ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Review of Cyber Threats in Social Networking Websites

Amrinder Singh[#1] and Amardeep Singh[*2]

# Department of computer engineering, Punjabi university,Patiala
Patiala,Punjab,india

*Professor, Department of Computer Engineering, Punjabi University, Patiala
Patiala, Punjab,India

Abstract— with the advancement in technology, internet emerged as the crucial part of human life. While focussing on the internet, social networking is the major thing that gains attention. The use of social networking sites is very high compared to another usage of internet. The main reason is people's desire to interact and communicate people all around the globe. It is not just the way to communicate, but also an open door for a business promotion. But increased use of social networking websites has also promoted the cyber criminals for cyber crimes. Facebook, Instagram, Twitter, LinkedIn, Myspace, etc. are the social networking websites used by the users. While sharing information on these websites, people are unaware of the security issues. Cyber criminals exploit personal information and other confidential information of users for hacking their other accounts. Thus, privacy and security became the major concern in social networking websites. Existing internet security system and antivirus system are not effective enough to protect the user accounts against these security threats. These papers aim to review and identify various cyber security threat in social networking websites. Also, it focuses on proposed some solutions to help people how to tackle the cyber security threats associated with the social networking websites.

Index Terms— Social Networking Sites, Security, Threats,

I. INTRODUCTION

Social networking sites or SNSs are online applications that allow people to communicate with each other by sharing text, images, profiles, files and other things with each other's [3]. A social network can be defined as a structure that consists of individuals or businesses, which are called nodes and these nodes are connected with each other because of friendship, relationship, knowledge, mutual interest, exchange of information and so on [1]. Social networking sites allow users to share views, images with the other people who are in their friend list. With the help of these locations, one can make their profiles, make new friends, delete or block existing friends and perform many other activities. Due to the advancement in the automation or Internet usage, almost all the people have started using the social networking sites for communicating with their relatives, friends, partners, family members, etc. [6]. These social networking sites allow people at remote locations to interact with each other very quickly and at negligible cost. All social networking sites enable users to register on them before using these sites. The registration is free for all the users. There are many social networking sites [7].

Following are the main social networking sites that are popular among the users.

1. Facebook

It is one of the commonly used social network sites, using this site one can communicate with others, share thoughts or views, make friends, upload photos or tag photos. One can also make groups of people sharing a common interest, can create pages, like pages, and join groups and much more [5].

2. Twitter

It is also leading social networking site in which one can post 140 characters tweet with other users. One can make followers on the Twitter and follow the others to whom he/she wants to follow. This helps one to get in touch with what's happening in the world [4].

3. LinkedIn

This social networking site helps business people to share their work related information with each other and with their clients [12].

Figure 1: Social Networking Sites

4. Orkut

This is the service provided by Google, and with the aid of this site one can connect with people located at remote places and can also change themes from a set of themes provided by the site [13].

5. YouTube

YouTube a video social networking site, which is searched just like the Google. YouTube includes the video of different types of various subjects like it includes videos on study topics, creativity topics, health related issues, etc. Anyone can like, view, share, comment the videos posted by anyone. It is one of the social networking site, which also helps the user to earn money through uploading videos [8].

Apart from these, there exist many other social networking sites like flicker, Classmates, Instagram, Snapchat and various others.

II. CYBER SECURITY ISSUES

Cyber security issues can be divided into three categories that are:

Cyber Crime: A cybercrime is a crime that is conducted by individuals either alone or in groups. This crime is performed with the intention of getting money, causing disruption, or obtaining private or valuable data. These crimes can be conducted for getting the credit/ debit card information, impairing the website operations and intellectual property [9].

Cyber War: A cyber war is undertaking by a nation for espionage against another country for causing disruption or extraction of data. Advance persistent threats are involved in these cyber wars.

Cyber Terror: A cyber terror is caused by an organization that is working independently for the purpose of performing terrorist activities through cyberspace.

III. CYBER THREATS IN SNS

These risks can be divided into two kinds of threats that are [1]:

Traditional network related threats: These threats are related to either with the security of the people or with the safety of the data that is stored in the systems. There are some individuals who are active on social media sites networks and thus having a huge amount of data of various users. Thus these systems are prone to threats like identity theft, cyber bullying, stalking, phishing attacks and many others.

