Computing Privacy Risk and Trustworthiness of Users in SNSs

Akansha Pandey *, Annie Irfan †, Kuldeep Kumar ‡, S. Venkatesan§

Department of Information Technology
Indian Institute of Information Technology, Allahabad, India
*Email: pnakansha@hotmail.com
† Email: leo23annie@gmail.com
‡ Email: kuldeepcs0018@gmail.com
§ Email: venkat@iiita.ac.in

***Abstract*—The immense growth of Social Networking Sites (SNSs) has provided fast interactions with strangers, friends and people known in person. This has increase the religious, political and social possibilities for maintaining virtually every type of significant bonds or groups. The personal information used while interacting on social networking sites is an asset for every user profile that may be traded intentionally by a third party for its benefits. Privacy of users is completely based on their awareness of how much of their personal information could be shared without risk. Moreover, users do not give much importance to the privacy risk arising by their information sharing activities. With the rise in different online crimes and malicious behaviors, it is necessary to evaluate the reliability of a profile user. The objective of this paper is to present a method for computing the trust value and privacy risk of users in online social networking sites by integrating basic trust parameters like personal information, recommendations, followings, and customized privacy settings. This will help other users in social network to check whether a person is trustworthy, before accepting him/her in their network. We used real-world data collected from Facebook for calculating and demonstrating the proposed trust model.**

***Keywords*—Social Networking Sites (SNSs); Trust value; Customized privacy settings; Privacy awareness; Privacy risk; Reputation; Sensitive personal information.**

I. Introduction

Social Networking Sites (SNSs) like LinkedIn, Facebook, etc. are online communities that allow users to share their resources, establish relationships with other online users and widen their social network circle. Recently, many real life incidents about cyber espionage, fraud, identity theft, etc. have been registered where personally identifiable information (PII) leakages were mined and utilize by third parties for their benefits [2], [3]. This proof social sites to be attack vectors with different functionalities such as posts, friend requests, photos and videos uploads, likes, comments, third party applications, advertisements and links to other websites making them potential avenues of information leakage [5], [14]. Privacy risk on disclosure of individual's sensitive information through online social interactions can be protected through access control [6] and algorithms like anonymization [8], [12] and decentralized modeling [9]. This represents a social network as a graph, applying various transformations to achieve security. But, according to 90/10 rule of information security [23], alertness among users is important for restricting the exposure of one's data with the right class of users. This indicates, that the privacy awareness among individuals on the SNSs is concerned with factors like reliability or trustworthiness of users and risk due to exposure of personally identifiable information (PII).

The trustworthiness of the user in online social network is a subjective context which shows the benevolence, capability and integrity of a user. The challenge of developing methods for accurately estimating trust between people is not a simple task as each user in SNS needs to check if the other people are reliable or not before interacting with them. To do that, the trust level of a user can be established based on the profile information, the reputation of a user and privacy alertness. Although trust proved as one of the important factors to influence social interactions in SNSs, there are following questions that need to be answered:

- What is the relationship between users privacy concern and their willingness to disclose information? and
- How trust level of a user can be derived based on a privacy concern and reputation?

In this paper, we are allowing user to give information about there privacy setting preferences, number of recommendations, endorsements, followers and profile information, thereby calculating probability to rate user under the category of "Trustworthy" or "Untrustworthy". By knowing information exposure and user alertness metrics we compute the privacy risk of disclosing user information in SNSs. The remaining section includes, related work, research hypothesis, proposed model,results analysis and conclusion and future work.

II. Literature Review

Gambetta, et al defined trust as a confidence in the intention or the ability of an individual to be trustworthy of something or someone at some time in the future which is based on different evidences through communication or information about another entity or individual [1]. Jennifer Golbeck, et al [19] gave the popular Tidal trust model in which users are grouped into the category of trusted and distrusted based on the transitive trust score from a users perspective using a shortest path algorithm. However, since trust is subjective, personalized and context dependent, a trusted person from

978-1-4673-6994-7/15 $31.00 © 2015 IEEE
DOI 10.1109/ICACC.2015.50

one's perspective may be distrusted for another person, thus lowering the efficiency of the trust inference algorithms. In a couple of years, researches and extensive discussions have been done to estimate trust score and privacy concern of a user in social network [16], [17] . In previous works, trust has been empirically measured by analyzing the intentions, disclosure behavior and its mediating factors, and leakages of personal information that delivered valuable insights [4] for a better understanding of privacy and privacy issues like in [14], [16]. Beside intentional analysis trust value of a user could also be based on popularity and engagement of a user in the community like in STrust [20], where building trust community motivates users to share their experiences, opinions and build better relationships keeping their information safe.

