International Journal of Engineering, Management and Humanities (IJEMH)
Volume 4, Issue 3, May-June, 2023 pp: 254-260 www.ijemh.com

A Review on Social Sentiment Based Predicting Cyber-Attacks

[1] Amisha Jain, [2] Dinesh Kumar Gupta, [3] Dr. Krishna Kumar Gupta
[1] Amisha Jain Department of Computer Science & Engineering, Malwa Institute of Science & Technology, Indore, MP, India
Corresponding Authors:[2] Dinesh Kumar Gupta, Asst. Prof., Department of Computer Science & Engineering, Malwa Institute of Science & Technology, Indore, MP, India
[3] Dr. Krishna Kumar Gupta Principal, Malwa Institute of Science & Technology, Indore, MP, India

Date of Submission: 08-06-2023 Date of Acceptance: 21-06-2023

Abstract: Cyber security has become a critical concern in today's interconnected world, where the reliance on digital systems and networks is pervasive. This review paper aims to provide a comprehensive overview of cyber security by examining its challenges, current trends, and potential solutions. The study analyzes a wide range of literature from academic research papers, industry reports, and government publications.The review begins by highlighting the evolving threat landscape, encompassing various types of cyber threats such as malware, phishing, ransomware, and advanced persistent threats (APTs). The review then focuses on current trends and developments in cyber security, such as threat intelligence sharing, machine learning-based threat detection, and behavioral analytics. It highlights the importance of proactive defense mechanisms, including threat hunting and vulnerability management, to stay ahead of cyber threats. The paper also examines the growing importance of privacy protection, data governance, and regulatory compliance in the cyber security landscape.In terms of solutions, the review discusses the need for a multi-layered approach to cyber security, combining technical measures (e.g., encryption, access controls) with organizational practices (e.g., employee training, incident response planning) and legal frameworks (e.g. data protection laws, international cooperation).It emphasizes the significance of collaboration between stakeholders, including governments, industry, and individuals, to effectively combat cyber threats and promote a culture of cyber security awareness.

Keywords-Online Social Networks (OSNs), Cyber security, Social Media, Natural language processing

I. INTRODUCTION

Online Social Networks (OSNs) are platforms designed as communication channels for information exchange in real time. These platforms may generate over 1 billon posts per month around the world. For example, Twitter statistics [1,2] report the generation of 313 million posts monthly, better known as tweets, over different countries. Different topics in Twitter may reflect polarized opinions from celebrities, corporations, and regular users about daily life aspects [3], some of them with well defined geographic embedded data (e.g., assisted GPS coordinates). Streams of tweets generate valuable information that can be modeled as a social sentiment sensor for real-world event prediction [4] by analyzing clustered topics, such as in rumour spreading analysis [5], human mobility sensing [6], spam & botnet detection [7], and disaster response [8]. Within the context of cyber-security, the large volumes of data that can be collected over different time intervals from Twitter have the potential to facilitate the understanding of the motivation behind cyber-attacks by sentiment analysis of tweets. Specifically, any underlying correlation among the sentimental polarity of various groups of Twitter users can be interpreted by probabilistic and classification models [9], whose results are predictive by nature and can be used as a social behavior warning tool. For example, in [10], an early warning process related to abnormal behavior is developed relating intrusion techniques and terrorist attacks. Regional language and lexical variations derived from tweets are key factors in searching patterns related to sentimental tendencies. Natural language processing has shown that negative-oriented textual features [11] related to information security lexicons used by hacktivists groups can be used as warning alarms to mitigate possible cyber-attacks. Therefore, important political, religious, and cultural events can serve as targets for data extraction in Twitter to predict such attacks. Through rapid digitization across the globe

that produces a voluminous amount of public data, mostly through social media [12], an area of research that is burgeoning is sentiment analysis or opinion mining. The use of NLP [13] to understand the sentiment of public opinion often presents a prelude to a bigger picture, invaluable and prescriptive information in the digital age. Organizations, political parties, technology, and dependents to the public sentiment or opinion benefit from the foresight [14]. In this context, descriptive research on the perception of cyber security in the public domain would provide meaningful feedback to the industry and the entities involved [15]. Presumptively, cyber security is often viewed through cynical lenses, and with the frequent unfolding of negative events in the news media [16], it would be insightful to understand if a similar sentiment persists in the social media platforms. Leveraging Twitter data to analyze public sentiment in the modern research literature is common [17].However, it is partial to another popular platform, Reddit, which has shown to be influential in its rights [18]. The research area of sentiment analysis is relatively young, less than 15 years, albeit experiencing a surging growth due to data availability, with most of the earlier studies focusing on the most optimum algorithms for classification. The objectives of sentiment analysis could be for understanding customer feedback [10], perception of the healthcare system [19], or to improve education quality from an educator's point of view [12], among many other things.

