International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 8, Number 1 (2016), pp. 15-24
© International Research Publication House
http://www.irphouse.com

Survey on Online Social Networking Threats and Solutions

Smita Vishnu More and Madhumita Chatterjee

PIIT, Department of Computer Engineering, New Panvel, Mumbai University

Abstract

Online social Networking has become the most appreciated form of social surfing and browsing. Day by day it’s increasing and gaining fame through its attractive applications and social sites. The online surfing has become a part of entertainment. The valuable information such as people’s likings, disliking and interests are shared on several different OSN sites. Hence, OSN (Online social Networks) provides a platform to share the information on broader way to be in connection with different people. Accordingly there existing threats to these networking sites which need to dealt with an appropriate solutions in order to secure the private and social information of the respective candidate.

Keywords— online social networking, OSN, browsing, surfing

I. Introduction

Due to the vast use of social networking there are several social sites available like Facebook, Google+, LinkedIn, Sina Weibo, Twitter, and Tumblr wherein there are several active users surfing on daily basis. These networks do allow the users to access what the share on their profiles, which arises the question of whether the information shared is secured or not? Hence in order to secure the data and information shared solutions need to be derived.

Accordingly, the standard paper [1] specifies the existing types of threats which are broadly classified as:

(1) classic threats, which are privacy and security oriented threats that not only jeopardize OSN users but also Internet users not using social networks.

(2) modern threats which are unique types of threats using the OSN infrastructure to endanger user privacy and security.

(3) combination threats, combines various types of attacks which together exploit the contents.

(4) threats specifically targeting children are the latest emerging types of threats targeting teenagers and children.

Hence accordingly there are solutions and its appropriate mechanisms are derived which are specified as per the threats.

II. TAXONOMY OF ONLINE SOCIAL THREATS

A. Classic Threats

Classic Threats, [1] are the most traditional threats, these are famous threats which categorizes malware, spam, cross-site scripting (XSS) attacks, or phishing types of attacks. These threats use the user's personal information published in a social network to misuse their and their friend's content for malicious purposes.

- *Malware-* These are software which are malicious in nature, generally used to interrupt the computer operations, so that the user's crucial information can be accessed.
- *Phishing attacks-* These are one amongst the Social engineering threats which acquire the user-specific sensitive and private information by indulging an unknown third party.
- *Spammers-* These are users who uses the electronic message medium to send the fake messages like the advertisements to different users.
- *Cross-Site Scripting (XSS)* - This attack is an assault against web applications. The attacker exploits the trust of the client in the web application and causes them to run the malicious code which gathers the sensitive data.
- *Internet fraud-* These are cyber frauds, in which the access to the internet is provided to scam the advantage of the people.

B. Modern Threats

Modern Threats [1], are the most specific types of threats in the OSN environments. These threats aim the user's private information along with his/her friend's personal information.

- *Clickjacking* –This is a malicious technique in which users click on something different other than their contents, accordingly the intruding code is intruded.
- *De-Anonymization Attacks* – This attacks are implemented in order to uncover the user's real identity, by using the techniques like tracking cookies, network topology, and user group memberships.
- *Face Recognition* – These attacks are observed mainly on Social Network sites like Facebook, twitter etc. when the users uploads their information related to photos and pictures.
- *Fake Profiles* – These are also known as Sybils or socialbots, which are automatic or semi-automatic profiles that resemble the human behaviors in the OSNs. Hence the vital information can be used in a mislead manner.
- *Identity Clone Attacks* – Attackers here replicate the user's online identity in the same network or over the different networks in order to obtain the cloned

user's friends or known contacts to form a good relationship and mislead their information.

- *Information Leakage-* when OSN networkers actively share their private and sensitive data on their profiles and keep them available to everyone, than the data related to any of their content can be misled by the intruders.
- ➢ The Decomposed Theory of Planned Behavior [2] an extension to Theory of Planned Behavior comprises that the attitude towards OSN use, Social Influence and Perceived Behavioral Control.
- ➢ Accordingly, there are control measures also, which take care of Information leakages; those are Information Security Policy (ISP), Security Education, Training and Awareness (SETA), and other Preventive Security Systems.
- *Location Leakage* – Several people uses and share their location related information like the check in, venue etc. on the online social sites.
- *Socware* - These are malicious applications or socware webpages which attract the victims by offering false rewards to users in order to retrieve the sensitive information. The MyPageKeeper [3] is an application which is proposed to detect the socware related posts. The application works in 6 modules: - User authorization module, Crawling module, Feature extraction module, Classification module, Notification module and User feedback module.

