User’s Privacy in Social Meadia using Altering Graph

[1]Bonepalli Pedda Uppalaiah, [2]Mandan Naresh
[1]Holy Mary Institute of Technology & Science, Asst.Prof, [2]Malla Reddy College of Engineering and Technology, Asst.Prof

Abstract— Social Media (SMs) have emerged as a very effective and popular means of communication among people from different region, religion age, sex, educational background, ethnicity etc. Popular SMs include Facebook, Twitter, LinkedIn etc. However, the recent Facebook Data Scandal of data breach has created many question of user’s data privacy. Researchers have found users to be much reckless towards protecting information at their own end. Due to weak privacy settings, users become vulnerable to SMs attacks such as information leakage, identity theft, cyberbullying, online harassment etc. In our work, I have discussed different privacy threats related to the SMs users. I have also conducted a survey based on the user perception about Online Social Network (SM) privacy and protecting his/her information from misuse. Based on our background study and our survey results, I have proposed a feature, in order to, make user aware of SM’s weak privacy settings. This feature will review user privacy settings and classify those settings standard as Safe, Unsafe and Critical Unsafe. A Pie graph used to show aforementioned classification while getting login to his/her favorite SM. This feature can be adopted by any popular SMs, thus creating privacy awareness among user. Through applying this feature, an SM user can view the level of privacy settings, thus, minimizing the chances for being victim to any SM threat.

Index Terms—SMs, Privacy, Information, Trust, threats

1 Introduction

Millions of people are connecting through SMs every day. Users of SMs vary in age, sex, region, ethnic, religion. However, teenagers are most attractive towards SMs like Facebook, Twitter, and Myspace etc. The term social networks introduced in 1960s. It describes the association of people together by relations in different aspects like family, work, hobby etc. In 1971, First social network was born by sending first email. However, Due to increase usage of SMs, various threats are affecting SMs users. All these threats related to SMs can be classified into two categories [1]:

a. Security-related threats
b. Privacy-related threads

Privacy of a user is very much significant in the context of SM. In this section, few important privacy-related threats are given.

i. User’s Anonymity:

Attackers can use the real name of person by making a fake account. Exploiting the anonymity phenomena in SMs, attackers can increase the number of victims for their own purpose [1].

ii. Leakage of personal information:

Due to poor privacy settings, attacker used to gain personal information like name, address, contact number, location of the victim [1]. This is a serious threat to a legitimate SM user.

iii. Identity theft:

Attackers steal the identity of a legitimate SM user and pretend them to be a real one while fooling other users connecting [1].

B. Security related threats

Security of a user is also an important aspect to be considered, in the context of SM. In this section, few important security-related threats are given.

i. Online Frauds:

SM users are generally, affected by frauds through wall posts, news feeds and through messages. For centuries, fraud has been utilizing by the criminals. In the Facebook world, frauds are effective particularly at attracting people simply by clicking on a link by an individual that would develop the interest of anyone. Spamming activities include providing information to scammers like credit card number or a Social Security number [18].

ii. Cyberbullying:

Cyberbullying includes the harassment of an individual through technology [10]. Cyberbullying carried through sending threatening messages to the SMs users. Under cyber law in any state, cyberbullying, which involves hacking or identity and password theft, are punishable.

iii. Identity theft:

Attackers steal the real IDs of the legitimate users. Attackers used to spoof the real identities of the users for illegal purposes [11]. Hackers often break into user’s personal e-mails. The main reason behind the lack of applying appropriate security controls on one’s own SM account.

iv. SMs Online individual harassment

Social networking sites (SNS) have been criticized for serving as a breeding ground for cyber -bullying and harassment by strangers. However, there is a lack of serious research studies that explicitly identify factors that make teenagers prone to internet abuse, and study whether it is SNS that is causing this recent rise in online abuse or is it something else [17].

In this research, our main purpose is to address privacy concerns of the user regarding SMs especially carefree users like teenagers etc. Therefore, I have conducted an online survey in the form of questionnaire regarding SM user privacy-consciousness, privacy-reviewing There is no such mechanism exist that would help user in reviewing his/her SM privacy.

The rest of this research article is divided into following sections: Section II includes Related Work, Section III describes methodology, Section IV contains the proposed solution, and in Section V Conclusion & Future Work is given.

2 Related Work

In this section, I discuss previous work on the privacy of SM user.

