DOIs:10.2017/IJRCS/202310011 --:-- Research Paper / Article / Review

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: A STUDY

Dr. Nimisha. M.N
Assistant Professor, Department of Management Studies
St. Aloysius College, Elthuruth, Thrissur, Kerala
Email - nimishanandan111@gmail.com

Abstract: *The frequency and sophistication of cyberattacks have both greatly increased during the past few decades. Therefore, developing a cyber-resilient strategy is of utmost significance. In the event of a cyberattack, traditional security measures are insufficient to prevent data leaks. Cybercriminals have mastered the use of cutting-edge methods and powerful tools to hack, attack, and breach data. Artificial Intelligence (AI) technology has been applied to the creation of intelligent models for securing systems against attackers. AI technologies can quickly advance to meet complicated problems, making them useful as fundamental cybersecurity tools. AI-based solutions can offer effective and potent cyber defence capabilities to identify malware attacks, network intrusions, phishing, spam emails, and data breaches, and to notify security incidents when they happen. In this essay, we examine the role of AI in cybersecurity and analyse the pertinent literature in terms of its advantages.*

Keywords: *Cybersecurity, artificial intelligence, cyberattack, cyber defence.*

1. INTRODUCTION :

An attack launched from one or more computers against other computers or networks is referred to as a cyberattack. The purpose of a cyberattack is to either disable the target computer, shut down the services, or access the data on the target computer[1]. The frequency and severity of cyberattacks have significantly increased since the first Denial-of-Service (DoS) assault in 1988. Indeed, maintaining cybersecurity has grown to be one of the most difficult challenges in the field of computer technology, and it is anticipated that cyberattacks will continue to get more sophisticated and numerous. One of the most serious challenges in cyberspace today is cybersecurity. Cybersecurity refers to the set of activities and measures, both technical and non-technical, intended to protect the 'real geography' of cyberspace as well as devices, software, and the information they contain communicated, from all possible threats[2].

Traditional cybersecurity techniques rely on static control of security equipment and operate in reaction to an attack. Security systems, for instance, keep an eye on nodes in the event of network intrusion attacks by a predetermined set of criteria. These procedures hold off until they receive word that an attack has happened. However, the conventional strategy is no longer effective given the rising number of cyberattacks. The Equifax attack in 2017, which exposed the data of up to 143 million consumers, is one illustration of the inadequacies of conventional cybersecurity techniques[3].Furthermore, because attackers often conceal their activity and launch attacks before software developers are aware of vulnerabilities due to emerging threat strategies like Advanced Persistent Threats (APT's) and zero-day attacks, it takes some time to fix the susceptible systems. Corporate security, national security, law enforcement, and the intelligence community are all impacted by a lack of adequate cybersecurity capabilities[4].

Government and private computer systems have been attacked by hackers who took advantage of security system flaws and malfunctions as well as weaknesses in IT infrastructure. Therefore, the classic passive defence strategies are no longer adequate. The only way to secure data in the uncertain climate of today, when cyberattacks occur often and are continuously changing, is by utilising aggressive cyber methods. Therefore, the new strategy must stop attacks before they start rather than wait to receive information after attacks have already taken place[5].The only way to secure data in the uncertain climate of today, when cyberattacks occur often and are continuously changing, is by utilising aggressive cyber methods. Therefore, the new strategy must stop attacks before they start rather than wait to receive information after attacks have already taken place. To provide the best solutions for cyber environments and strengthen cybersecurity capabilities against cyber-attacks, this research examines the necessity for the evolution of cybersecurity strategies.