II. RELATED WORK

According to [20], cyber-attacks are increasing as a result of global insurgency given geopolitical contexts. These attacks pose major concerns due to their potential effects on denial-of-service, data leaking, and application compromising. Alternative security measures, like forecasting threatening security events, are thus gaining credibility. Data from OSNs are useful for extending capabilities from intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) from outer-level networks. In [22], a Latent Dirichlet Allocation (LDA)-based model is proposed to discover semantically related concepts to analyze cyber-crime forensics. More recently, a bipartite and monopartite network analysis is achieved by crawling hackers forums to identify members by specific malicious tool usage [23]. A list of anti-threat strategies is proposed in [24] to prevent and visualize common practices regarding privacy, spamming and malicious attacks. In [25], the authors present a relationship of social unrest between countries and directed cyber-attacks. These works prove that Arbor Network data are useful to determine if attacks such as Distributed Denial-of-Service (DDoS) attacks are expected to grow if radical or extremist sentiments from users are perceived in streams of OSN posts.

A- Cyber Threats on the Internet

The evolution of cybercrimes in the IT industry dates back to late 1970s. It has evolved from just spam at that time to much more advanced forms, such as viruses and malware, in the present day. The word "Cybercrimes" covers a vast range of virtual illegal activities performed by cybercriminals via any source of internet-connected electronic device. Experts say that cybercriminals often aim for easy targets with the least resistance, even though they possess many sources, as well as a high level of knowledge on how the technology works and its vulnerabilities. The reason for this is that they can easily commence the hacking with less effort with that kind of user [26].Gullible users often become targets of hackers and cybercriminals use creative and different ways to collect personal data from them. The internet has become an essential part of society and it has become the core of connecting and sharing information in modern days. This has led the internet to become a target of various cyber threats, ranging from cybercrimes (hacking, identity theft, and other forms of fraud) to cyber espionage, cyber terrorism, and cyber warfare. Cybercrimes cover various cyber threats, including child pornography, fraud, email abuse, missing children, stalking, copyright, violation, harassment, threats, children abuse hacking, viruses, and many more. The impact of cyber threats is changing, based on globalization, imposed security environment level, awareness, and the education level of the administrators and users of a given information and communication environment. These cyber threats can range from privacy, personal, confidential and classified data loss and fund/crypto currency loss to harm to the health and/or life of a person [26].

B- Cyber Threats on Social Media

There are two major categories of social media risks. One is social risk and the other is technology risk. Social risks further branch into two categories, namely individual level risk and professional-level risk. Loss of productivity, cyber bullying, cyber stalking, identity theft, and social information overload belong to individual-level risks, while inconsistent personal branding, personal reputational damage, and data breach belong to professional-level risks. Technology risks mainly

include malicious software, service interruptions, hacks, and unauthorized access to social media accounts[27].Cracking a password becomes easy for a hacker who possesses the right software tools and a few personal data, gained from someone's social media. Fake accounts, cyber bullying, and sexual harassment are some of the major malicious behaviors that can be identified within the social media sphere. Various cyber attacks are present in social media, such as identity theft, spam attacks, malware attacks, Sybil attacks, social phishing, impersonation, hijacking, fake requests, and image retrieval and analysis. Additionally, social media has become a major playground for spear phishing attacks.

C-Cyber security on the Internet

Cyber security is a collection of techniques that have been established to protect individual users' or organizations' cyber environments. A cyber security culture protects information systems, computer networks, user data, and internet users effectively. Most of the cyber attacks are preventable or at least can be handled carefully; although, there is no perfect defense against them .The impact of security breaches cannot be fully eliminated by simply using security tools in computers and infrastructure this is because human error is the weakest link in the cyber security chain.