A. Challenges in using Online Social Networks

In [12] authors have discussed various challenges related to SMs. With the ever-increasing number of users, SMs platforms are not a more a safe haven for users. Shared data includes pictures, text, videos etc. Moreover, they have discussed the semantic security related to SMs. This is a survey-based research focusing on the security as well as privacy threats also. These threats include Identity theft, loss of personal information, phishing, Sybil and spamming attacks etc. [1]

B. User Privacy related Threats

In [3], the authors explain the user requirements to be their data always private. When a user posts this data online, many attacks affect the data including spamming etc. These kinds of attacks cause harm to the users. Attacker steal the user data by sending his/her a spam messages. The terrorists and social engineers usually carry out these types of attacks. In this research two divisions of threats are created. One belongs to the privacy-related and other links to the Traditional-based Networks Threats. Privacy-based online threats might include leakage of user's sensitive information like age, sex, contact no, birthday, address etc. Authors have proposed some solutions to these aforementioned problems. These include Building awareness for information disclosure, elevating educational campaign and modifying legislation.

C. SMs online attacks

Authors [4] have described some of the recent attacks that can affect user privacy. The reasons include the carefree attitude of user regarding sharing information and inadequate privacy measures by the SMs operators. Creating awareness among user is the major way to counter these types of attacks. In addition, there is need to build high profile security at the end of SM service providers.

D. Controlling Loss of unintended information on SMs

In [5] the problem of unintentional information loss was addressed. In order to, detect unintentional loss of information, a tool named as 'Priware' is developed. This tool helps in reporting loss of user information over the SMs.

E. SMs: User Privacy threats and Defenses:

In [6] the four causes of SMs user's privacy leakage were explained. These include the flaws in the design, the flow of information, and the user's limitations. Through controlling the aforementioned causes, the user can be safe from threats.

F. User Privacy threats and their solutions:

Authors in [7] have focused on privacy problems with a different perspective. They have found that the privacy risk is an important aspect not be ignorable. The user is bound to rely on the services provided by the SM owner. However, owners are not always trustworthy. They have created some mappings regarding users to SMs, SMs to data, user privacy to both users and SMs owner. They have proposed the privacy-related solutions on the base of such mappings.

G. User's willingness for protecting information, based on, improvement in privacy features of SMs

In [8] Author found the "information sharing" to be one of the major cause of threat to SM users. He criticizes the current privacy settings by measuring the privacy altitude. He had found that privacy should be based on user's own will. For this purpose, researcher had conducted interviews of different SMs users, therefore, find the type and nature of online privacy feature that user actually wants from the SM provider. In the end, he had proposed a solution to limit privacy threats, on the basis, of improved privacy features by user's own willingness.

H. Loss of User Trust in SMs:

The problem discussed in [9] is the limited trust of users in SMs. According to the research, there is an emerging trend of leaving SMs by the people. The foremost reason behind this act are the serious privacy concerns. Privacy, as well as Security threats, are also one of the main cause in creating concerns about using SMs. However, improvement in access-controls in SMs can enhance user trust level.

TABLE 1
COMPARISON OF POPULAR SMS IN TERMS OF THEIR PRIVACY FEATURES

Features	Facebook	Twitter	LinkedIn
Limit profile visibility upon sign up	Yes	No	No
Give the facility to control searching	Yes	No	Yes
Who can see when you are connected	Yes	No	Yes
Prevent from tagging in the post	Yes	No	Yes
Select the friends who can see your photo	Yes	No	Yes
The facility of blocking the user	Yes	Yes	Yes
Enable two-factor authentication	Yes	Yes	Yes
Limit data sharing with third-party app	Yes	Yes	Yes
Remove your account	Yes	Yes	Yes
Delete Address Information	Yes	Yes	No
Turnoff Location Tracking	Yes	Yes	No
Message controlling option	Yes	No	Yes

I. User's concern over privacy:

Authors in [13] have discussed on the concerns of the user regarding privacy. They have compared various privacy features of SMs. A single user usually have accounts in more than one SM. Hence, it is possible to have privacy leakage from any platform. Authors have also discussed the various

Privacy weaknesses found in SMs such as Facebook, Twitter, Myspace etc. Proposed solution consist of user awareness, strong password enforcement, awareness of personal information leakage, policy for changing password etc.