Moreover, many social networks and web based trust model have used the concept of recommendation [21] in online social networks using Bayesian concept that requires explicit contributions of members of an SNSs but, is limited to those relations which explicitly been rated. In fact, deriving trust from feedback(ratings) help in promoting a sound relationship among participants. Preeti Yadav, et al [18] has proposed a trust model to calculate trustworthiness of a person who has been rated as trustworthy by his acquaintances based on five factors such as Information Sharing, Known in Person, Conversation History, Mutual Friends and Common Interest.

There has been several quantification models for evaluating privacy score in SNSs. Agrima Srivastava, et al [22] has proposed a framework using existing privacy measuring models that caters the utility needs of a profile item and ensures the privacy of users by comparing with respect to their circle in the OSN. Yongbo Zeng, et al provided an intuitive and quantitative trust-aware privacy evaluation framework TAPE [11] for computing the privacy risk using privacy awareness and a privacy trust algorithm to help the users to know their best privacy settings. Additionally, Kun Liu and Evimaria Terzi [17] examined the sensibility and visibility of SNSs users profiles to compute the privacy score using Bayesian probability and Item Response Theory.

To the best of our knowledge, though there have been researches, that are trying to solve the privacy problems involving friends [10], users privacy preferences and personal information through ratings, but none of them take full advantage of a users profile information, recommendation, endorsements and customized privacy settings at the same time. Since the real users conceive their privacy settings based on some rules which are implicit in nature. This motivated us in proposing the method to quantitatively infer the trustworthiness of an individual. Here we combined different factors based on the limited amount of information collected from there profile and knowing their preferences for their hidden privacy settings.

III. Research Hypothesis

Most of the SNSs information is either completely visible to the public or if the user is aware about the privacy settings, to some extent selected friend lists. Surveys have also shown that users being vigilant about customizing their privacy settings have considered certain profile information's such as email address, occupation, working detail, location, relationship status, posts, etc. causing potential security threats and impacts [5], [14], [16]. These facts and figures motivated to conceive the idea of computing users trust based on profile information, reputation and customized privacy settings. Our model also showed how privacy risks of disclosing information is related to users trust.

Our model consists of the following steps, Figure 1. effectively explains the process of measuring trust and privacy risk.

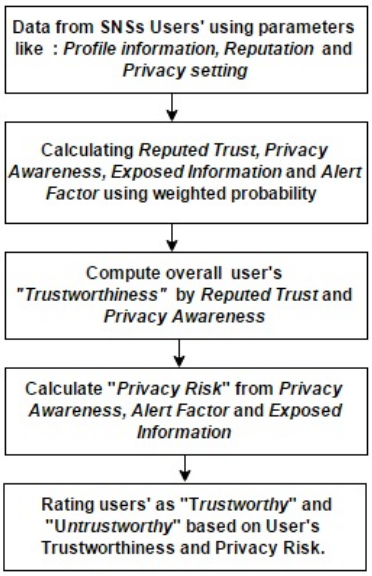

Figure 1. Work flow of our proposed model.

We empirically tested our hypothesis using survey data set conducted on 200 users from different SNSs.

We categorize collected data set into three parameters: Profile information, reputation and customized privacy settings. The three parameters and other metrics derived are explained as follows:

A. Profile Information (PI):

By creating an account, every SNSs (e.g. Facebook) encourage user to upload personal details onto a page known as Profile . Experimental results in [7] showed, that there are stronger relationship between Facebook activities like number of groups, wall posts, number of friends etc. altogether and a users trust score. Using the result, we collected publicly available information's of users profile like name, education, occupation, number of friends, number of groups and time period of using Social Network.