C. ***Combination Threats***

These are the combination of modern and classic types of threats together, for example: the phishing and clickjacking attack can be used together to attract the victim to perform the malicious activity.

D. ***Threats targetting Children***

These are the emerging types of attacks [1] which specifically target the teenagers and children.

- *Online Predators* – These are also known as Internet pedophiles, who try to target children to remove their sensitive information for their malicious purposes, these can be harm from content, contact and conduct.
- *Risky Behaviors* – these comprises of the direct interaction with unknown people, through the chat sites of online social networks. The talks includes sexual explicit communications and sharing of private information like photos to them.
- *Cyberbullying* – These are cyber related crimes, generally referred as cyber abuses. In which the ragging or bullying types happens within the technological communication platforms, emails, chats, phones conversations, and OSNs, by an attacker.

III. TAXONOMY OF ONLINE SOCIAL NETWORK THREATS SOLUTIONS

In recent years, [1] online social network operators, academic researchers and security companies, have tried to deal with the below-mentioned threats by proposing a variety of solutions. These are some of the assured solutions which help the information to be secured.

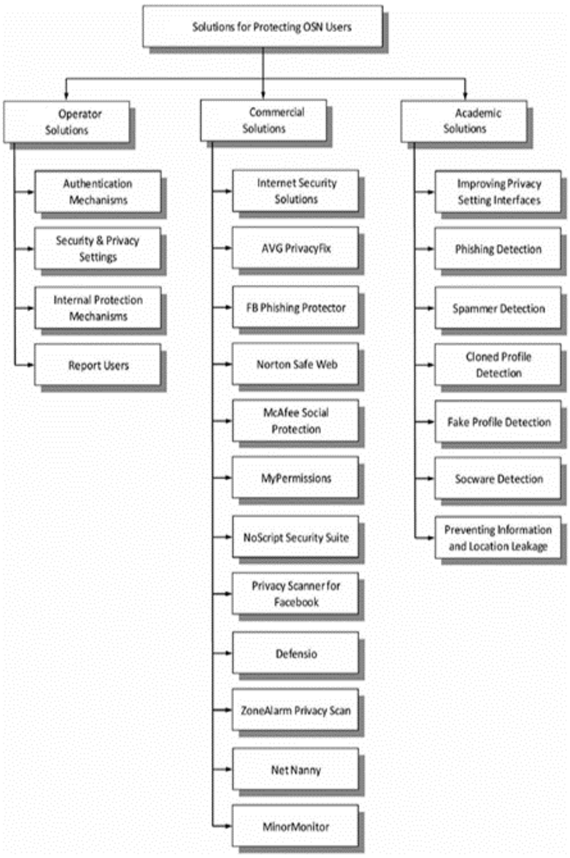


Figure 1:- Online Social Threats Solutions [1]

The above solutions are operated by OSN users to monitor their perspective contents on the online social networking sites.

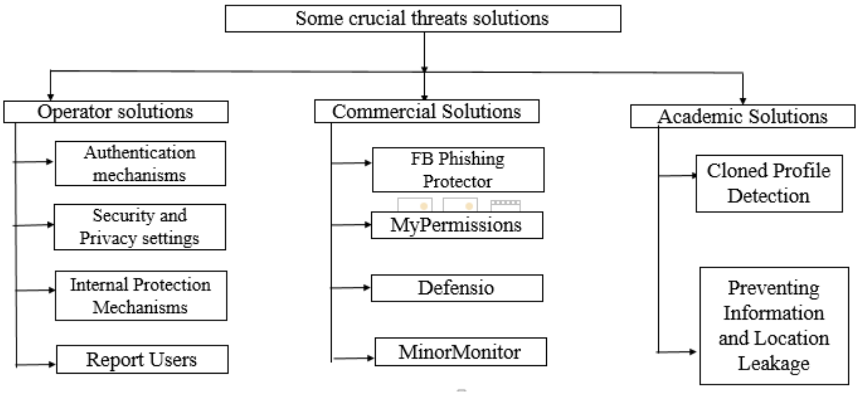

Some crucial threats solutions
Operator solutions
Authentication mechanisms
Security and Privacy settings
Internal Protection Mechanisms
Report Users
Commercial Solutions
FB Phishing Protector
MyPermissions
Defensio
MinorMonitor
Academic Solutions
Cloned Profile Detection
Preventing Information and Location Leakage

Figure 2:- User –Oriented OSN Threats Solutions

These are the Solutions which operates only on user access mechanisms. Among all the existing solutions some solutions need to be filtered from User access point of view in order to secure the upcoming threats and attacks. Hence the above filtered solutions are user –oriented to secure the online social contents.

