation process

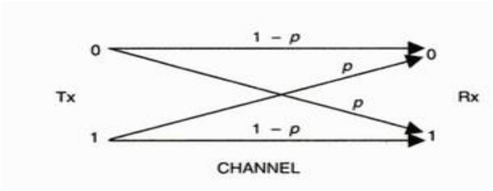


Figure 4. Binary Symmetric Channel

H(f_u *)=* - $\sum_{i=0}^{1} P(f_{ui}) \, log \, P(f_{ui})$ = *-q* $log_2(f_{ui}^c)$ *-(1-* (f_{ui}^c)*)-* log_2*(1-* (f_{ui}^c)*))*

The conditional entropy is given by
$H(\frac{f_u}{f_u^c})= \sum_{i=1}^{n} \sum_{j=1}^{m} P\left(f_{ui}, f_{uj}^{c}\right) log \frac{1}{P(\frac{f_{ui}}{f_{ui}^{c}})}$

d) Relation Entropy With Attested Mechanism

The Relationship between two individuals can be calculated based on the Relation Entropy[8][12]. It is clearly states in the below Figure.

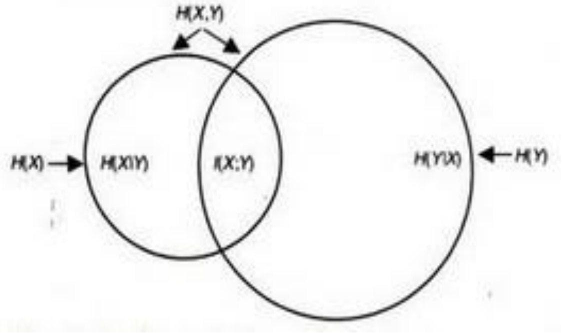


Figure 5. Friends Relationship

The below equation states the two nodes and trust level will also be known the friend set and friend will also be determined.

H($f_{u\,,f_u^c}$ *)= H(* f_u *)+H((* f_u^c *)| (* f_u *))= H((* f_u^c *)+H((* f_u *)|* f_u^c *))*

I($f_{u\,,f_u^c}$ *)= H(* f_u *)+H((* f_u^c *)-H(* f_u*,*f_u^c *)*

e) ***Hierarchical Tree Structures:***

The Total no of friends will be assumed in structure of Hierarchical tree hence the friend recommendation will easily carried out By using the hierarchical tree structure The attested mechanism will be carried out. The below Figure will clearly states the hierarchical structure[13]. Its also states the Friends of Friends. By using the Hierarchical Tree structure the relationship between the each individuals can also be found. The common attributes will also be determined. The expanding the friends circle will also be explained in the below equation

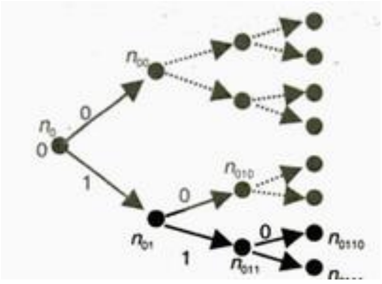


Figure 6. Hierarchical Tree Structure

We observe that in code tree of the order n=n_L, The number of terminal nodes eliminated from the total number of 2^n terminal nodes is

$$\sum_{k=1}^{L} 2^{n-n_k} \leq 2^n$$

We can easily extend the proof for prefix codes over an friends list size of M. For the proof we will have to consider an M-ary tree instead of a binary tree.