B. Reputation (R):

Researches in [21] have shown that ratings and endorsements from the person in specific domain have significant influence on trust inference. In this regard, we define reputation of a user in SNSs as the number of recommendations or endorsements (e.g. on LinkedIn) and followings (e.g. on Facebook).

C. Customized Privacy Settings (PS):

Often personal information's in SNSs are seen directly by people (e.g. known in person), and this through liking or

sharing can even flow to thousands of other people (e.g. friends of friends). Studies in [5], [14], [16] have shown personal information's like interest, email id, photos/videos, relationship status, conversation history, religious/political beliefs etc. if disclosed, can severely impact the privacy of user. Additionally it has been found, that social relationships have significant influence on the trust, so type of accepted friend requests (e.g. friends, strangers or known in person) will help to protect privacy [9]. We define customized privacy settings as all the personal information that are hidden or shared with selected people, by users preferences.

1) Exposed Information (EI): Exposed information is defined as, the amount of users significant sensitive information's such as email id, photos/videos, relationship status, conversation history, religious/political beliefs, etc. [15] that are disseminated, disclosed or made available publicly intentionally or unintentionally in any manner whatsoever. This can be misused by third party for its benefits.

2) Alert factor (AF): Hootan Rashtian, et al [4], showed that factors like mutual friends, location, photo etc. help users to make better decisions in regards to accept friend request from strangers. Taking these facts, we described alert factor of a user as the probability of being vigilant about the factors like mutual friends, known in person in real world, photo, common background, past conversations, user activity pattern, date of creation of profile, location and wall posts/status when responding to friend request.

3) Privacy Awareness (PA): A Privacy awareness is the probability of a user being aware about safeguarding their personal sensitive information's by adopting better privacy settings and making good decisions before responding to any friend request.

4) Privacy Risk (PR): A Privacy risk is the probability of exposed personal sensitive information's due to user's unawareness and unalertness about their privacy settings, thus increasing the chances of attacks and exploitation of the users privacy rights.

IV. Proposed Model

In this section, we compute the user's trustworthiness and privacy risk based on above defined parameters and metrics.

A. Computing individual parameters

For defining our model, we assumed there exist a social-network *S* that maintains profile P_j of jth user U_j, where $j \in \{1, ..., N\}$ and *N* is the total number of user's profile. Every j_{th} user profile consists of *n* profile information I_n^j. As mentioned in above section IV, our data set consists of three parameters: profile information *PI*, reputation *R* and privacy settings *PS*. Each of these parameters contains different factors f_i where *i* is the number of factors. Each of these factors contains *k* options selected by user. The selected k_{th} option of user U_j has been collected as the response r_k for i_{th} factor. Based on different order of preferences, we rated (denoted as m) each options in factor f_i between $[1, k]$ such that, if k_{th} option is preferred more over $(k-1)_{th}$ option then rating will be *k* and (*k*-1) respectively. Figure 2., shows all the factors under each parameters used in model.

Parameters	Factors	Options
1. Profile Information	**a. Occupation**	**None or working/student**
	b. Qualification	**None or 12th/UG/PG/above**
	c. Number of groups	**None, 1 to 10, 10-20 or greater than 20**
	d. Number of friends	**0 to 50, 50 to 100, 100 to 300 or greater than 300**
	e. Time period of using SNS	**Less than a year, 1-7 year or greater than**
2. Reputation	**a. No. of Followers(e.g. in Facebook)**	**None, 1 to 10 or greater than 10**
	b. No of Recommendation/ Endorsement (e.g. in LinkedIn)	**Never, rarely or frequently**
3. Privacy Settings	**a. Person you accept in your profile**	**Only friends, Known in person, everyone**
	b. User preference to actively Safeguard of information in SNS: email id, photos/videos, relationship status, conversation history, religious, political beliefs, posts/status.	**Highly, somewhat or none**
	c. Consider privacy setting as important	**Always or never**

