IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. I (Jan.- Feb. 2018), PP 53-60
www.iosrjournals.org

Preventing User Becoming Vulnerable By Measuring the User Behavior in OSN

S. Revathi[1], Dr.M.Suriakala[2]
[1] *Asst.Professor, Dept of Computer Application, A.M. Jain College, Chennai, India.*
[2] *Asst.Professor, PG & Research, Dept of Computer Science, Dr.Ambedkar Govt Arts College, Chennai, India.*
Corresponding Author: S. Revathi

Abstract: *Social Media propagates many information, but everything that is distributed in facebook, twitter etc need to be trustful. Before accepting news from a recipient we need to know whether the information is from a friend or vulnerable persons. After sharing information which is private between user and his/her friend, and it has been made public by his/her own friend which is a great threat to the privacy o f the user, then a decision has to be made whether to make him/her continue has a friend or not. User vulnerability must be checked. The validity of a user is determined by how much a user is active in Online Social Network (OSN), so more active he is more vulnerable. Previous methodologies reveal that by measuring the visibility of a user in OSN, vulnerability check can be estimated. But exclusion of user behavior in measuring user visibility is a drawback in previous methodology which we are going to take into account in this paper.*

Keywords: *User vulnerability, Visibility, User behavior, Information Provenance, Community.*

Date of Submission: 06-01-2018 Date of acceptance: 25-01-2018

I. Introduction

Social media is defined in as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content."
There are many social media websites which include social networking sites that is Facebook, LinkedIn, etc., blogging websites such as Huffington Post, Business Insider and micro-blogging websites such as Twitter, Tumblr etc. There are other kinds of social websites

- Wikipedia,
- Wikitravel,
- Wikihow, etc.,

Social news channels are Digg, Slashdot, Reddit, etc.

The other kinds of social media website are social bookmarking websites such as Delicious, StumbleUpon, etc, media sharing websites such as Youtube, Flickr, UstreamTV, etc. The opinion, reviews, and rating websites such as Epinions, Yelp, Cnet, etc. and community Q&A websites such as Yahoo Answers, WikiAnswers [1] are also a part of social media websites network.

A social networking site enables the users to share their profile in a web-based service. The users can create their profiles which can be shared with a network of friends and other users. Usually, the network for each user is a group of friends or known people.

Social media websites are used a means to share their thoughts on various topics whether it is personal or a social subject. The users in a group react to the shared information which creates interest and awareness in the group. Communication is the main agenda behind these websites which made them popular [2].

While it is true that social media websites have broken the barriers when it comes to communication it becomes tough for users to understand the validity of the information. It is dangerous to share the information that is passed by an unknown user as this can be invalid or can be against the rules of sharing in the social media.

Sometimes the information that is shared publicly can cause damage to the reputation of the shared person or he/she can get into a legal situation when it is about the other person. Provenance data can help in such situations as this can validate the statement. The non-availability of provenance data to the users makes it tough.

The availability of provenance data is tough as it needs a change in the infrastructure of the social media. The provenance data can be very useful as the social media users can know the facts. The provenance

data is mining for the facts and it requires the careful management of metrics so as to provide facts to the social media users.

The social media is becoming an intrusion into private life which is not a favorable situation. The provenance data is also in threat as the unknown information which is not valid is spread in social media. The intrusion of privacy and spreading of false information is possible by taking some measures by an individual and as a community.

Social media websites should act as a channel of communication for interaction, content sharing, and collaboration between users of the network. Social media mining has many areas such as user vulnerability, behavior analysis, location-based social network analysis, Information provenance etc.

The Rapid progress of information technology has changed the way how people interact, express themselves and behave in social media. Due to this challenging behavior the information spread by them is subject to the question of reliability and authenticity which leads to trustworthiness. In OSN like facebook the individual users may join in any community they want if its open and they can join in any community with admin's approval if it's a closed group. In facebook they also have facility to send request to add them as friend to anybody they like to be a friend and they have options to friend, unfriend and message to the person who send friend request to the user.

Once the user became friend and joined the community, the user's large amount of personal information and the user status, posting on his walls are open to them. So the user must be confident that the recipient is a friend before accepting the request. Many times and there are chances the persons added as friends may acts as foe by breach of privacy friends [4].

The paper proceeds as follows

- Linking Information Provenance with User Vulnerability
- Defining Vulnerability and Visibility
- How vulnerability influences Community?
- What is a Community Structure?
- User Behavior in Community
- Giving the related works in user vulnerability and user visibility
- Defining the Proposed algorithm to protect user becoming more vulnerable.
- Future work and conclusion.