Facebook's Data scandal has recently affected more than 80 million users word wide and more than 50 million users in America. However, most of the people have not even change their login credentials on Facebook, Twitter or other social media [14]. This was also observed that people with weak privacy settings, affected most by the recent Facebook scandal.

However, Facebook has recently improved its privacy settings page following the famous "Cambridge Analytica" scandal [15]. Nonetheless, an anonymous group on Twitter had hacked successfully a very popular twitter account with more than 15 million followers [16].

3 METHODOLOGY

SMs privacy is of great concern for a user. A user may be using any SM platform. SMs vary in features, usages etc. However, information is the main aspect that is the vital part of any SM. In order to, protect the information a number of steps needed from user awareness to the improvement of SMs privacy features. In Table 1, I have compared different SMs features that can affect user's privacy. I have taken the famous SMs like Facebook, Myspace, and LinkedIn for our comparison. The results show that Facebook provides much better privacy features as compare to other two famous SMs. However, on the user side, I are unable to find any mechanism of reviewing their privacy settings. Users are usually unaware of the important privacy features, in order to; make their information limited to themselves only. Therefore, I have designed and conducted an online survey. The main purpose of this survey is to find out the factors influencing user privacy leakage. Below you can find the results of our survey and a brief discussion on these results.

Q.1) Do you have accounts in more than one Online Social Networks?

a. Yes

b. No

Results:

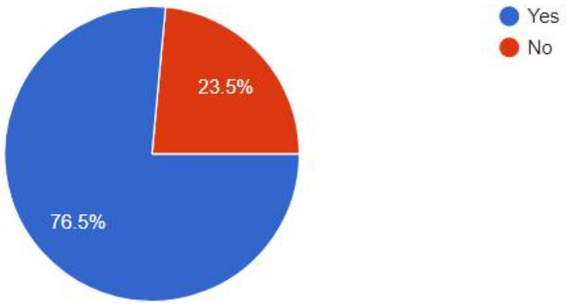


Fig. 1 Result of survey Q.1

Q.2) Which SMs do you think, offer the best privacy features.

a. Facebook

b. Twitter

c. LinkedIn

d. Thumbler

Results:

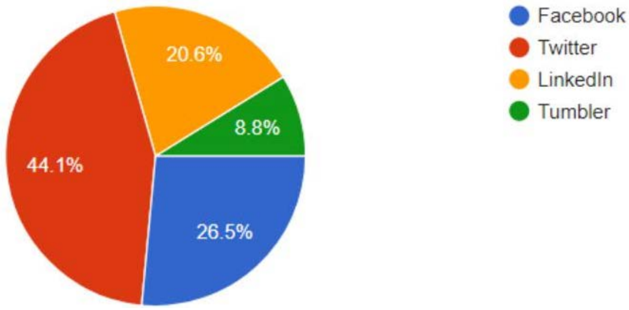


Fig. 2 Result of survey Q.2

Q.3) Have you ever affected by any attack on Online Social Network?

A. Yes

B. No

C. Not even know about that

Results:

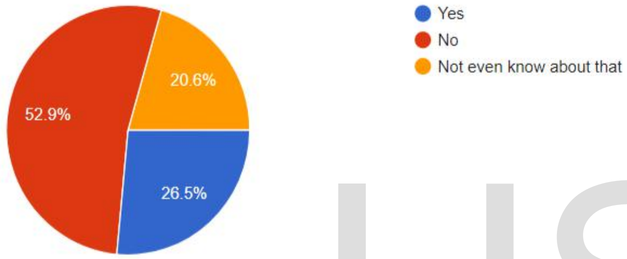


Fig. 3 Result of survey Q.3

Q.4) How many times you need to have change your passwords for Online Social Networks?

A. Never

B. Once in a Year

C. Once in a month Results:

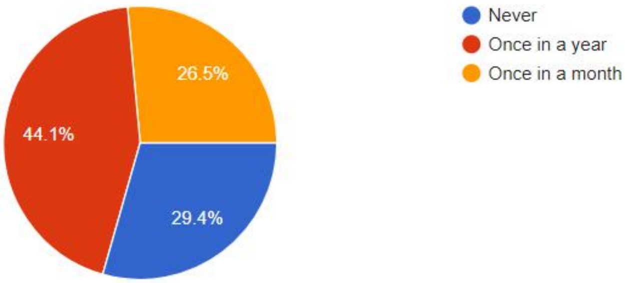


Fig. 4 Result of survey Q.4

Q.5) Have you ever hide your personal Information (Contact no, Address, Birthday etc) from the strangers?