A. ***Operator Solutions***

OSN operators secure their contents [1] through these types of solutions, wherein the operators access their private and secured data.

- *Authentication Mechanisms-* These solutions uses the concept of CAPTCHA, in the photos-of-friends identification, multi-factor authentication, and in some cases even requesting the operator to send a copy of his or her government issued ID. The Photo-based social authentication [4] is a mechanisms which includes the node and edge attributes. There are challenging questions and answers which are taken into consideration in this approach and accordingly the authentication is provided.
- *Security and Privacy Settings-* Several OSNs support different configurable user privacy data settings that helps the users to protect their personal data from other users or applications. According to the survey conducted by the respective authors there is a procedural approach of Security and Privacy Settings which consisted of survey of privacy attitude, [5] collection of intentions, identification of potential violations and confirmation of violations. Through these steps the data posted are surveyed and accordingly characterized.
- *Internal Protection Mechanisms –* Various OSNs secure their operators by providing the additional internal protection mechanisms to obstruct the attacks performed from the outside intruders, like the spammers, hackers and fake profile generators. Facebook, for example, protects its account members from suspicious attacks and information collecting by activating the Facebook Immune System (FIS) [1]. The FIS is described as an adversarial learning system that operates on real-time checks and classifications on read-and-write actions on Facebook's database.
- *Report Users-* The active OSN [1] surfers can sometimes mislead the shared information for their motives, hence such users can be reported and accordingly the review can be shared and taken into consideration. This prevents the teenage harassment if teenagers fid any suspicious activity on their social site.

B. ***Commercial solutions***

These are commercially [1] derived applications and web services which are used to secure the content on the online social networking sites.

- *FB Phishing Protector –* It is a Firefox add-on which warns Facebook users when an unknowing malicious activity is detected, like script-injection attempt. The add-on provides protection against various phishing attacks. The FB Phishing Protector add-on operates on blocking and detecting XSS (cross side script) injection in the Facebook content.

- *Mypermissions* – It's a web service technology which provides the users with essential links to the permission pages of many OSNs like the Facebook, Twitter, and LinkedIn. Hence the provided links help the users to view and revoke the assigned permissions, for the betterment of the privacy.
- *Defensio* – Defensio is Websense's web services which helps and protects the networkers from malicious threats such as links to malware. This services helps in preventing the information leakage of the published data in which it removes some words from the posts or even filter some comments. It [1] detects Spam content, Attempts to distribute malware, Links to undesirable content categories (e.g., adult material, gambling, etc.), Links to executable files and the inclusion of JavaScript or VBScript.
- *MinorMonitor* – MinorMonitor is a web service which helps parents to control their spouse's dashboard, their Facebook activities and online friends. Here the parents can be informed about questionable content that may have been revealed to their child, and they can identify overage friends in their child's Facebook friend's lists.

C. ***Academic solutions***

These types of solutions majorly [1] focuses on identifying the malicious users and applications, they provide cutting-edge insight while surfing with social networking threats. These solutions can be used by OSN operators to enhance the user's security and privacy.

- *Cloned Profile Detection* – these are used by sending the falsified or fake messages in order to cause harm to the original user. Accordingly, the victim on the other side has no idea of the existing fake profiles while having a communication.

In order to detect the cloned profile accounts [6] the prototype methodology is proposed which consist of the Information Distiller, Profile Hunter, and the Profile Verifier.