II. Linking Information Provenance With User Vulnerability

Before accepting information from a recipient the user must be confident that the recipient is a friend or otherwise he/she should not accept the information and pass it on because the information is not trustworthy.

The social media users become vulnerable when they share private information on the social networking sites. There can threats such as

1) When personal information is posted on social networking websites, an individual or group of people with malicious intentions try to take the advantage of the information which makes them vulnerable.
2) The information in the hands of malicious people can be a reason for great pain to the users as the personal information can be morphed or changed in a bad way and circulated in the social media websites.
3) Sometimes the social media user can bring threat to his/her associates or friends by posting personal information about them without their permission.

III. Vulnerability And Visibility

With the advent of social media websites, sharing of information whether they are pictures, the current location of the person or any other personal information, this can lead to the breach of privacy. The sharing of personal pictures or information by friends or relatives is also the breach of privacy.

It should be kept in mind that the information that is shared on social media websites is prone to leakage to other users. The visibility of the user determines the percentage of increase in sharing the information. The visibility of a user is the number of people with whom the user is friend with and how popular the user on the social media websites. It also depends on the visibility of the friends the user has.

It becomes important to take care that the user on social media websites has less number of vulnerable friends as they can increase the vulnerability score. If the removal of a friend in a user's group decreases the vulnerability score, the friend is considered as vulnerable. A method to find the vulnerability on social media websites was proposed in [5].

Information that is sensitive i.e., which hurt the religious sentiments of others or some statements about some anti-social groups can create havoc when spread on the social media websites. These kinds of information or any other personal information about themselves or others can be dangerous. The information is usually shared through user's profile, status updates, messages etc.

The social media websites have information revealing options such as the information such as the friends of the user, residential address of the user, interests related to movies, interests related to shopping etc. These sites also have options to reveal personal information through various attributes.

The sharing of personal information with other members of the group increases the responsibility of the friends or the members to keep the private information safe and secure. The privacy settings in these websites can be used to reveal only information that is believed safe to be safe to share. But many users do not use the privacy settings for many reasons which include lack of knowledge.

The privacy settings if not used properly can lead to the breach of privacy. the information that is public can be taken advantage by stalkers, spammers, and hackers who use the information for various wrong causes. Especially children and teenagers can get into trouble or worse can happen if proper measures are not taken to protect the privacy of the users.

Especially users who are public figures in entertainment and political arenas get affected by the comments they get on the social media websites. People with high profiles such as the founder of the Facebook has also faced many emotionally disturbing situations which he himself admitted. Even the private users are in a danger of getting breached of their privacy if the personal information is shared by other users in an irresponsible way. These friends can be considered as vulnerable [6] on the social media websites.

There are many factors which can make the friends on the social media websites as vulnerable friends. Any user on identifying his/her vulnerable friends should take proper measures for protecting themselves on the social media website. To protect the privacy of the users, the social media websites proposed in [7], which have categorically divided the attributes on social networking websites as personal attributes and attributes that are related to friends and family. Personal attributes comprise of user's information which is related to the user. Community attributes include information about friends, tagged pictures, wall interactions, etc. The personal attributes can be seen by friends but they may not be accessible to all the members of the group.

The visibility of the individual attributes can be taken care using the privacy settings but this may not be possible in case of the community attributes. Especially the pictures that are tagged and the information that is shared on the wall cannot be controlled on Facebook. Efforts are being taken to protect the private attributes but the community attributes are being left vulnerable.

Usually the information which can be seen by everyone is vulnerable on social websites.

IV. How Vulnerability Influences Community

The social media network consists of a number of websites that allows users to have conversations with their friends, share the information and know the information about other users. Broadcasting is sending or sharing a piece of information with everyone in the group at a time. Twitter can be considered as a good example of broadcasting.

E-mail or other conversations on Facebook are one to one, but Twitter allows anyone to broadcast the message to everyone who is following the user who is broadcasting the message. The tweet can be sent intending to a particular person by placing a @ followed by a username even though the tweet is being shared with everyone [8].

The research studies reveal that most of the adults use the social media on a wide range which includes Instagram, Facebook, Twitter etc. There are an estimated 1 billion Facebook users worldwide. Facebook is not only for sharing information and interacting, this can be used to pass the message to someone who can help in danger. This is a real case scenario which was shared on Facebook where two young girls were missing during a storm drain accidentally in Austraila. The girls were able to use the distress message on Facebook using a cellphone.