Figure 2. Response collected from user in each parameters

The formula for computing responses r_k given by user as:

$$r_k = \frac{m_k}{\sum k} \tag{1}$$

where, m_k is the ratings for k_{th} option. Since, users' trust can be derived from their profile information *PI*, reputation *R* and privacy settings *PS*, we computed weighted probability of individual parameters (*PI*,*R*,*PS*) as:

$$P(PI_j) = \frac{\sum W_i^{PI} * r_k}{\sum W(f_i^{PI})} \quad where, i \in \{1, 2, 3, 4, 5\} \tag{2}$$

Here, $P(PI_j)$ is the probability of Profile Information *PI* of jth user and W_i^{PI} is the weight of factor f_i on Profile Information *PI*. For our calculation we have taken W_i^{PI} = 1 for each factor.

$$P(R_j) = \frac{\sum W_i^{R} * r_k}{\sum W(f_i^{R})} \quad where, i \in \{1, 2\} \tag{3}$$

Here, $P(R_j)$ is the reputation *R* of jth user and W_i^R is the weight of factor f_i on Reputation *R*. For our calculation we have taken W_i^R = 1 for each factor.

$$P(PS_j) = \frac{\sum W_i^{PS} * r_k}{\sum W(f_i^{PS})} \quad i \in \{1, 2, 3\} \tag{4}$$

Here, $P(PS_j)$ is the privacy settings *PS* of jth user and W_i^{PS} is the weight of factorf_i on Privacy Settings *PS*. For our calculation we have taken W_i^{PS} = 1 for each factor.

B. Trust value

The overall trust value $\top_j$ of user *j* is based on the reputed trust τ_j, privacy awareness PA_j and alert factor AF_j metrics. Each of this metrics are computed as:

1) Reputed Trust τ_j: The reputed trust refers to the trustworthiness of the user U_j from the perspective of other users in the friend circle which is calculated as:

$$\tau_j = \alpha * P(PI_j) + \beta * P(R_j) \quad where, \alpha = \beta = \frac{1}{2} \quad (5)$$

τ_j is the reputed trust. α and β are system parameters used as normalization factor. Recall that $P(PI_j)$ and $P(R_j)$ have been calculated by Equation (1) and(2) and depends on the responses *r* collected by user.

2) Alert factor: Using factors f_i, we created polytomous matrix of $i \times z$ where, as mentioned *i* is the number of factors from 1 to 9 and *z* is the ratings given by user to each of the factors from 1 to 9 where, 1 means higher preference and 9 refers to lower preference. The factor which have got higher ratings, is the one which user preferred to check mostly when responding to friend requests. Assuming this fact, we arranged all the nine factors f_i in decreasing order from $\{ 1, \cdots, 9 \}$ as shown in Figure 3.

Factors
1. Known in person in real world
2. Mutual friends
3. Past conversations
4. Photo
5. Location common background
6. Wall posts/Status
7. User activity pattern/ Open profile informations about user.
8. Date of creation of profile
9. Verifying user by Google search

Figure 3. Factors preferred while responding to friend request

Let the matrix $U_j \times f_i$ shows the preferences of the user for different factors where $\rho_i^{U_j}$ is the preference of the j_{th} user U_j for i_{th} factor, which is derived as:

$$\rho_i^{U_j} = \frac{z_i}{\sum i} \quad where, i \in \{1, \cdots, 9\} \quad (6)$$

such that $\rho_i^{U_j}$ can take any value in (0,1) and z can take value from $\{1,\cdots, 9\}$. Using equation (6), the probability of alertness $P(AF_j)$ of j_{th} user before responding to friend request can be computed as follows:

$$P(AF_j) = \frac{\sum W_i * \rho_i^{U_j}}{\sum W(f_i^{PI})} \quad where \quad i \in \{1, \cdots, 9\} \quad (7)$$

where, W_i is the weight for each factor mentioned on matrix $U_j \times f_i$. W_i takes value from $\{ 1, \cdots, 9 \}$ according to the order of factor on matrix $U_j \times f_i$.

