International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 1 ǁ 2021 ǁ PP. 13-18

Evaluation of Cyber Threats in Social Networking Websites

REENA RAVEENDRAN
Research Scholar
University of Kerala

Abstract: — *with the development in era, internet emerged because the important a part of human life. Even as focussing on the net, social networking is the major element that gains attention. Using social networking websites could be very excessive compared to some other utilization of net. The main purpose is human beings's desire to engage and talk humans all over the globe. It isn't simply the manner to speak, however additionally an open door for an enterprise advertising. But multiplied use of social networking websites has additionally promoted the cyber criminals for cyber crimes. Fb, Instagram, Twitter, LinkedIn, MySpace, etc. are the social networking web sites utilized by the users. Even as sharing facts on those web sites, humans are ignorant of the security problems. Cyber criminals take benefit of personal facts and unique private records of users for hacking their extraordinary debts. Therefore, privacy and protection have become the major concern in social networking net websites. Existing internet protection gadget and antivirus machine are not powerful enough to guard the user debts in the direction of these protection threats. Those papers reason to study and pick out various cyber safety threats in social networking websites additionally, it makes a speciality of proposed some solutions to help people a manner to tackle the cyber safety threats related to the social networking net websites.*

Index phrases—*Social Networking websites, safety, Threats,*

Date of Submission: 07-01-2021 Date of acceptance: 22-01-2021

I. INTRODUCTION

Social networking sites or SNSs are on line applications that allow people to speak with every special through sharing textual content, pics, profiles, files and various things with every deferent's [3]. A social network can be described as a shape that includes individuals or groups, which are called nodes and people nodes are related with every different because of friendship, courting, know-how, mutual interest, change of statistics and so on [1]. Social networking web sites permit users to percentage views, snap shots with the alternative folks that are in their pal listing. With the help of these places, one may want to make their profiles, make new pals, delete or block present pals and carry out many exclusive sports. Due to the development in the automation or internet usage, nearly all of the people have started out the usage of the social networking websites for communicating with their cherished ones, buddies, partners, family members, and so forth. [6]. these social networking websites permit human beings at some distance flung places to engage with every different in no time and at negligible cost. All social networking internet sites allow customers to sign in on them in advance than the use of the ones internet websites. The registration is free for all of the clients. There are numerous social networking net websites [7]. Following are the precept social networking web sites that are popular many of the users.

1. Facebook
It is one of the typically used social community web sites, the usage of this website you'll be in a position to talk with others, percent mind or views, make friends, add pix or tag pix. One can also make businesses of people sharing a not unusual interest, can create pages, like pages, and be a part of companies and plenty greater [5].

2. Twitter
It's additionally main social networking internet page in which it is easy to put up a hundred and forty characters tweet with other clients. You could make followers on the Twitter and observe the others to whom he/she wants to observe. This permits one to get in contact with what's occurring in the global [4].

3. LinkedIn
This social networking website on-line facilitates organization people to share their art work related data with each different and with their clients [12].

4. Orkut
This is the service provided by using manner of Google, and with the useful resource of this internet site you may connect with people placed at distant places and also can exchange issues from a fixed of subject matters furnished through the web page [13].

5 YouTube
YouTube a video social networking internet site, which is searched similar to the Google. YouTube consists of the video of numerous types of various subjects find it irresistible includes movies on look at topics, creativity topics, health associated issues, and so forth. Genuinely everybody can like, view, percentage, observation the movies published with the aid of all of us. It is one of the social networking web pages, which moreover allows the customer to earn cash via importing motion pictures [8].
Other than these, there exist many other social networking web sites like flicker, Classmates, Instagram, Snap chat and diverse others.

II. CYBER SAFETY TROUBLES

Cyber safety problems can be divided into 3 classes that are:

Cyber Crime: A cybercrime is a crime this is conducted via individuals either on my own or in organizations. This crime is carried out with the purpose of having cash, inflicting disruption, or acquiring non-public or treasured information. These crimes may be performed for getting the credit score/ debit card facts, impairing the website operations and intellectual belongings [9].

Cyber war: A cyber battle is mission by means of a state for espionage towards any other country for inflicting disruption or extraction of facts. Enhance persistent threats are concerned in these cyber wars.