We can come to a conclusion that Facebook was able to save the girls as the friend on Facebook forwarded the information to the local authorities. The social media websites can be used to browse the public content posted or an account can be created and follow other users in the network.

Some social media websites allow the third party messages, for instance, the online marketers can use the Twitter to broadcast the messages about their products. The access to a broad range of people made the social media websites a source of reaching the customers which can also generate income through advertising. The broadcasting of information, the people in the group who look at the information has become a source of earning revenue for the social media websites.

Broadcasting on the social media websites has created a new range of audience called the digital audience which is estimated to be in millions. Someone like Justin Beiber who has millions of followers has the capability to reach the millions of audience. This following can be used to promote a brand of clothing or accessories by many companies. The ability to engage the audience can be useful to the user who is able to collect and engage the audience as well as the organization which uses the user to broadcast the message [9].

V. Community Structure

Social media networks allow peer-to-peer connection and they encourage the users to establish more and more connections. A community in a social media network is a collection of people who have joined the network to connect with friends and other users.

Sometimes the users in a group connect and they may become good friends. The difference between Social networks is that these are generally top-down in structure and these social networks support broadcast mechanisms whereas communities are more flexible and allow member input and discussion.

Social networks may contain communities and are made up of social communities. Social networks can be defined as a mutually exclusive website. The instance can be taken as Google+ because the content from this website cannot be posted on Facebook.

Social communities are usually platforms which are usually in nature and where the contents of all types can be shared. The content can be from social networks or the original content [10].

VI. User Behavior In Community

The research conducted on social communities says that behavior of users includes many social activities. The activities can be making friendship with users in the community, publishing content/blogs, browsing profiles, chatting with friends, making comments on the content or posts of other users etc. Many users are harmless and their activities are not dangerous to other users while some users can cause harm to other users through their malicious activities.

There are innumerable accounts in the social community who create trouble for other users by creating posts or sending messages. The best way to protect them is to block the users whose intentions are malicious.

The User may think his/her friend is protecting the privacy after accepting him/her as a friend but sometimes this rule may be violated. The User's friend may behave differently in some situations or in all situations he/she may not protect the privacy of the user. Particularly in Community privacy may be shattered and distress may be caused by the user's friend. The user is becoming vulnerable because of Friend (foe).

VII. Related Work

The vulnerability and visibility of the user are determined by the amount of personal information that is revealed online and also on the friends of the user. Recently in [11] evaluated the less amount of personal information revealed on social media websites and the efficiency in using the privacy settings can minimize the visibility and vulnerability of the user.

The studies revealed that only a less number of users on social media network can change the default options related to privacy on the Facebook. In [12] the users on social media network are not protected fully. Inadequate and inconsistent conditions and settings make the social networking sites vulnerable.

In a scheme proposed for deanonymization [13] the users of the group share or use the information on social media websites with malicious intentions which causes the breach of privacy. Some of the users create wrong profiles by filling the attributes with wrong information and describing themselves with rich attributes.

These kinds of users make the social networking sites vulnerable and the research is being done to make the users aware of the risks and vulnerability of these sites. In [14], it is discussed how the personal information can be misused by third parties with malicious intentions.

The research done on the social media websites related to the protection of privacy suggests that some fundamental changes have to be done in the social networking sites to create privacy in these sites. In [15] new techniques which are related to collective privacy mechanism are much useful for managing the privacy of the content that is shared on the websites.

In [16], it is discussed on the ways of helping users of how the simple privacy settings are used and the meaning and usage of other attributes or shared data ownership are confusing and not used properly. In [17] it is explained how an action can exploit a user on social media networks. The information that is shared on the social media network gets leaked by followers sharing the information and how visible the user is in the network topology.

The chances of information being leaked in the social media network depend on the connectivity of the user with other users directly or indirectly. It depends on the choice of the user which information to share and reveal. It is better not to share the information which is considered to be private as the information shared will be revealed or shared on the social media network by the other users and friends.

In [18] a framework of social media network is designed where users have the choice to share the information with particular users on the group through encryption-decryption algorithms. The framework which is designed is supposed to address the privacy issues of the users. This comes at the cost of increased response time from a social networking site.

In a study to reduce the vulnerability of the user unfriending or blocking the vulnerable friend [19] is the method proposed. In [20] a method is proposed to measure the visibility of the users in social community networks. The procedure that is stated depends on the percentage of information leaked.