3) Privacy Awareness: A privacy awareness of jth user U_j is based on his/her privacy settings and their alert factor such as:

$$PA_j = P(AF_j) * P(PS_j) \quad (8)$$

where, $P(AF_j)$ and $P(PS_j)$ as computed from Equation (4) and (7) can take any value between [0,1]. The overall trust value of user *j*, denoted by $\top_j$ depends on the user's awareness for his/her privacy and reputation of the user, this can be derive as:

$$\top_j = (PA_j + \tau_j)/2 \quad (9)$$

The overall trust value $\top_j$ of j_{th} user is normalized into [0, 1].

C. Privacy Risk

As defined in previous section IV, the privacy risk PR_j for a user U_j is the risk of exposing personal sensitive information.

1) Exposed Information: The exposed information EI_j of j_{th} user is calculated by collecting responses on how user safeguard their q_{th} personal sensitive information. Figure 4. shows all the personal sensitive information that are considered hidden or not disclosed, if selected by user.

Personal Sensitive Information
1. Relationship status
2. Photo/videos
3. Post/Status
4. Contact details
5. Location/city
6. Wall posts/Status
7. Interests like hobbies, music and sports preferences
8. Date of birth
9. Political/ religious view
10. CV and Business details
11. Email Id
12. Post about recent activities (what are we doing now)

Figure 4. Personal sensitive information that are hidden on users choice

Here,we collected responses as 0 or 1 using dichotomous $N \times q$ matrix where j is the number of users on social network from $\{1,...,9\}$ and q is the number of personal sensitive information. In matrix, whenever j_{th} user who prefer q_{th} personal sensitive information to be hidden, the response r_{jq} is marked as 1 and 0 otherwise. The exposed information is computed as:

$$EI_j = (1 - \frac{\sum_{q \in 1}^{12} r_{jq}}{\sum q}) \quad (10)$$

In theory, the concept of risk is modeled as the expected value of an undesirable outcome. That is

Risk = (probability of happening of undesired event) $*$ (expected loss of the accident)

In the context of privacy risk, we propose that privacy risk PR_j for a user U_j as a function of privacy awareness, privacy settings and the exposed information. That is:

$$PR_j = \frac{(1 - PA_j) + (1 - P(AF_j))}{2} * EI_j \quad (11)$$

The value of the privacy risk lies in the range of [0,1], which shows the risk of information exposure to any malicious third party if user is unaware and unconcerned about his/her privacy.

V. Result Analysis

In this section, we introduce the results of the analysis of our proposed trust model and privacy risk. For our model, we have taken a sample of 50 users from our data set . After analyzing, we consider the overall trust level $\top = 0.56905$ as neutral. Therefore, users with trust value above 0.56905 is considered to be Trustworthy and below are Untrustworthy.

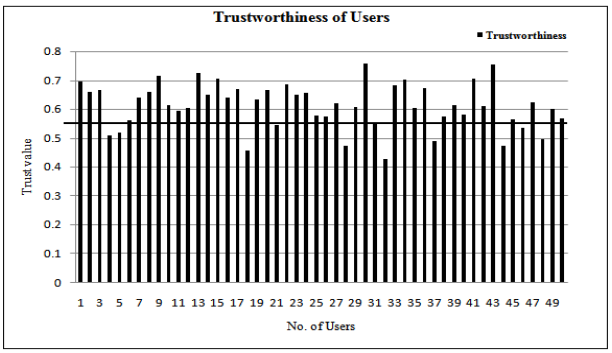

Figure 5. Computed trust value

Figure 6. represents the value of privacy risk derived from Equation (12). The maximum privacy risk according to our model as derived from data set, is 0.53 which shows the risk for user on exposure of personal information. The user with minimum privacy risk i.e. 0.07, are having better understanding of privacy settings and are aware of the consequences of information exposure in social network.

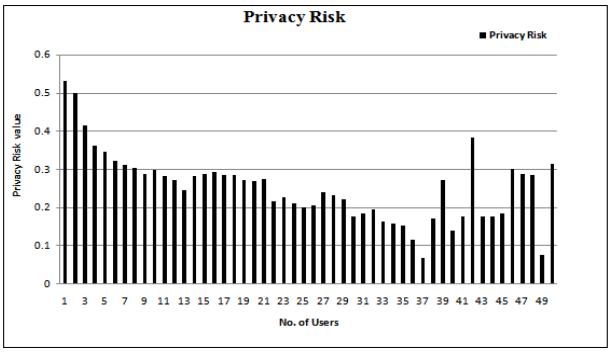

Figure 6. Computed Privacy Risk

In Figure 7. we showed how privacy risks of the user relates to trustworthiness of the user. Here, we found an inverse relationship between trust value and privacy risk, that means, if any user A has high trust value, then his/her privacy risk will be less based on its preferences to privacy settings. This can be explained in the context that if the inferred trust of the user is more than trust level, then the user has high privacy awareness which lower the risk of information exposure.