Cyber Terror: A cyber terror is due to a commercial enterprise employer this is running independently for the purpose of appearing terrorist sports activities via our on-line world.

III. CYBER THREATS IN SNS

These risks can be divided into two kinds of threats which might be [1]:

Traditional community associated threats: Those threats are related to both with the safety of the humans or with the protection of the statistics that is saved inside the systems. There are some people who are active on social media web sites networks and as a result having a huge quantity of information of numerous customers. For this reason those systems are at risk of threats like identification theft, cyber bullying, stalking, phishing attacks and lots of others.

Privateness associated Threats: Those threats can be faced because of the publishing of data at the social networking web sites. Users put a large amount of private records at the same time as creating profiles including addresses, cell phone numbers, and birth information and so on. Hackers can use this record for social engineering for getting the advantages from private records.

IV. PRIVACY MAINTAINING STRATEGIES

Privacy can be described because the manipulate of consumer over his/her facts. This record can't be used or disclosed without the proprietor’s facts. it's miles the proper of the proprietor to determine whether or not to disclose his/her data or no longer. Privacy of the personal data over the social networking sites has end up a good sized problem that desires to be paid attention. To protect or hold the non-public statistics, privateness preserving strategies may be used which includes given under:

k-Anonymity: that is a way of constructing after which evaluating the algorithms and structures that expose records along with the posted statistics will restriction the records that can be discovered about the

entities houses. as an instance, if one is having the records the gender and zip code and need to pick out someone then there exist k individuals in an effort to fit the gender and zip code. k- Anonymity makes use of the quasi-identifier for controlling the disclosure of facts. Those can result in assaults like homogeneity assault, does not cope with characteristic disclosure assault and face history know-how attacks.

L-variety: This technique diversifies the touchy attributes and result in prevention of homogeneity attacks, background know-how assaults and save you touchy attribute disclosure. but this additionally faces issues like skew and similarity assault [3].

T-Closeness: The troubles of the L-diversity and okay-anonymity strategies are solved through the t closeness technique. This technique considers the semantic hole among the touchy attributes and as a result prevents the previous techniques assaults [4].

Different strategies: an included set of rules that is composed the capabilities of both ok-anonymity and l-range is also introduced for preserving the non-public information. And this result in boom the level of privateness of social networking customers through anonymizing and diversifying the disclosed information.

V. SOLUTIONS

For securing statistics at the social networking web sites, following tips can be followed [11].

1. Restrict the quantity of records which you divulge at the social networking websites.
2. Don't make friends who're strange to you.
3. Don't constantly consider records that are posted on line as it could be deceptive statistics.
4. Personalize your settings according to your wishes. Don't permit it by way of default.
5. Keep away from the use of such utility that you had been locating suspicious and also permit programs to access the restricted information of yours.
6. Strong passwords have to be hired so that no one else can login for your account and exploits your private records [8].
7. Antivirus software program ought to be used for coping with a plague which can come from the internet due to the use of social networking websites and may lead to stealing or deleting your valuable statistics from your computer.
8. Try to make certain whether or not your network is secure or now not. Attempt to make your system cozy, due to the fact the unsecured community can lead to lack of your private statistics [15].
9. Don't pick out the identical password for all social accounts because if whilst web site's password is compromised then there full probabilities that your all accounts statistics can be hijacked.
10. Pick out an appropriate authentication scheme so none can hack one's info. -component authentication can function a very good authentication system [14].

VI. LITERATURE OVERVIEW

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 kinds 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].

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 was 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

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 favourite 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 cyber bullying on social sites. Cyber bullying was going beyond its boundaries, and a high percentage of cyber bullying was found unreported. It was found that one-quarter of cyber bullying occurred because of the presence of third-party observers. As the minimal research has been conducted for analyzing the third party observers witnessing cyber bullying, thus the study focused on identifying the role of third party observers in curbing the cyber bullying [15].

VII. FINDINGS

This segment offers perception into the findings of the studies.