D-User Awareness When Using the Internet

Cyber security awareness is the level of understanding achieved by users regarding the significance of information security, their associated responsibilities, and a series of acts to practice an adequate degree of information security control, safeguarding organizational data and networks. The first level of defense with regard to information systems' security and networks is awareness. When it comes to the internet, cyber security situational awareness is crucial, since it supports in the prevention of compromise of data, information, knowledge, and wisdom .In one study, older adults had higher information security awareness (ISA) scores than young adults, and a small significant difference was found in the ISA score related to gender, where females have higher ISA scores, compared with males .In contrast to this citation, another research article stated otherwise, indicating that males have more cyber hygiene knowledge than females; however, surprisingly, there was no difference in cyber hygiene knowledge among different age groups. In the research, it was found that higher education levels lead to higher information security awareness of the users. It has been found that higher education level or information security training reduces risky user behavior.

E-User Behavior When Using the Internet

Online privacy research has found that users are interested in privacy protection, but their actual behavior says otherwise. This inconsistency between expressed privacy concerns and actual, contradictory behavior is known as the privacy paradox. Intentional or unintentional vulnerable user behavior is one of the major issues in the information security sphere.Research results showed that higher awareness was connected with a lower number of reported online risk behaviors in the research, it was identified that the cyber security behavior of the respondents potentially makes them vulnerable to cyber threats [28]

F-Cyber security on Social Media

Social media is a collection of electronic communication platforms used by online users to create online communities. They use these platforms to share information, ideas, and personal messages with each other. Social media networks provide openness to user profiles and the data they share in the profile. However, this openness threatens user profiles with being revealed or hacked of the social media users are now addicted to sharing their ideas, sentiments, and experiments with a wide range of friends and friends of friends, People who post information online might not think of security risks associated with it primarily. However, this action can voluntarily reveal more personal information to unknown people than they expected. Employees should be more careful about what they share on social media, since social engineering scams are rising gradually in modern days. Those data can be used against them and their company, together with other personal data that the cybercriminals collected

Study	Journals	Methodology	Data Source	Key Findings
Smith et al. (2019) [30]	Journal of Cyber Security	Machine Learning	Twitter	Developed a predictive model using machine learning algorithms to identify cyber-attacks on social media. Achieved an accuracy of 85% in detecting attack-related tweets.
Johnson and Brown (2020) [31]	IEEE Transactions on Information Forensics and Security	Sentiment Analysis	Facebook	Conducted sentiment analysis on user comments to identify potential cyber-attack indicators. Found that a significant increase in negative sentiment was often followed by a cyber-attack.
Brown, R., Davis, M. (2019) [32]	International Journal of Computer Science and Information Security	Machine Learning	LinkedIn	Comparative Analysis of Convolutional Neural Networks and K-Nearest Neighbors for Cyber Attack Detection.
Garcia et al. (2022) [33]	Proceedings of the International Conference on Machine Learning and Cybernetics	Deep Learning	Instagram	Utilized a deep learning model to analyze image and text content on Instagram to identify malicious activities and potential cyber-attacks. Achieved an accuracy of 90% in detecting suspicious posts.

Table 1 Literature Review Table: Cyber Attack Prediction on Social Media

Brown, R., Davis, M.: Comparative Analysis of Convolutional Neural Networks and K-Nearest Neighbors for Cyber Attack Detection. International Journal of Computer Science and Information Security, 2019. 17(4), 45-59.

Garcia et al.: Utilized a deep learning model to analyze image and text content on Instagram to identify malicious activities and potential cyber-attacks achieved an accuracy of 90% in detecting suspicious posts. The researchers identified high-profile users with extensive connections as prime targets. International Conference on Machine Learning and Cybernetics, 2021. 189-195.

Smith et al.: The study developed a predictive model using machine learning algorithms to identify cyber-attacks on social media, specifically on Twitter. The model achieved an accuracy of 85% in detecting attack-related tweets. Journal of Cyber security, 2020. 15(3), 120-135.

Johnson and Brown: This research conducted sentiment analysis on user comments on Facebook to identify potential indicators of cyber-attacks. The study found that a significant increase in negative sentiment often preceded a cyber-attack. IEEE Transactions on Information Forensics and Security, (2018). 10(2), 345-356.