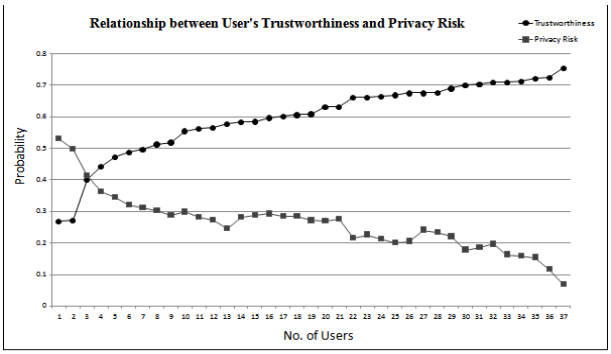

Figure 7. Relationship between user's trustworthiness and privacy risk

A. Standard Error

The trustworthiness of a user is a personal and subjective concept that depends upon user's choices of disclosing information. This creates some amount of ambiguity and challenges in evaluating the confidence for users trust value. Thus, we calculated the accuracy and performance of the trust value using standard error (SE) as:

$$SE = \sqrt{\frac{P(1-P)}{N}} \tag{12}$$

Where P is success rate and N is number of people in data set. Figure 8. shows the standard error in derived trust value for sample data set of 50 users.

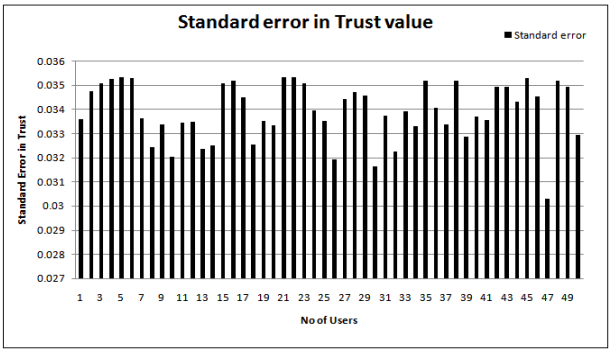

Figure 8. Standard error in trust value

In case of user's trustworthiness, the maximum overall standard error calculated for the given set is 3.59 %. Thus, for the collected data, 65% of the users are evaluated to be Trustworthy.

VI. Conclusion and Future Work

We have presented a method to compute the user trustworthiness based on available profile information, recommendations, endorsements and followers and their customized privacy settings. We illustrated the impact of exposed information and unawareness of user by computing privacy risk. Our model helps to set conclusion, that users willingness to disclose information and knowledge of privacy settings affect the trust value. A present work illustrates how a user can check the

trustworthiness of other user before accepting his/her friendship request and letting him in his/her network. In case of a large number of users there are possibilities of fake cases where a user intentionally sets his/her profile information and privacy settings similar to a trusted user. For identifying such cases we need to rank user's profile as fake and trusted profile on the basis of parameters such as verifying from mutual friends or from his/her mentioned organizations and work place. As for our future work, we will try to improve the privacy of users by refining our model in large network where we can differentiate between fake and real profile users.

REFERENCES

[1] D. Gambetta, "Can We Trust Trust? Trust: Making and breaking", Cooperative Relations, UK University of Oxford, 2000, pp.213-237.

[2] *http://www.telegraph.co.uk/news/uknews/defence/10948490/Troops-leaked-confidential-data-on-Twitter-and-Facebook.html.*

[3] *http://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud.*

[4] Hootan Rashtian, Yazan Boshmaf, Pooya Jaferian, Konstantin Beznosov, "To Befriend Or Not? A Model of Friend Request Acceptance on Facebook",in CMU Symposium On Usable Privacy and Security, 2014

[5] Nurul Nuha, Abdul Molok Shanton Chang, Atif Ahmad,"Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats", Australian Information Security Management Conference Security Research Institute Conferences, 2010.