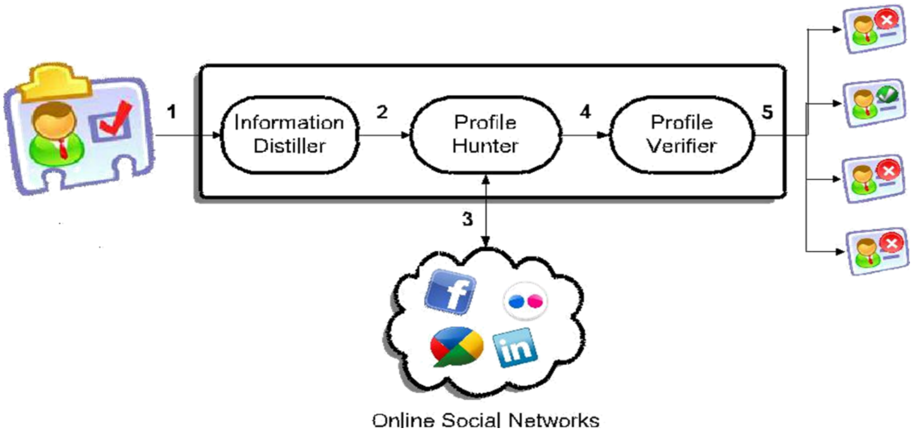


Figure 3:- Prototype model for cloned profile detection [6].

- *Preventing Information and Location Leakage-* These are secured mechanisms to prevent the information and location data from being misused.

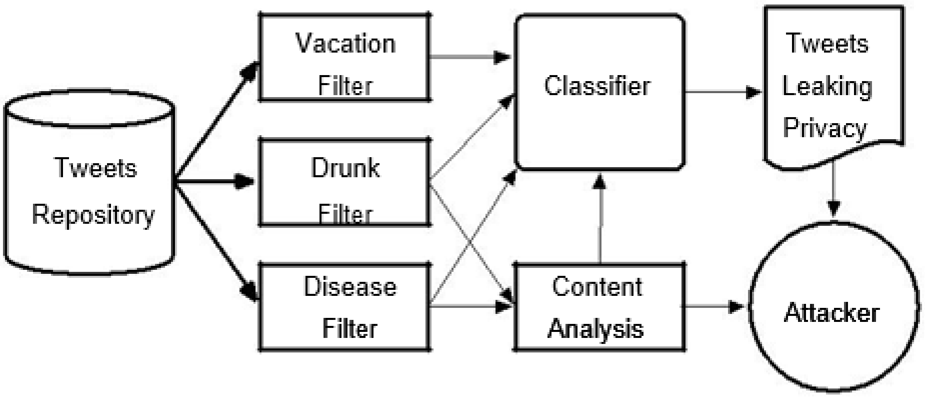


Figure 4; - Three Filter module [7]

The three filter modules [7] identify topical tweets which are based on keyword matching. These tweets are then filtered through classifiers to detect the sensitive tweets. The content analysis module features the types of privacy leaks for each of the three categories (vacation, drunk, and disease tweets)
This "guardian angel service" monitor networker's tweets and alert them for the potential privacy violations.

IV. NEED FOR ACCESS CONTROL MECHANISMS

From the above survey, it is observed that still the data posts on online social networking sites are not that secured hence, a major separate solution is required to resolve the existing threats.

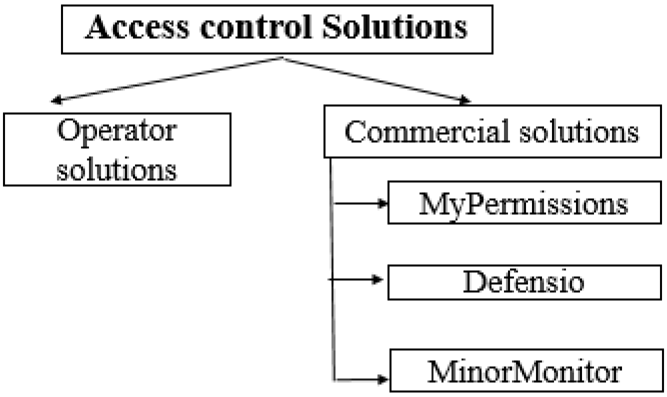


Figure 4- Taxonomy for Access Control Solutions

These are the extracted access solutions from the existing solutions, which is accessed only by the user. As, the need to emerging threats are increasing daily through advance in hacking and networking technologies; there is a need for more access-oriented approach to solve these threats hence; access control solutions are classified to resolve the problems. Hence, the taxonomy related to access control.

Importance of Access control-

Online social networks (OSNs) have analyses [8] large growth in recent years and become a saturation for hundreds of millions of OSN users. These OSNs offer the attractive means for digital social communications and information exchange, with this it also increases a number of security and privacy issues. Hence a restriction mechanism is needed to secure the data and provide an appropriate privacy by providing an access control over the social network. These issues give rise to the need of an access control mechanisms, as it has become the prime need to secure the online social networking surfing and browsing.