Privacy Related Threats: These threats can be faced due to the publishing of information on the social networking sites. Users put a vast amount of personal information while creating profiles such as addresses, phone numbers, and birth data and so on. Hackers can use this data for social engineering for getting the benefits from personal information.

IV. PRIVACY PRESERVING TECHNIQUES

Privacy can be defined as the control of user over his/her information. This information cannot be used or disclosed without the owner's information. It is the right of the proprietor to decide whether to disclose his/her information or not. Privacy of the personal information over the social networking sites has become a significant concern that needs to be paid attention. To protect or preserve the private information, privacy preserving techniques can be used such as given below:

K-Anonymity: This is a method of constructing and then evaluating the algorithms and systems that disclose information such as the published information will limit the information that can be revealed about the entities properties. For example, if one is having the information the gender and zip code and want to identify a person then there exist k individuals that will match the gender and zip code. K- Anonymity uses the quasi-identifier for controlling the disclosure of information. These can lead to attacks like homogeneity attack, does not handle attribute disclosure attack and face background knowledge attacks.

L-Diversity: This technique diversifies the sensitive attributes and lead to prevention of homogeneity attacks, background knowledge attacks and prevent sensitive attribute disclosure. But this also faces problems like skew and similarity attack [3].

T-Closeness: The problems of the L-diversity and K-anonymity techniques are solved by the t closeness method. This method considers the semantic gap between the sensitive attributes and thus prevents the previous techniques attacks [4].

Other methods: an integrated algorithm that consists the features of both k-anonymity and l-diversity is also introduced for preserving the private data. And this lead to increase the level of privacy of social networking users by anonymizing and diversifying the disclosed information.

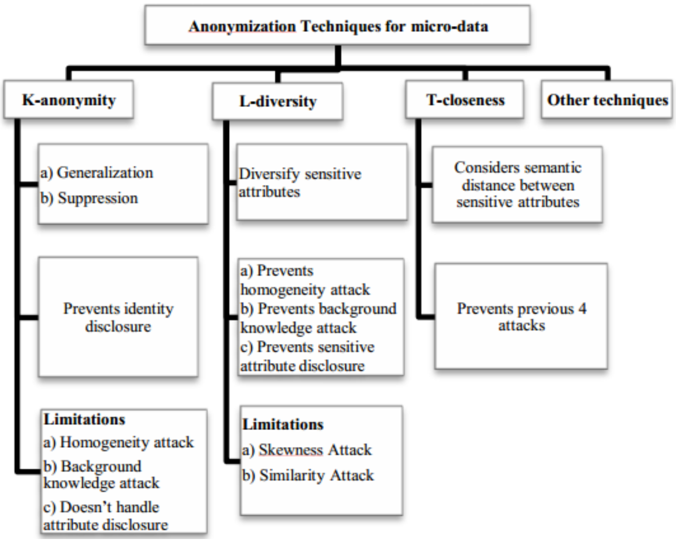
Anonymization Techniques for micro-data
K-anonymity
L-diversity
T-closeness
Other techniques
a) Generalization
b) Suppression
Prevents identity disclosure
Limitations
a) Homogeneity attack
b) Background knowledge attack
c) Doesn't handle attribute disclosure
Diversify sensitive attributes
a) Prevents homogeneity attack
b) Prevents background knowledge attack
c) Prevents sensitive attribute disclosure
Limitations
a) Skewness Attack
b) Similarity Attack
Considers semantic distance between sensitive attributes
Prevents previous 4 attacks

Figure 2: Privacy preserving techniques [4]

V. SOLUTIONS

For securing information on the social networking sites, following guidelines can be followed [11].

1. Limit the amount of information that you disclose on the social networking sites.
2. Don't make friends who are strange to you.
3. Don't always believe information that is posted online as it can be misleading information.
4. Customize your settings according to your needs. Don't let it by default.
5. Avoid the use of such application that you were finding suspicious and also allow applications to access the limited information of yours.

6. Strong passwords should be employed so that no one else can login to your account and exploits your personal information [8].
7. Antivirus software should be used for dealing with a virus that may come from the internet due to the usage of social networking sites and can lead to stealing or deleting your valuable data from your computer.
8. Try to make sure whether your network is secure or not. Try to make your system secure, because the unsecured network can lead to loss of your personal data [15].
9. Don't select the same password for all social accounts because if when site's password is compromised then there full chances that your all accounts information will be hijacked.
10. Choose the suitable authentication scheme so none can hack one's details. Two-factor authentication can serve as a good authentication system [14].