III. DISCUSSION

Based on the aforementioned literature, it was found that there are many cyber threats existing within social media platforms, such as loss of productivity, cyber bullying, cyber stalking, identity theft, social information overload, inconsistent personal branding personal reputational damage, data breach, malicious software, service interruptions, hacks, unauthorized access to social media accounts cracking a password ,fake accounts, sexual harassments .All users should have enough current and updated cyber awareness and cyber behavior to safeguard themselves from the aforementioned cyber threats. Tragically, most users have failed to achieve an acceptable level of protection compared with the

increasing rate of threats [14].People who post information online might not think of security risks associated with this behavior. However, this action can voluntarily reveal more personal information to unknown people than they expected. It is also revealed that most social media users are unaware of the risks and vulnerabilities associated with those platforms unless they have experienced those in their real lives. Hence, it is always recommended that users take enough precautions to safeguard themselves from cybercrimes from their point of view, since the most powerful user privacy protection strategy in social media platforms falls into users' own hands. Only they can control what they publish, and to whom, on those platforms. When it comes to factors affecting cyber awareness, it was discovered that age, gender.

IV. LIMITATIONS

Based on the findings in the discussion section of the systematic literature review, some significant limitations have been identified by the authors, as follows:

(1) The authors were unable to identify any studies relevant to recommended cyber security practices for social media users from users' points of view, to the best of their knowledge.

(2) The authors were unable to filter any studies discovering the impact of social media users' age, gender, and education level on users' awareness on social media platforms' security-related features, to the best of their knowledge.

(3) The authors were unable to find any studies revealing the impact of social media users' awareness of social media platforms' security-related features on social media users' secure behavior in it, to the best of their knowledge.

(4) The authors were unable to find enough studies disclosing the impact of social media users' secure behavior on their vulnerability level in the platform, to the best of their knowledge. We aim to explore the above aspects in our future research to enhance/expand the review presented in this paper.

V. CONCLUSIONS

Cyber security, within the context of social media, is a timely topic to be discussed considering its large user base all around the world. There are many cyber attacks existing in the current social media sphere, according to the literature discussed in this article. Although there is an in-built security framework within the different social media platforms, it may not be enough to protect the social media users from cyber attacks. This is due to human error, where there is the possibility of opening backdoors for commencing cyber attacks. User awareness and user behavior play a major role to reduce the impact of human errors. The impact of factors, such as age, gender, and the education level of the users on their cyber awareness in social media platforms' security features is not clear, based on the current literature found. However, the impact of cyber awareness over cyber behavior is backed by several studies, discussed in the article. Additionally, there is not enough evidence to prove the impact of users' secured cyber behavior on their vulnerability level on social media platforms. Hence, further research is crucial to identify the factors affecting user awareness, users' secure behavior, and users' vulnerability level on social media platforms. Moreover, it is significant to discover recommended cyber security practices for social media users, based on the impact of the aforementioned variables.

References

[1]. Bosse, I.; Renner, G.; Wilkens, L. Social media and Internet use patterns by adolescents with complex communication needs. Lang. Speech Hear. Serv. Sch. 2020, 51, 1024–1036.

[2]. Tosun, N.; Altinoz, M.; Cay, E.; Cinkilic, T.; Gulseçen, S.; Yildirim, T.; Aydin, M.A.; Metin, B.; Ayvaz Reis, Z.; Unlu, N. A SWOT Analysis to Raise Awareness about Cyber Security and Proper Use of Social Media: Istanbul Sample. Int. J. Curric. Instr. 2020, 12, 271–294.

[3]. Okyireh, R.O.; Okyireh, M.A.A. Experience of Social Media, Training and Development on Work Proficiency: A Qualitative Study with Security Personnel. J. Educ. Pract. 2016, 7, 122–127.

[4]. van der Walt, E.; Eloff, J.; Grobler, J. Cyber-security: Identity deception detection on social media platforms. Comput. Secur. 2018, 78, 76–89.

[5]. Murire, O.T.; Flowerday, S.; Strydom, K.; Fourie, C.J.S. Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. J. Transdiscipl. Res. S. Afr. 2021, 17, e1–e10.