The percentage of information leakage depends on the number of users/friends in the vicinity of the user in a single or more jumps. The information leakage also depends on the factors such as the neighbor nodes in the OSN.

The study reveals that the number of vicinity nodes a user has, who are interested in the user's information can be a factor which determines the visibility of the user in the social media network. The technique [21] proposed to determine the type of attributes.

Personal attributes are those which reveal the personal information of the user. The other attributes are the ones which reveal the information about friends of a user. These two types of attributes cab be seen by the friends of the user but not by other users.

The privacy settings of a profile can be used to control the visibility when it comes to personal attributes but may be tough with most other attributes. The instance of Facebook reveals how the users can control certain information about friends but how the user cannot control certain information when shared through photo tagging and wall interactions.

The topological properties of the network are used to measure the visibility of the user in the social network. The results from various studies state that the visibility of the users in a social network depends on the local topological properties.

The observations from studies help to develop simple techniques to determine the visibility of the user. The local topological characteristics are used to determine the visibility of the user. A method is developed to evaluate the visibility of the users depending on the structure of the social media network. The real OSN graph generated by follower's dataset of Twitter is used to determine the visibility of the users in case of Twitter.

The studies also showed that the structure of the network is assortative. The probability of connection is more with similar nodes and with similar topological characteristics. These studies were used to develop a technique to estimate the visibility of the users depending on their local topological properties. This mechanism can be used to calculate the visibility and can be used to tune their privacy settings accordingly.

The factor of user behavior is not taken into when calculating the visibility of the user. The user behavior can be defined as how much active the user is on the social media network. In this paper, the technique is to include the missing factor called the user behavior. The user behavior is calculated based on the activity of the user in the OSN and the other factors such as sharing the user makes on the social media network.

The software called the Social Privacy Protector software (SPP) is developed to protect the privacy of Facebook users in [22]. The SPP software has three main parts:

1) Friends Analyzer Facebook application - This application is responsible for identifying a user's friends who can be a threat to the privacy of the user.
2) SPP Firefox Add-on - This application analyzes the user's privacy settings and also helps the user to improve the privacy settings with just one click.
3) HTTP Server - This application is responsible for storing the results of each user. This can help in determining the potential threat of privacy [23] by the user's friends. The application helps in finding the potential threat by the user's friends by calculating the credibility score for each friend of the user. The credibility score is calculated by using some sophisticated algorithms.

The Social Privacy Protector Firefox Add-on application is also part of the SPP software. This application helps in improving the privacy settings of the user easily. The Addon helps in monitoring the user's internet activity and also the number of applications installed on the user's Facebook profile.

The application also warns about the applications can pose a threat to the user's privacy [24]. The Add-on also informs about the vulnerable friends to be restricted. The software prepares a webpage, which has a sorted list of all his/her friends and the friend's score. The friends with the low vulnerability score have the highest likelihood of having fake profiles. These names appear on the top of the list. The user can restrict the access to the potential fake friends by simply clicking the restrict button attached to the friend [25]

The application also provides the user with an interface to view all the friends in an alphabetical order. The user can restrict any of the friends easily which makes it easy to protect themselves not only from fake friends but also from all the users [26].

The Tool introduced by Michael fire et al called as SPP software in FB, does not suit for communities, it can access only on limited data set, Chrome and IE does not support this software.

VIII. Proposed Algorithm

The Facebook (SPP) software created by many disadvantages, as mentioned above. So in order to overcome all those difficulties, an algorithm is proposed. One thing has to be considered that algorithm for fake user identification. Another methodology stated is that user behavior in OSN reveals that more the user is active then he/she propose a threat to his/her friend. A method was proposed to measure visibility of a user which didn't include User Behavior (UB) factor. They concentrated on network topology how many hops he/she makes. But the proposed methodology is to identify the friends who are turning foe by not protecting his/her friend's privacy. So this proposed methodology is for Facebook users who can be protected from becoming vulnerable user by using this proposed method. The proposed method is as follows, By making the User Behavior (UB) factor taken into account if a user behaves like whenever information is shared by the user his/her friend shares it in community, Whatever the information may be, but the friend shares with everybody. Then this behavior is noted as the UB, if the UB factor becomes high then particular user's visibility measure becomes high. If the visibility is high then he/she is a dangerous friend to share private information. So the dangerous friend of this user makes him/her vulnerable and hence he/she must be avoided in the community.
This technique is used to transform the structure of the social media network. This is done by removing the friends who increase the vulnerability of the user in the social media websites.