VI. LITERATURE REVIEW

W. Gharibi and M. Shaabi, [2015] described various social networking sites for examining the cyber threats on social networking sites. In the paper, the detail about some users on social networking sites like Myspace, Flickr, Facebook, Classmates and so on was discussed. Also, social networking websites taxonomy, their security and privacy issues were also highlighted. Anti-threat strategies were suggested for dealing with privacy and safety risks faced by the social networking sites. The development of the tools that will able to deal with Trojan horses, spies, attackers, viruses and other malware were suggested. Thus study visualized the future trends for cyber threats [1].

R. Jabe and A. Alam, [2016] conducted a survey for finding the users' perception of privacy and security issues that occur on social networking sites. The research particularly focused on the one of the primary social networking site Facebook. The study not only discussed the perception of users' regarding privacy and security issues but also presented the notion of improvement in the default privacy setting offered by the Facebook so that reduction and prevention in the cyber crimes could be achieved. It was found that users were not aware of the privacy setting and did not want to change the default settings. Thus it was concluded that users should be aware of the default settings and should change these so that they would not become the victim of security breaches. Moreover, Facebook should also pay attention towards the safety settings for preventing users' from any security breaches [2].

V. L. Yisa et al. [2016] examined the usage of social networking sites along with the experienced risks that were faced by the university students of North Central Nigeria. Investigation of three tertiary institutions in the North Central Nigeria was conducted. Questionnaires were used for data collection. The people that were participated for responding to the surveys were full-time undergraduate students, males, and students within the age of 24 to 29. Findings obtained indicated that the use of online social networking sites was done by most users' for interacting with their friends. Users' also uploaded the information regarding their locations on the social networking sites. It was revealed that use of the social sites also affected some users' positively whereas some had to experience various risks and various attacks [3].

A. Singh, et al. [2014] discussed the privacy preserving techniques that were required to be developed and implemented to prevent users' from experiencing security risk or breaches. As the social networking sites had gained popularity among almost all users, and risks and safety issues were increasing day by day. Thus research described various kind of privacy breaches, challenges that occurred while publishing data on these sites. Along with this, the techniques like L-diversity integrated K-anonymity L-diversity, and K-anonymity were also described. But these techniques were not able to prevent security breaches. Therefore the study suggested improvement in the techniques to provide privacy preservation that includes no loss of data and better utilization of published data [4].

M. Fire, et al. [2014] presented the detail on the various kinds of privacy and security risks that were occurred on the social networking sites along with the solutions that can prevent these threats or breaches. Examples of different experienced threats were provided, and the existing solutions were discussed for maintaining the privacy of users'. The study concluded that the techniques or solutions were not antidotes for managing the security. Thus users' had to aware about what kind of things they were posting online. The simple recommendations for improving safety and privacy were also presented along with a suggestion for further research directions [5].

Y. Najaflou, et al. [2013] reviewed the safety challenges and solutions of mobile social networks. The discussion was presented from the perspective of security, trust, and privacy. Further, the trust, safety, and confidentiality were categorized into other categories for proper analysis. The broad investigation on each type was conducted properly to review specific issues and solutions. In the end, the study concluded significant research problems and research directions for future [6].

D. Hiatt, Y. B. Choi, [2016] discussed the role of privacy and security in the social networking sites. The introduction to the concept of social networking, risks that were experienced due to the usage of social sites was discussed. The relation of privacy and security was also described. The solutions for maintaining safety and privacy were also provided. Thus it was revealed through the study that both users and organizations should pay attention to improving safety and privacy on the social networking sites [7].

L.S.Y. Dehigaspege, et al. [2016] presented a highly secure authentication method for prevention of cyber threats on the social networking sites. The research showed the use of an algorithm that uses a voice recognition system for the users that allows users to login based on their voice. The location identification system, the CAPTCHA program were also included in the algorithm, so that distinction among the bots and human users was possible. Thus study provided the secure authentication algorithm for defending the security attacks occurred on social networking sites [8].

M. L. Prasanthi, T. A. S. K. Ishwarya, [2015] discussed the cyber-crimes and also about their prevention and detection techniques. As cyber-crime was increasing day by day and criminals were becoming more intelligent and also targeting users from private and public organizations. Thus it became necessary that Defense techniques will be made stronger for defending this kind of cyber-attacks. Therefore the authors provided the detail about the case studies of cyber-crimes and various methods for detection and prevention of these crimes like configuration checking tools, anomaly detection technologies, and honeypots were discussed. Thus the research provided the knowledge about prevention and detection of cyber-crimes [9].