[6] Yu-Jong Jang1 and Jin Kwak2, "Access-control-based Efficient Privacy Protection Method for Social Networking Services", International Journal of Security and Its Applications Vol.7, No.5 (2013), pp.305-314, 2013.

[7] Bapna, R., Gupta, A., Sundararajan, A., Rice, S., Trust, Reciprocity and the Strength of Friendship Ties: Experiments on an Online Social Network, 2012: National Bureau of Economic Research Summer Institute on the Economics of IT and Digitization, 2011, Cambridge, MA.

[8] Raymond Chi-Wing Wong, Ada Wai-Chee Fu, Ke Wang and Jian Pei.,"Anonymization-Based Attacks in Privacy-Preserving Data Publishing" 1986: Harvard University Press.

[9] Ali El Attar, Antoine Pigeau, Marc Gelgon " A decentralized and robust approach to estimating a probabilistic mixture model for structuring distributed data.", IEEE/ACM Int. conf on Web Intelligence, Aug 2011, Lyon, France. pp.372-379, 2011.

[10] Chaochen Qian, Xiaochun Xiao, Siming Chen, Xueping Wang., "Grouping Friends to Improve Privacy on Social Networking Sites" in Conference Anthology, IEEE,2013.

[11] Yongbo Zeng1, Yan (Lindsay) Sun, Liudong Xing, and Vinod Vokkarane, "Trust-Aware Privacy Evaluation in Online Social Networks." , in University of Rhode Island, Kingston. IEEE ICC 2014 - Communication and Information Systems Security Symposium.

[12] Prateek Joshi , C.-C Jay Kuo, Security and privacy in online social networks: A survey, Proceedings of the 2011 IEEE International Conference on Multimedia and Expo, p.1-6, July 11-15, 2011

[13] Arnostka Netrvalova and Jiri Safarik.,"Trust Model For Social Network"

[14] Ralph Gross, Alessandro Acquistion, and H. John Heinz.,"Information revelation and privacy in online social networks.", ACM Workshop on Privacy in the Electronic Society (WPES 2005): November 7, 2005, Alexandria, Virginia, USA ;, pages 7180, New York, 2005. ACM Press.

[15] Guido Barbian,"Assessing Trust by Disclosure in Online Social Networks", in proceedings of the 2011 International Conference on Advances in Social Networks Analysis and Mining.

[16] C. Dwyer, S. Hiltz, and Katia Passerini " Trust and privacy concern within social networking sites: A comparison of facebook and myspace.", in Association for Information Systems, editor, Proceedings of the 13th Americas Conference on Information Systems (AMCIS), page paper 339,2007.

[17] Kun Liu and Evimaria Terzi,"A Framework for Computing the Privacy Scores of Users in Online Social Networks", in ninth IEEE International Conference on Data Mining,2009.

[18] Preeti Yadav, Savita Gupta, S. Venkatesan.,"Trust Model for Privacy in Social Networking using Probabilistic Determination.",in International Conference on Recent Trends in Information Technology, 2014.

[19] Jennifer Ann Golbeck,"Computing And Applying Trust in Web-Based Social Networks", Doctor Of Philosophy, 2005.

[20] Surya Nepal, Wanita Sherchan, Cecile Paris.,"STrust: A Trust Model for Social Networks ",in Information Engineering Lab .CSIRO ICT Centre, Australia.International Joint Conference of IEEE TrustCom- 11/IEEE ICESS-11/FCST-11, 2011.

[21] Guanfeng Liu, Yan Wang, Mehmet Orgun,"Trust Inference in Complex Trust-oriented Social Networks", International Conference on Computational Science and Engineering,2009.

[22] Agrima Srivastava, G Geethakumari,"A Framework to Customize Privacy Settings of Online Social Network Users", IEEE Recent Advances in Intelligent Computational Systems (RAICS),2013.

[23] *http://its.ucsc.edu/security/training/intro.html*