2. AI BASED APPROACHES IN CYBER SECURITY :

The expense of preventing threats rises due to the high cost of hiring specialists. The development and application of algorithms to identify those dangers likewise involves a significant amount of time, money, and effort. Utilising AI-based techniques is one remedy for those problems. AI is capable of quickly, correctly, and efficiently analysing massive amounts of data. An AI-based system can predict future assaults that will be similar to those that have already occurred by using threat history, even if the patterns of those attacks vary. These factors make AI applicable in cyberspace. AI can handle vast data, find new and significant changes in attacks, and continuously improve its security system's response to threats.[6]

AI does, however, have certain drawbacks. For example, an AI-based system requires a sizeable amount of data, and processing this volume of data demands a lot of time and resources. Frequent false alarms are also a problem for end users, and delaying any necessary responses reduces efficiency. The AI-based system can also be attacked via adversarial inputs, data poisoning, and model theft. Recent research has shown how AI methods can be used to recognise, thwart, and address cyberattacks.

Three categories best describe the most prevalent categories of cyberattacks:

- **Software exploitation and malware identification**

  Every software has flaws, and some of those flaws can be used to an attacker's advantage by the attacker who is aware of the flaw to attack the underlying software program. Buffer overflow, integer overflow, SQL injection, cross-site scripting, and cross-site request forgery are a few common software vulnerabilities. Certain flaws are found and corrected. The ideal situation would have been if software developers had identified and repaired every vulnerability throughout the design and development phase, but this is exceedingly challenging given the high cost of software development and the urgency to get products to market. Therefore, identifying and resolving issues is a constant process. Going line by line through the code to correct software defects is a laborious operation, but computers are capable of doing it if they are taught what the vulnerabilities look like. It seems possible that AI could complete these duties. Malicious software can be classified as viruses, worms, and Trojan horses. Malware attacks can have a significant impact on politics and the economy, so it's important to stop them and mitigate the damage they inflict. Therefore, there have been numerous studies about implementing AI technology.
  A deep learning architecture was constructed using a different method to identify sophisticated malware. The subject of the current malware detection study was mobile malware[7]. To recognise malware, a deep convolutional neural network was used. To recognise malware, the authors defined a brand-new machine-learning method called rotation forest.[8]

- **Network intrusion detection**

  Denial of Service (DoS) is one of the most frequent attacks that happen when authorised users are prevented from accessing data, devices, or other network resources as a result of a fraudster's activity. The authors suggested a system that uses distributed artificial neural networks with an anomaly-based approach and a signature-based approach.[9]
  Intrusion Detection System (IDS) guards against anomalous occurrences, violations, and immediate dangers in a computer system. AI-based technologies are suitable for creating IDS because of their adaptability, quick computations, and easy learning. AI-based algorithms seek to reduce false alarms by optimising features and strengthening classifiers. To develop a model for IDS, the authors merged a support vector machine and a tweaked version of k-means. The authors presented a reinforcement learning strategy based on fuzziness for IDS. To improve the performance, they combined supervised learning with unlabelled sample datasets. Another

strategy predicts network traffic for a specified period by using evolutionary algorithms and fuzzy logic for network intrusion detection.[10]

- **Phishing and spam detection**

The goal of a phishing attack is to steal user identity. Examples of phishing attempts include dictionary and brute-force assaults. A phishing detection system called phishing email detection system made use of reinforcement learning and customised neural networks. Feng et al. used a neural network in conjunction with the Monte Carlo method and a risk-reduction strategy to detect phishing websites.[11]

Spam detection refers to the uninvited bulk email. Spam emails could contain incorrect information, which raises security concerns. Spam emails can be filtered using AI-based algorithms. To filter spam emails, this system integrated the support vector machine with a naive Bayes algorithm. AI can be used to analyse data for attack detection and retaliation in a variety of cyberspace areas. AI may also automate operations, which enables security experts to swiftly identify cyberattacks using semi-automated systems. AI techniques can spot dangers and stop attacks before they happen. This is typically done by using a model that examines large datasets of cybersecurity events and spots patterns of hostile behaviour. Indicators of Compromise (IoC) that have been recorded and previously monitored data are often included in the model, which is used to track, detect, and instantly react to threats. As a result, if comparable behaviours are found, the models are used to automatically identify them. IOC datasets are used by Machine Language (ML) classification algorithms to recognise the various behaviours of malware in datasets and categorise them. Additionally, behavioral-based analysis examines the behaviour of hundreds of malware using machine language clustering and classification techniques. Security analysts and other automated systems can also profit greatly. For instance, ML algorithms can train to recognise such assaults automatically utilising historical datasets that include specific occurrences of WannaCry ransomware attacks[12].