$$\sum_{k=1}^{L} M^{-n_k} \leq 1.$$

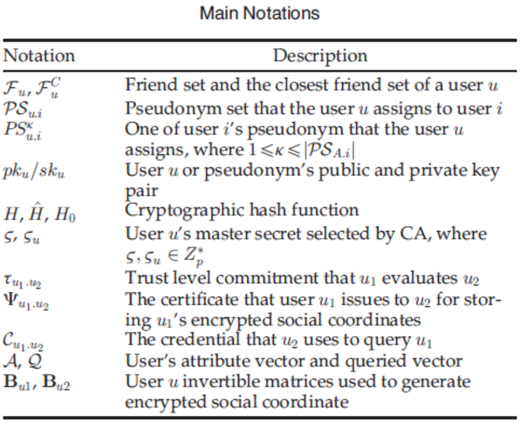
The above equation relates the relationship between the individual

f) Error Correction and Detection

The below graph shows that by using attested mechanism we are rectifying errors for friend recommendation and image sharing techniques in social media and accurate privacy will be detected and corrected by using the Average Mutual Information. The below equation shows the probability error detection and correction.

$$\mathrm{I}(\mathrm{f_u},\mathrm{f_u^c}) = \iint_{-\infty}^{\infty} \mathrm{p}(\,\mathrm{f_u})\mathrm{p}(\mathrm{f_u^c}|\mathrm{f_u})\log\frac{\mathrm{p}(\mathrm{f_u^{c|f_u)}}}{\mathrm{f_u}}\,\mathrm{dxdy}$$

The Probability of errors will be reduced and privacy level will also be increased.



Main Notations

Notation	Description
$\mathcal{F}_u, \mathcal{F}_u^C$	Friend set and the closest friend set of a user u
$\mathcal{PS}_{u.i}$	Pseudonym set that the user u assigns to user i
$PS_{u.i}^{\kappa}$	One of user i's pseudonym that the user u assigns, where $1 \leqslant \kappa \leqslant \lvert\mathcal{PS}_{A.i}\rvert$
pk_u/sk_u	User u or pseudonym's public and private key pair
$H, \hat{H}, H_0$	Cryptographic hash function
ς, ς_u	User u's master secret selected by CA, where $\varsigma, \varsigma_u \in Z_p^*$
$\tau_{u_1.u_2}$	Trust level commitment that u_1 evaluates u_2
$\Psi_{u_1.u_2}$	The certificate that user u_1 issues to u_2 for storing u_1's encrypted social coordinates
$\mathcal{C}_{u_1.u_2}$	The credential that u_2 uses to query u_1
$\mathcal{A}, \mathcal{Q}$	User's attribute vector and queried vector
$\mathbf{B}_{u1}, \mathbf{B}_{u2}$	User u invertible matrices used to generate encrypted social coordinate

Table 1: Table showing the notation of above equation

III. CONCLUSION

By using Attested Mechanism along with cryptographic techniques the friend recommendation and image sharing process will be carried out with accurate privacy. The Trust level is calculated and it is also completely achieved using cryptography algorithm for both sender side and receiver side with complete security and privacy level is also increased from the initial level of 20% to the final level 90 %.

IV. RESULT AND FUTURE WORK

By following the above step privacy level will be increased upto 90% by using attested mechanism while recommending and multimedia file sharing process. The friend circle expansion is also achieved without disturbing the privacy. The main motive of the paper is to expand the friend the friend circle with accurate privacy and security.

The Assuring Security for Online Social Networking is a mandatory process. The users may vary in type and style the user the reliability and trust level in social media is very low and there are many chances of fraudulent and forged activities in social media. So to provide a minor solution to this problem I have introduced an attested mechanism solution to provide security to all the users. But the question arises that if the attacker uses the snapshot method to capture the user images then how to ensure security? The solution to the problem will be discussed further in our future works.

V. REFERENCES

[1]. Linke Guo, Member, IEEE, Chi Zhang, Member, IEEE, and Yuguang Fang, Fellow, IEEE, “A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social NetworksIEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 4, JULY/AUGUST 2015

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. NATERGM: A Model for Examining the Role of Nodal Attributes in Dynamic Social Media NetworksShan Jiang and Hsinchun Chen, Fellow, IEEE , VOL. 28, NO. 3, MARCH 2016

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. L. Guo, X. Liu, Y. Fang, and X. Li, “User-centric private matching for ehealth networks—A social perspective,” in Proc. IEEE Global Commun. Conf., 2012, pp. 732–737.