A. Yes

B. No

Results:

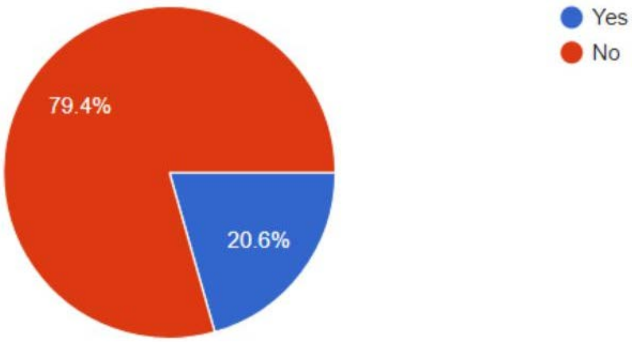


Fig. 5 Result of survey Q.5

Q.6) Are you satisfied with the current privacy features of the online social network you often login into:

A. Yes

B. No

Results:

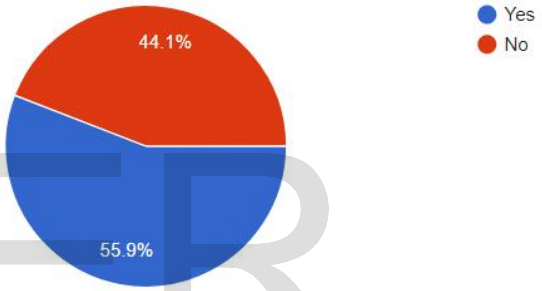


Fig. 6 Result of survey Q.6

Q.7) Do you trust in online social networks, in terms of sharing your relevant information (Posts, Pictures, Messages, Contact details) with any third party?

A. Yes

B. No

Results:

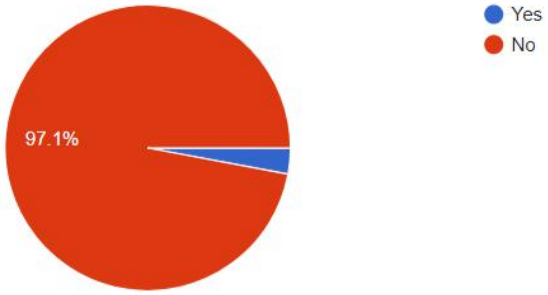


Fig. 7 Result of survey Q.7

Q.8) Have you ever decided to leave online social networks fearing the leakage of information and your privacy too?

A. Yes

B. No

C. I don’t care about that

Results:

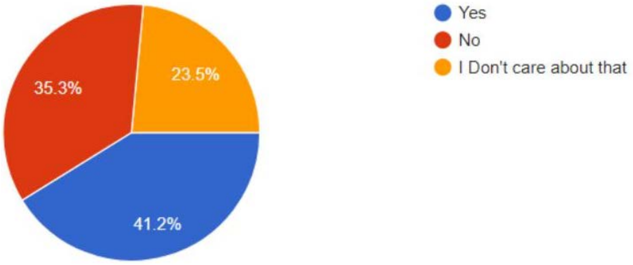


Fig. 8 Result of survey Q.8

Q.9) How much do you rate your information protection on SMs.