R. Chouhan [2015] presented an analytical approach about trends used in the cyber-crimes. The paper shed light on the different methods of committing the cyber-crimes, who commits these and the reason behind committing the cyber-crimes. Findings obtained from the study revealed that India had become the favorite place for cyber criminals for performing cyber-attacks and cyber-crimes revenue had increased. Thus improvement will be required so that safety and security can be achieved [10].

A. Kumar, et al. [2013] discussed the social networking sites and their security issues in detail. The architecture for secure exchange of the data was also presented in the research. The security issues and attacking scenario were discussed. For defending these attacking situations, the prevention strategies were advised like don't post anything which would put you in trouble, be careful about adding strangers as your friends, knowledge about the ways in which criminals fooled the users and so on. Thus study helped to have knowledge about the ways in which users can get rid of the attacks [11].

S. D. Trivedi, et al. [2016] presented an analytical study of cyber threats on social networking sites. The paper discussed the history of the existence of social networking sites, their categories. Also, the threats that could be faced were examined along with the prevention measures that can be followed by defending and preventing the cyber-crimes. Thus study concluded that although social networking sites were helping as an interaction tool, it can also lead to attacks of a different kind [12].

R. Chandramouli [2011] discussed the emerging threats that were experienced on the social networking sites. Cyber threats were emerging with a rapid speed such that it became possible for an average user to use the social site for malicious purposes. It had become tough for governments and organizations to find methods for detecting, identifying and preventing such kind of threats. Therefore, the knowledge about challenges from technologies to policies was provided through this paper [13].

A. Bendovschi [2015] presented the cyber threats trends, patterns, and countermeasures. As the rate of cyber threats was increasing day by day, thus there was a requirement for improvement in the social sites for defending the attacks. The author suggested that global awareness was a need, a set of laws and regulation about data privacy and theft in each region or state, authorities should think about the safety of citizens, and it was a responsibility of an individual for prevention of thefts or threats. Thus study focused on the universal awareness to handle the crimes [14].

M. A. Carter, [2013] presented the perspectives of undergraduate students' of third party observers witnessing cyberbullying on social sites. Cyberbullying was going beyond its boundaries, and a high percentage of cyber bullying was found unreported. It was found that one-quarter of cyberbullying occurred because of the presence of third-party observers. As the minimal research has been conducted for analyzing the third party observers witnessing cyberbullying, thus the study focused on identifying the role of third party observers in curbing the cyber bullying [15].

VII. FINDINGS

This section provides insight into the findings of the research.

Year	Researchers	Algorithm/Method	Results/ Solution
2012	W. Ghari and M. Shaabi [1]	Analyzed various cyber security threats and classified their types.	The study suggests various anti-threats strategies.
2016	R. Jabee and M. Afshar [2]	Studied the requirement to improve the default privacy settings in Facebook.	The research suggests that the users must be more aware and concerned regarding the default security settings in Facebook.
2016	V. L. Yisa, O. Osho, and I. Soje [3]	Measured the impact of the Online Social Networks (OSNs) on the performance of the students.	The result of the study represents that there is the positive effect of the OSNs on the student performance. Also, various students experienced security risks while using these online social networks.
2014	A. Singh, D. Bansal, and S. Sofat [4]	explored various privacy preservings techniques such as L-diversity, K-anonymity and integrated K-anonymity L-diversity	The result of the study shows that the data preserving techniques analyzed in this research are not effective enough to prevent the data loss and significant improvement is required in these techniques.
2014	M. Fire, R. Goldschmidt and Y. Elovici [5]	Thoroughly reviewed the different privacy and security risks and presented existing security solutions to prevent the personal information loss.	Suggested solutions are effective for the ONS users to improve privacy and security issues while using these platforms.
2015	Y. Najaflou, B. Jedari, F. Xia, L. T.	The study provides a consistent categorization on different security	The privacy engages provinces were categorized into three classes including private matching, fairness