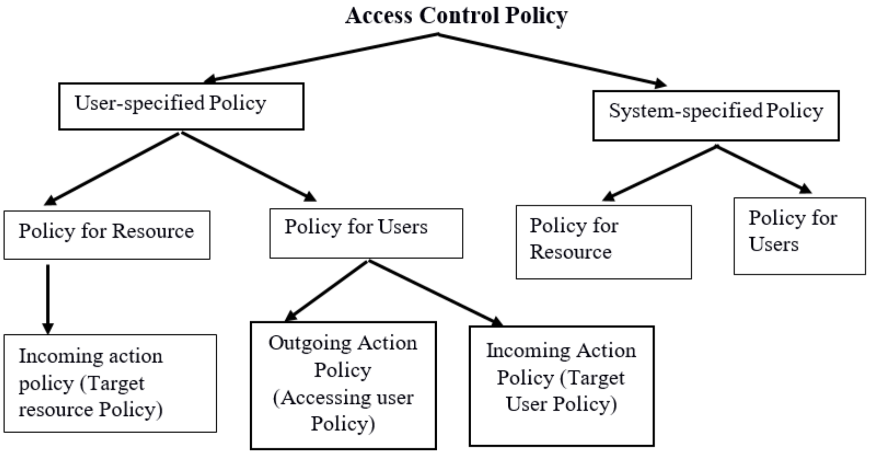

Access Control Policy
User-specified Policy
System-specified Policy
Policy for Resource
Policy for Users
Policy for Resource
Policy for Users
Incoming action policy (Target resource Policy)
Outgoing Action Policy (Accessing user Policy)
Incoming Action Policy (Target User Policy)

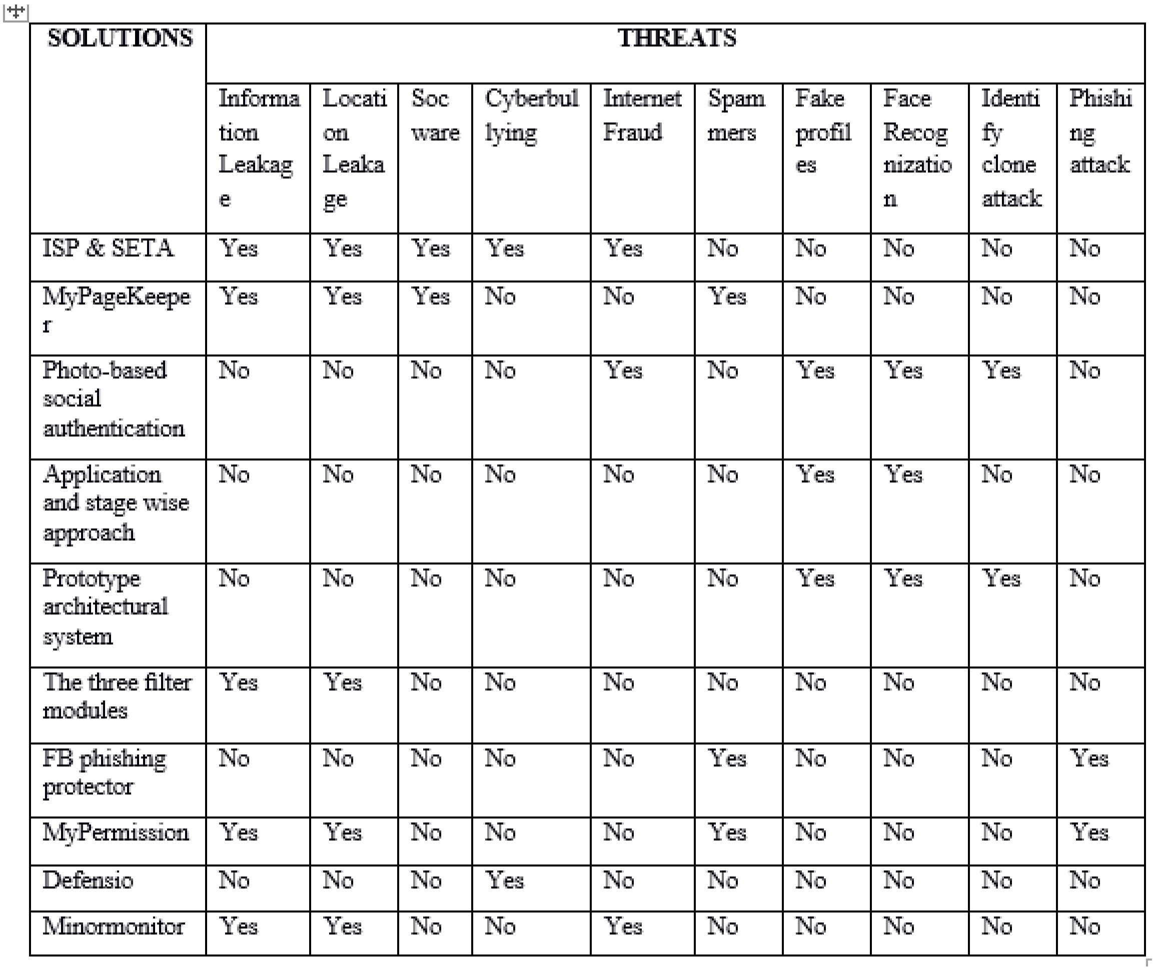
Figure 5- Existing Access Control Policies