PROCEDURE UBF (id,C,G,node,pnode)
vcount=0, UB=0, n_s =0
id_s← connected components (G)
For all id €id's do
G_i€← G(id, id)
End for
For all G €G do
(C,Q) ← Community(G)
For all node € G do
n = node € C
pnode = node
if vcount(pnode) == null then
exit
elseif vcount (pnode) → n_n then
vcount(pnode) ← vcount(pnode) + 1
end if

if vcount(pnode(n_s)) > vcount(pnode) then
UB = UB + 1
Else
Print UB
End if
If UB == threshold value then
Delete (pnode)
Else
Accept (pnode)
End if
End for
End for

Working of Algorithm

Say in a network topology nodes (n1,n2, n3…..) are the users if n1 hops n times in the cluster then it is normal and score is n times. When the score of say n2 hops to n3 m times and for n1 m*m times in h hours then the UB factor is given as mm times which is high and he/she should be rejected.

The work and the techniques provide an efficient technique for improving the privacy and security of the users in the social media network. These methods and techniques in this proposed algorithm are not discussed in the previous algorithm which is the user behavior factor. This proposed algorithm provides an efficient way to measure user behavior in OSN. This algorithm traverses all nodes in the graph or network, and after the user shares information to a friend and it is been leaked public then this algorithm tries to identify the friend. A visit count variable is created and that node is incremented whenever the friend visits some of the community members. If the private information is shared by a foe (friend) then ns(sharing) is determined for the present node. If vcount (pnode(ns)) that is the visit count of the shared variable for the present node reaches a

high then UB is incremented, When UB reaches a threshold value then the friend is deleted from the community otherwise he/she is accepted. Nodes that are represented here is user and their friends in community. If the user passes an information to n(m) friends i.e., there may be n friends in community but he/she is passes the information to anyone of the trusted friend. But the trusted user makes n+m hops which mean he/she shares the 10 out of 10 information's to all users in community which is very delicate for a trusted friend. So here the user becomes vulnerable, so by inducing the UB factor the user may check on the trusted friends in the community thus who is leaking the information.

So network topology must be included and the cluster of community friends must be checked whenever necessary. This method can be implemented by adding a privacy button in the Facebook not restricting the fake user but to protect the user from his/her friend who is behaving like a foe.

IX. Future Research And Conclusion

The Algorithm proposed here provides an efficient way to identify vulnerable user and to find the dangerous friend of user and determines to get rid of the friend (foe).

Some of the friends on the social networking sites may be of malicious intent or with fake profiles. The users can improve their privacy by finding the vulnerable friends and by removing them from the list of friends. This can lessen the use of the social networking service but this strategy improves the security and the privacy of the user.

In future research overcoming the problems like fake ids and working of this algorithm in original dataset will be a challenge. Yet, to produce better method for protecting user's privacy is most important step to trust the data in social media. So this proposed method is the first step to trust friends in OSN and to give better ways to protect user's privacy and a path to use OSN without any threats.

References

[1] Altshler, Y.Elovici, A,B.Cremers, N.Aharony,and A.Pentland, "Security and Privacy in Social Networks" Springer NewYork, 2013.

[2] D.Irani, M.Balduzzi, D.Balzorotti, E.Kir da, and C.Pu, " Reverse Social Engineering Attacks in Online Social Networks" detection of intrusions and malware and vulnerability assessment, PP.55-74, 2011

[3] M.Conti, R.Poovendran, and, M.Secchiero, " Fake Book: Detecting Fake Profiles in Online Social Networks" Advanced in Social Network Analysis and Mining (ASONAM), 2012,IEEE/ACM International Conference on Pages, 1071-1078.

[4] A.Singh, A,H.Toderici, k.Ross, and M.Stamp, "Social Networking for Botnet Command and Control", MECS,I.J.Computer Network and Information Security,2013, 6,pp 11-17.

[5] A Kumar, S.K Guptha, A.K Rai, S Sinha, (2013), "Social Networking Sites and Their Security Issues", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013.

[6] M Chewae, S Hayikader , M H Hasan,(2015), "How Much Privancy We Still Have on Social Network", International Journal of Scientific and Research Publications, Volume 5, Issue 1, January 2015.

[7] Anjitha T, Harsha V, (2016) "Secure Authentication and Cyber Crime Mitigation for Social Networking Sites", International Journal of Science and Research (IJSR) ISSN 2319-7064.