YEAR	RESEARCHERS	SET OF RULES/APPROACH	END RESULT/SOLUTION
2012	W. Ghari and M. Shaabi [1]	Analyzed numerous cyber security threats and labeled their types.	The study shows numerous anti-threats techniques.
2016	R. Jabee and M. Afshar [2]	Studied the requirement to enhance the default privacy settings in fb.	The studies show that the users should be extra conscious and involved concerning the default protection settings in

			fb.
2016	V. L. Yisa, O. Osho, and I. Soje [3]	Measured the effect of the web Social Networks (OSNs) on the performance of the scholars	The end result of the study represents that there may be the tremendous impact of the OSNs on the scholar overall performance. Additionally, numerous students' skilled safety risks at the same time as the use of those online social networks.
2014	A. Singh, D. Bansal, and S. Sofat [4]	Explored numerous privateers preserving strategies including L-variety, okay-anonymity and integrated k-anonymity L-diversity	The end result of the look at shows that the information preserving strategies analyzed in this study are not effective sufficient to save you the records loss and massive improvement is needed in those strategies.
2014	M. Fire, R. Goldschmidt and Y. Elovici [5]	Very well reviewed the unique privateness and safety risks and offered present safety solutions to prevent the personal statistics loss.	Advised answers are powerful for the ONS users to enhance privateness and safety troubles at the same time as the usage of those structures.
2015	Y. Najaflou, B. Jedari, F. Xia, L. T Yang and M.S.Obaidat	The examiner offers a regular categorization on exclusive protection. Challenges and explores various solutions in the Mobile Social Networks.	The privacy engages provinces had been classified into three classes along with private matching, fairness. Encouragement, and obfuscation
2016	D. Hiatt and Y. B. [7]	The issue of protection in social networking web sites and how it pertains to the privateness is defined in this paper.	Offer numerous tremendous steps to enhance the security and privateness on social networking websites.
2016	L. Dehigaspege, U. Hamy, H. Shehan and D. Dhammearatchi[8]	Proposed voice popularity method at the side of area identity and CAPTCHA's mechanism to protect the cyber protection attack.	The proposed technique is powerful to protect the cyber safety assault and effectively pick out the area from where the social networking account is accessed.
2015	M. Prasanthi, [9]	The study described numerous law acts that are imposed towards the cybercrime	Encouraged numerous protection suggestions to apply social networking web sites.
2015	R. Chouhan[10]	Delivered an analytical method to define diverse traits utilized in cyber crime	Advised numerous techniques to combat the cyber protection problems along with technological attitude, strategic attitude, and legal perspective.

VIII. CONCLUSION

Social Networking web sites (SNS) provide numerous advanced techniques to talk and have interaction with human beings around the world. Human beings can without problems gain their cherished ones and buddies through Social networking internet sites. Despite the fact that there are numerous advantages of social

networking web sites, in addition they raise numerous worrying conditions for the clients; extra specially the security and privacy problems. Those security and privacy threats are possibilities for the attacks, viruses and different malicious actors. Therefore, there may be a call for to decorate the safety answer techniques.

In this paper, I reviewed various social networking net web sites, their safety and privacy problems. I reviewed the research that already has been executed to prevent the dearth of data and breaches due to the security and privateness threats. Additionally, the paper suggests several steps to the users for improving the safety at the equal time as the usage of the social networking net web sites.

BIBLIOGRAPHY

[1]. W.Ghari and M. Shaabi"Cyber Threats in Social Networking Websites," International Journal of Distributed and Parallel Systems, 2012.

[2]. R. Jabee and M. Afshar, "Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)," International Journal of Computer Applications, 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, 2016.

[4]. A. Singh, D. Bansal, and S. Sofat, "Privacy Preserving Techniques in Social Networks Data Publishing - A Review," International Journal of Computer Applications, 2014.

[5]. M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," IEEE Communications Surveys & Tutorials, 2014.

[6]. Y. Najaflou, B. Jedari, F. Xia, L. T. Yang and M. S. Obaidat, "Safety Challenges and Solutions in Mobile Social Networks," inIEEE Systems Journal, 2015.

[7]. D. Hiatt and Y. B., "Role of Security in Social Networking," International Journal of Advanced Computer Science and Applications, 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, 2016.

[9]. M. Prasanthi, "Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, 2015.

[10]. R. Chouhan, "Cyber Crime: A Changing Threat Scenario in the State Of Art," International Journal of Engineering Research and General Science, 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, 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, 2016.

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

[14]. A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance, 2015.

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