V. COMPARATIVE ANALYSIS

These are some of the proposed and existing solutions which controls the developing threats.

Hence, from the above all survey the comparative analysis regarding the existing and commercial solutions is obtained which states that there is no such existing solution which can conquer over the online social networking threats. As these threats are huge in number every threats is managed by a different application or a solution mechanisms. For example: from the below analysis it can be found that the ISA and SETA known organization are able to find out the leakage related to information and location; socware cyberbulling and all but they are not able to detect the profile related threats. Similarly, from the commercial solutions the MyPermission application is able to keep a track on the attacks relying on spams, phishing and information leakages but not on the profile detections. Hence further work need to be done to secure any social profile from user perspective for which the access oriented approach can be implemented.

Table 1- Comparative Analysis of the existing and commercial solutions



SOLUTIONS	THREATS									
	Information Leakage	Location Leakage	Soc ware	Cyberbullying	Internet Fraud	Spammers	Fake profiles	Face Recognization	Identify clone attack	Phishing attack
ISP & SETA	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
MyPageKeeper	Yes	Yes	Yes	No	No	Yes	No	No	No	No
Photo-based social authentication	No	No	No	No	Yes	No	Yes	Yes	Yes	No
Application and stage wise approach	No	No	No	No	No	No	Yes	Yes	No	No
Prototype architectural system	No	No	No	No	No	No	Yes	Yes	Yes	No
The three filter modules	Yes	Yes	No	No	No	No	No	No	No	No
FB phishing protector	No	No	No	No	No	Yes	No	No	No	Yes
MyPermission	Yes	Yes	No	No	No	Yes	No	No	No	Yes
Defensio	No	No	No	Yes	No	No	No	No	No	No
Minormonitor	Yes	Yes	No	No	Yes	No	No	No	No	No

Acknowledgment

I remain immensely obliged to Dr. Madhumitta Chatterjee, H. O. D of COMPUTER DEPARTMENT, PIIT for providing me with the idea of this topic, and for her invaluable support in gathering resources for me either by way of information or computers also her guidance and supervision which made this seminar happen.

I would like to thank my college Pillai Institute of Information Technology, New Panvel and our principal Dr. R. I. K. Moorthy for the invaluable support.

I would like to say that is has indeed been a fulfilling experience for working out this seminar topic.

References

[1] Online Social Networks: Threats and Solutions, Michael Fire, Roy Goldschmidt, and Yuval Elovici, 2014

[2] Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats, Nurul Nuha Abdul Molok University of Melbourne Shanton Chang, 2010

[3] Efficient and Scalable Socware Detection in Online Social Networks, Md Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, Michalis Faloutsos, 2012

[4] New Directions in Social Authentication, Sakshi Jain ,Juan Lang, Neil Zhenqiang Gong, Dawn Song, Sreya Basuroy, Prateek Mittal, 2015

[5] The Failure of Online Social Network Privacy Settings, Michelle Madejskiy Maritza Johnson, Steven M. Bellovin, 2011

[6] Detecting Social Network Profile Cloning, Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, 2011

[7] New Directions in Social Authentication, Sakshi Jain ,Juan Lang, Neil Zhenqiang Gong, Dawn Song, Sreya Basuroy, Prateek Mittal, 2011

[8] An Access Control Model for Online Social Networks Using User-to-User Relationships, Yuan Cheng, Jaehong Park, and Ravi Sandhu, 2015