[8] Yikader S, H Hasan, M. Chewae, M.C. Ibrahim J, (2015), "How Much Privacy We Still Have on Social Network.", International Journal of Science and Research (IJSR), Volume 5, Issue 1, p3755.

[9] Michael Fire, Roy Goldschmidt, Yuval Elovici, (2014), "Online Social Networks: Threats and Solutions", Ieee Communication Surveys & Tutorials, Vol. 16, No. 4.

[10] Shanley L, Lovell A, Center W, (2012), "On Cybersecurity, Crowdsourcing, And Social Cyber-Attack",https://www.wilsoncenter.org/sites/default/files/127219170.

[11] Mohamed Shehab a, Anna Squicciarini b, Gail-Joon Ahn c, Irini Kokkinou "Access control for online social networks third party applications" Elsevier-Computers & Security 31 (2012) 897-911.

[12] Ratnapala I P, R G Ragel and S Deegalla, "Students behavioural analysis in an online learning environment using data mining,"IEEE 7th International Conference on Information and Automation for Sustainability, pp. 1-7,2014.

[13] Yunlong Wang and Petar M. Djuric, "Social Learning with Bayesian Agents and Random Decision Making," IEEE Transactions on Signal Processing, vol. 63, no. 12, 2015.

[14] Song, Yang, Zheng Hu, Xiaoming Leng, Hui Tian, Kun Yang and Xin Ke, "Friendship influence on mobile behavior of location based social network users," Journal of Communications and Networks,vol. 17, no. 2, pp. 126-132, 2015.

[15] Berjani, Betim and Thorsten Strufe, "A recommendation system for spots in location based online social networks," ACM 4th Workshop on Social Network Systems,2011.

[16] A. Algarni, Y. Xu, and T. Chan, "Social Engineering in Social Networking Sites: The Art of Impersonation," Proc. 11th Int. Conf. Serv. Comput. IEE Comput. Soc., pp. 797-804, 2014.

[17] A. Vishwanath, "Habitual facebook use and its impact on getting deceived on social media," J. Comput. Commun. ,vol. 20, no. 1, pp. 83-98, 2015.

[18] G. Nandi and A. Das, " A Survey on Using Data Mining Techniques for Online Social Network Analysis", in the International Journal of Computer Science Issues,'November 2013, vol. 10, issue 6, pp. 162-167.

[19] C. G. Akcora, B. Carminati andE.Ferrari, "User similarities on social networks", Social Networks analysis and Mining Journal, pp. 1-21, 2013.

[20] S. Nilizadeh, S. Jahid, P. Mittal, N. Borisov, and A. Kapadia, "Cachet: A Decentralized Architecture for Privacy Preserving Social Networking with Caching," in CoNEXT, 2012.

[21] A. Feldman, A. Blankstein, M. Freedman, and E. Felten, "Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider," in Usenix Security , 2012.

[22] Ferran Pla and L Hurtado. Political Tendency Identification in Twitter using Sentiment Analysis Techniques. In Proceedings of the 25th International Conference on Computational Linguistics , COLING'14, pages 183–192, 2014.

[23] Paridhi Jain, Ponnurangam Kumaraguru, and Anupam Joshi. @I Seek 'fb.me': Identifying Users Across Multiple Online Social Networks. In Proceedings of the 22nd International Con- ference on World Wide Web, WWW '13 Companion, pages 1259–1268, New York, NY, USA,2013. ACM.

[24] Un Ito, Kyosuke Nishida, Takahide Hoshide, Hiroyuki Toda, and Tadasu Uchiyama. Demo- graphic and Psychographic Estimation of Twitter Users Using Social Structures. In Online Social Media Analysis and Visualization, pages 27–46. Springer, 2014.

[25] Arco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, Moreno Carullo Department of Computer and Communication, University of Insubria "a system to filter out unwanted messages walls OSN user" IEEE Transactions on Knowledge And Engineering Flight Data: 25 Year 2013.

[26] Ying Chen, Yilu Zho, "Detecting Offensive Language in Social Media to Protect Adolescent Online Safety", ASE/IEEE International Conference on Social Computing, 2012.26. J. Sun, X. Zhu, and Y. Fang. A privacy-preserving scheme for online social networks with efficient revocation. In Proceedings of the 29th conference on Information communications (INFOCOM), pages 2516–2524. IEEE, 2010.

S. Revathi "Preventing User Becoming Vulnerable By Measuring the User Behavior in OSN." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 53-60.