A. Excellent

B. Normal

C. Poor

D. Do not care about that Results:

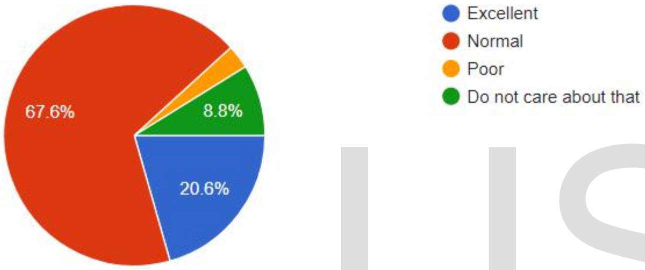


Fig. 9 Result of survey Q.9

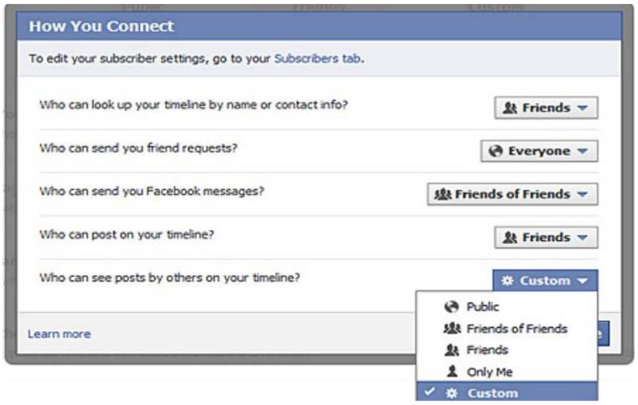
After compiling the results of our online survey, I have observed that most people do not bother to hide their sensitive information on SMs. Moreover, results show that a majority of people is satisfied with the current privacy features of SMs, yet they do not trust SMs in terms of sharing information openly on SM. People are also carefree about updating passwords and hiding sensitive information over SMs.

3 Proposed Solution

In the light of above results and the previous work done so far, I am going to suggest some generic solution in terms of SMs privacy and password policy. These are as follows:

1. For user Privacy awareness, an "Alerting Graph" (AG) must show to the user based on his/her privacy settings.

User should be preempted to change his/her password periodically on any social media.



How You Connect

To edit your subscriber settings, go to your Subscribers tab.

Who can look up your timeline by name or contact info? Friends

Who can send you friend requests? Everyone

Who can send you Facebook messages? Friends of Friends

Who can post on your timeline? Friends

Who can see posts by others on your timeline? Custom

Fig. 10 A sample of Privacy features/option of an SM

In the first step of showing an "AG" to the user, I have proposed a feature. This feature will analyze the current privacy settings of the user. The user can mark, for example, tagging option in Facebook as on or off. An "On Tagging" option has a positive value (say 1) and an "Off Tagging" option has some negative value (say -1). Based on the cumulative result of all possible privacy features of an SM, an "AG" will show the result. The interesting point is the graph will keep showing to the user during his/her online session. I also divide this graph into three categories, which form the basis of risk level associated with user regarding his or her privacy settings.

1. Critical Unsafe
2. Unsafe
3. Safe

A "Safe" level is the user's utmost adoption of the desired SM privacy settings. Moreover, an "Unsafe" level is the user's negligence to ignore some important privacy features. "Critical Unsafe" comes when the user has a minimum level of privacy settings for his or her SM.

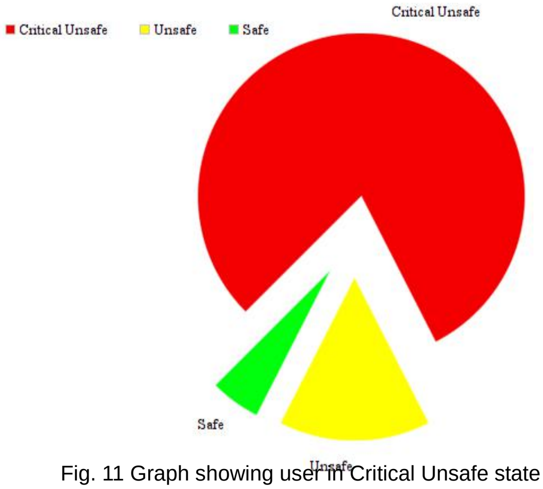


Fig. 11 Graph showing user in Critical Unsafe state

In Fig 11, a graph is shown to the user. This graph indicates that user has not applied all privacy settings to his or her own profile. The user after seeing this get aware about the alert level based on privacy.

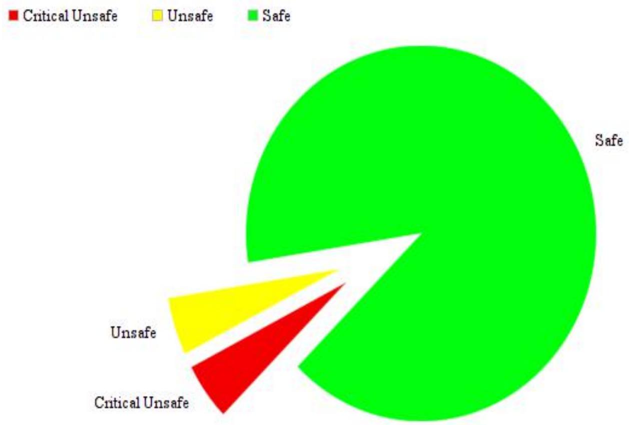


Fig. 12 Graph showing user in safe state

In the Fig 12, a graph shows that user have adopted maximum privacy features on SMs. User is marked safe in this case against any known privacy threats.