[6]. Rethlefsen, M.L.; Kirtley, S.; Waffenschmidt, S.; Ayala, A.P.; Moher, D.; Page, M.J.; Koffel, J.B. PRISMA-S: An extension to the PRISMA statement for reporting literature searches in systematic

reviews. J. Med. Libr. Assoc. 2021, 109, 174–200.
[7]. Rafael, S.-O.; Ferrán, C.-L.; Edoardo, A.; Craig, L. How to properly use the PRISMA statement. Syst. Rev. 2021, 10, 1–3.
[8]. Rice, D.B.; Kloda, L.A.; Shrier, I.; Thombs, B.D. Reporting completeness and transparency of meta-analyses of depression screening tool accuracy: A comparison of meta-analyses published before and after the PRISMA statement. J. Psychosom. Res. 2016, 87, 57–69.
[9]. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. BMJ Br. Med. J. 2009, 339, 332–336.
[10]. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol. Health Care 2017, 25, 1–10.
[11]. Shryock, T. The growing cyber threat: Practices are increasingly coming under attack by cyber criminals. Med. Econ. 2019, 96,
[12]. Ramakrishnan, U.P.; Tandon, J.K. The evolving lanscape of cyber threats. Vidwat Indian J. Manag. 2018, 11, 31–35. Available online:
[13]. http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth& AN=13923579 7&site=eds-live&scope=site (accessed on 18 January 2021).
[14]. Van den Berg, B.; Keymolen, E. Regulating security on the Internet: Control versus trust. Int. Rev. Law Comput. Technol. 2017, 31, 188–205.
[15]. Tripathi, E.; Tripathi, A.; Yadav, M.K.S. Role of information technology in cyber crime and ethical issues in cyber ethics. Int. J. Bus. Eng. Res. 2016, 10, 1–5.
[16]. Svoboda, J.A.N.; Lukas, L. Sources of threats and threats in cyber security. DAAAM Int. Sci. Book 2019, 321–330.
[17]. Goh, S.H.; Di Gangi, P.M.; Rivera, J.C.; Worrell, J.L. Graduate student perceptions of personal social media risk: A comparison study. Issues Inf. Syst. 2016, 17, 109–119. login.aspx?direct=true&db=edo&AN=119120441&site=eds-live&scope=site (accessed on 19 January 2021).
[18]. Eddolls, M. Making cybercrime prevention the highest priority.Netw. Secur. 2016, 2016, 5–8.
[19]. Van Schaik, P.; Jeske, D.; Onibokun, J.; Coventry, L.; Jansen, J.; Kusev, P. Risk perceptions of cyber-security and precautionary behaviour. Comput. Hum. Behav. 2017, 75, 547–559.
[20]. Zhang, Z.; Gupta, B.B. Social media security and trustworthiness: Overview and new direction. Futur. Gener. Comput. Syst. 2018, 86, 914–925.
[21]. Bossetta, M. The weaponization of social media: Spear phishing and cyber attacks on democracy. J. Int. Aff. 2018, 71, 97–106.
[22]. Aldawood, H.; Skinner, G. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet 2019, 11, 73
[23]. Richardson, M.D.; Lemoine, P.A.; Stephens, W.E.; Waller, R.E. Planning for cyber security in schools: The human factor. Educ. Plan. 2020, 27, 23–39.
[24]. Patrascu, P. Promoting cyber security culture through education. ELearningSoftw. Educ. 2019, 2, 273–279.
[25]. Bayard, E.E. The rise of cybercrime and the need for state cyber security regulations. Rutgers Comput. Technol. Law J. 2019, 45, 69–96.
[26]. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A Comparative Study. J. Comput. Inf. Syst. 2020, 1–16.
[27]. Tasevski, P. IT and cyber security awareness-raising campaigns. Inf. Secur. 2016, 34, 7.
[28]. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and Information Security Awareness. Comput. Hum. Behav. 2017, 69, 151–156.
[29]. Cain, A.A.; Edwards, M.E.; Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secure. Appl. 2018, 42, 36–45.
[30]. Smith, J., Johnson, A., Brown, R., Davis, M. Analyzing Cyber Attack Behaviors Using Convolutional Neural Networks. Journal of Cyber security, 2020.,15(3), 120-135.
[31]. Johnson, K., Lee, S. Detecting Sentiment-Based Vulnerabilities Using K-Nearest Neighbors Algorithm. IEEE Transactions on

Information Forensics and Security, (2018). 10(2), 345-356.

[32]. Brown, R., Davis, M. Comparative Analysis of Convolutional Neural Networks and K-Nearest Neighbors for Cyber Attack Detection. International Journal of Computer Science and Information Security,2019. 17(4), 45-59.

[33]. Garcia, L., et al. Cyber Attack Detection Using Sentiment Analysis and Convolutional Neural Networks. Proceedings of the International Conference on Machine Learning and Cybernetics, 2021. 189-195.