	Yang and M. S. Obaidat [6]	challenges and explores various solution in the Mobile Social Networks.	encouragement, and obfuscation.
2016	D. Hiatt and Y. B. [7]	The issue of security in social networking sites and how it relates to the privacy is described in this paper.	Provide various significant steps to improve the security and privacy on social networking sites.
2016	L. Dehigaspege, U. Hamy, H. Shehan and D. Dhammearatchi [8]	Proposed voice recognition technique along with location identification and CAPTCHA's mechanism to defend the cyber security attack	The proposed method is effective to defend the cyber security attack and successfully identify the location from where the social networking account is accessed.
2015	M. Prasanthi, [9]	The study described various regulation acts which are imposed against the cybercrime.	Recommended various safety tips to use social networking sites.
2015	R. Chouhan [10]	Introduced an analytical approach to define various trends utilized in cyber crime	Suggested various techniques to combat the cyber security issues including technological perspective, strategic perspective, and legal perspective.

VIII.CONCLUSION

Social Networking Sites (SNS) offer various advanced ways to communicate and interact with people around the globe. People can easily reach their relatives and friends through Social networking sites. Though there are numerous benefits of social networking sites, they also raise various challenges for the users; more specifically the security and privacy issues. These security and privacy threats are opportunities for the attacks, viruses and other malicious actors. Thus, there is a requirement to improve the security solution techniques. In this paper, we reviewed various social networking sites, their security and privacy issues. We reviewed the research that already has been done to prevent the loss of data and breaches because of the security and privacy threats. Also, the paper suggests various steps to the users for improving the security while using the social networking sites.

REFERENCES

[1] W. Ghari and M. Shaabi "Cyber Threats in Social Networking Websites," International Journal of Distributed and Parallel Systems, vol. 3, no. 1, pp. 119-126, 2012.

[2] R. Jabee and M. Afshar, "Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)," International Journal of Computer Applications, vol. 144, no. 3, pp. 36-40, 2016.

[3] V. L. Yisa, O. Osho, and I. Soje, “Online Social Networks: A Survey of Usage and Risks Experience among University Students in North-Central Nigeria,” International Conference on Information and Communication Technology and Its Applications, pp. 129–133, Nov. 2016.

[4] A. Singh, D. Bansal, and S. Sofat, "Privacy Preserving Techniques in Social Networks Data Publishing - A Review," *International Journal of Computer Applications*, vol. 87, no. 15, pp. 9-14, 2014.

[5] M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2019-2036, 2014.

[6] Y. Najaflou, B. Jedari, F. Xia, L. T. Yang and M. S. Obaidat, "Safety Challenges and Solutions in Mobile Social Networks," in *IEEE Systems Journal*, vol. 9, no. 3, pp. 834-854, Sept. 2015.

[7] D. Hiatt and Y. B., "Role of Security in Social Networking," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 2, 2016.

[8] L. Dehigaspege, U. Hamy, H. Shehan and D. Dhammearatchi, "Secure Authentication: Defending Social Networks from Cyber Attacks Using Voice Recognition," *International Journal of Scientific and Research Publications*, vol. 6, no. 10, pp. 120-126, 2016.

[9] M. Prasanthi, "Cyber Crime: Prevention & Detection," *International Journal of Advanced Research in Computer and Communication Engineering,* Vol. 4, Issue 3, pp. 45-48, 2015.

[10] R. Chouhan, "Cyber Crime: A Changing Threat Scenario in the State Of Art," *International Journal of Engineering Research and General Science*, vol. 3, no. 2, pp. 1206-1216, 2015.

[11] A. Kumar, S. Kumar Gupta, S. Sinha and A. Kumar Rai, "Social Networking Sites and Their Security Issues," *International Journal of Scientific and Research Publications*, vol. 3, no. 4, pp. 1-5, 2013.

[12] S. D. Trivedi, M. Chandani, M. Tosal and T. Pandya, "ANALYTICAL STUDY OF CYBER THREATS IN SOCIAL NETWORKING," *International Conference on Computer Science Networks and Information Technology*, vol. 3, no. 2, pp. 32-36, 2016.

[13] R. Chandramouli, "Emerging social media threats: Technology and policy perspectives," *2011 Second Worldwide Cybersecurity Summit (WCS)*, London, 2011, pp. 1-4.

[14] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24-31, 2015.

[15] M. Carter, "Third Party Observers Witnessing Cyber Bullying on Social Media Sites," *Procedia - Social and Behavioral Sciences*, vol. 84, pp. 1296-1309, 2013.