Network risk scoring is a quantitative measure that assigns risk rankings to various network segments. Based on the risk scores, this method is used to rank the importance of cybersecurity resources. By examining historical cybersecurity records, AI can automate this process by identifying the parts of networks that are more exposed to or participating in particular sorts of attacks.

AI can automate routine procedures carried out by security analysts during security operations. Analysing reports on previous actions produced by security analysts can be used to automate processes and successfully identify and counteract specific assaults. This information is used by AI algorithms to create a model that may later be used to find related online actions. With this concept, AI algorithms react to assaults devoid of human interpretation. It can be challenging to fully automate the security process at times. In this scenario, AI can be integrated into the cybersecurity workflow, allowing system analysts and computers to work together to complete tasks.

3. CONCLUSION :

Virus identification, network intrusion detection, and phishing and spam detection are the key goals of AI-based cybersecurity algorithms. Numerous studies have combined various AI techniques, such as Machine learning (ML) or Deep Learning (DL) techniques with bio-inspired computation, or various learning techniques, such as supervised learning and reinforcement learning. Such mixtures produce excellent outcomes. Even though AI will inevitably play a part in resolving cyberspace challenges, several issues surrounding AI trust and AI-based threats and attacks should still be taken seriously.

REFERENCES :

1. Chen, H., & Dongre, R. (2014). Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, *4*(10), 40–42. https://doi.org/10.22215/timreview/838
2. Guan, Z., Li, J., Wu, L., Zhang, Y., Wu, J., & Du, X. (2017). Achieving efficient and secure data acquisition for Cloud-Supported internet of things in smart grid. *IEEE Internet of Things Journal*, *4*(6), 1934–1944. https://doi.org/10.1109/jiot.2017.2690522

3. Equifax Says Cyberattack May Have Affected 143 Million in the U.S. (2017, September 7). *The NewYork Times*. Retrieved September 4, 2023, from https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html%20.
4. Wilner, A. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. *International Journal*, *73*(2), 308–316. https://doi.org/10.1177/0020702018782496
5. Chowdhury, M., Rahman, A., & Islam, R. (2017). Malware analysis and detection using data mining and machine learning classification. In *Advances in intelligent systems and computing* (pp. 266–274). https://doi.org/10.1007/978-3-319-67071-3_33
6. Venkatraman, S., & Alazab, M. (2018). Use of data visualisation for Zero-Day malware detection. *Security and Communication Networks*, *2018*, 1–13. https://doi.org/10.1155/2018/1728303
7. Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). Learning and classification of malware behavior. In *Lecture Notes in Computer Science* (pp. 108–125). https://doi.org/10.1007/978-3-540-70542-0_6
8. Alejandre, F. V., Cortés, N. C., & Anaya, E. A. (2017). Feature selection to detect botnets using machine learning algorithms. *2017 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, 1–7. https://doi.org/10.1109/conielecomp.2017.7891834
9. Alzahrani, S. M., & Hong, L. (2018). Detection of Distributed Denial of Service (DDoS) Attacks Using Artificial Intelligence on Cloud. *2018 IEEE World Congress on Services (SERVICES)*. https://doi.org/10.1109/services.2018.00031
10. Ashfaq, R. a. R., Wang, X., Huang, J. Z., Abbas, H., & He, Y. (2017b). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*, 484–497. https://doi.org/10.1016/j.ins.2016.04.019
11. Smadi, S., Aslam, N., & Zhang, L. (2018). Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. *Decision Support Systems*, *107*, 88–102. https://doi.org/10.1016/j.dss.2018.01.001
12. Broniatowski, D. A., Jamison, A. M., Qi, S. H., Alkulaib, L., Chen, T., Benton, A., Quinn, S. C., & Dredze, M. (2018). Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *American Journal of Public Health*, *108*(10), 1378–1384. https://doi.org/10.2105/ajph.2018.304567