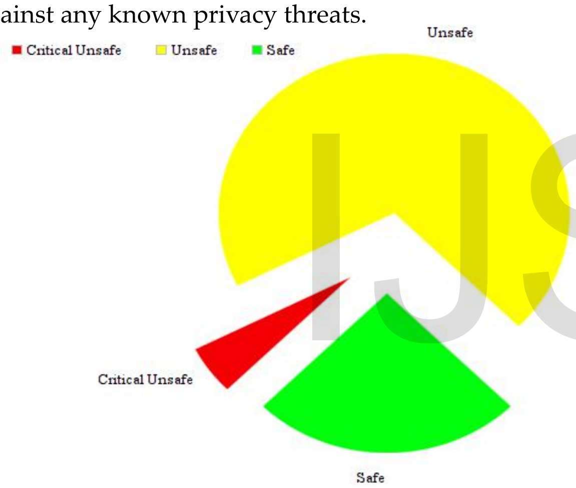


Fig. 13 Graph showing user in unsafe state

Fig. 13 shows a user profile's privacy level as "Unsafe". The reason is the missing of some important privacy features to be checked by the user.

In the second step of "Password change Policy". I have found that popular SMs such as Facebook, do not preempt user to change password periodically. Here, word periodically, means that this policy can be enforced once in a week, in a month or in a year depending upon the current demand of the SM vendor based on security.

3 Conclusion & Future Work

In our research, I have elaborated various important online privacy threats to SMs users. A survey has been conducted, in order to, analyze the user awareness about current privacy threats and its mitigating factors in modern SMs. In the end, I have proposed the solution of making a graphical representation for the user about current privacy settings. A periodical password changing policy has also been suggested to make user information more secure. In the future, I will work on user's privacy enhancement through integration of Short Message Service) SMS alerts (in case of illegitimate login attempt) and face recognition (for improving authentication in SMs).

References

[1] D. Gunatilaka, "A survey of privacy and security issues in social networks," Available: http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.html

[2] A.Yadav, S. Chakraverty, R. Sibal,"A survey of implicit trust on social networks," IEEE Green Computing and Internet of Things (ICGCIoT), 2015 Noida India.

[3] W. Gharibi, M. Shaabi, "Cyber threats in social networking websites," International Journal of Distributed and Parallel Systems (IJDPS) vol.3, No.1, January 2012.

[4] E. Franchi, A. Poggi, M. Tomaiuolo,"Information attacks on Online Social Networks," Journal of Information Technology Research (JITR) vol.7, No.3, pp. 54-71, July 2014.

[5] J. Becker, H. Chen," Measuring Privacy Risk in Online Social Networks," Computer Science Department, University of California, Available:
web.cs.ucdavis.edu/~hchen/paper/w2sp2009.pdf

[6] S. Mehmood, "Online Social Networks: Privacy Threats and Defenses," in Security and Privacy Preserving in Social Networks, pp. 47-71, Springer.

[7] M. Beye, A. Jeckmans, Z. Erkin, P. Hartel, R. Lagendijk, and Q. Tang,"Privacy in Online Social Networks," in Computational Social Networks: Security and Privacy, pp. 87-113, Springer.

[8] A. AL Hasib,"Threats of Online Social Networks,"International Journal of Computer Science and Network Security (IJCSNS), vol.9, No.11, pp. 288-93, 2009.

[9] B. Fu, D. O'Sullivan,"Trust management in Online Social Networks," University of Dublin, 2007.

[10] B. O'DEA, A. Campbell,"Online Social Networking and the experience of Cyber-Bullying," Sept 2012.

[11] Ed. Novak and Q. Li,"Security and Privacy in Online Social Networks-A Survey," Department of Computer Science, College of William and Marry, 2012, Available: cs.wm.edu.

[12] F. Persia and D. D'Auria,"A survey of Online Social Networks: Challenges and Opportunities," IEEE International Conference on Information Reuse and Integration, 2017.

[13] S. Kumar, Saravanakumar and Deepa,"On Privacy and Security in Social Media – A Comprehensive Study," International Conference on Information Security and Privacy (ICISP2015), 11-12 December 2015, Nagpur, India.