NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 9, ISSUE 9, Sep. -2022

A CRITICAL EXAMINATION OF SHIELDING THE CYBERSPACE: A REVIEW ON THE ROLE OF AI IN CYBER SECURITY

Teja Reddy Gatla
Sr. Data Scientist, Associate Director, Department of Information Technology

ABSTRACT

This review focuses on the critical analysis of AI's role in cybersecurity to investigate the issues in the cybersecurity space. By utilizing synchronous and scattered sources on the topic in question, the opinion paper focuses capacity on AI-embedded technologies to enhance cybersecurity and discourage cyber-attacks making critical infrastructure impenetrable by malicious persons [1]. The paper is concerned with applying AI solutions paired with research documenting theoretical outcomes obtained from academic sources, field reports, and practical case examples. Suggestions, pros, and cons of those solutions, as well as the implications, are presented. More importantly, the paper does not only touch on the ethical and policy aspects of AI application in cyber security, but there is also a need for a detailed approach to cyber security, an approach that unites technological innovation to privacy, transparency, and accountability [1]. In contrast, the article brings attention to future developments and innovations in AI-based cybersecurity, which is a crucial need of the hour. AI evolution is seen in different aspects, such as designing complex Machine Learning algorithms till the inclusion of AI in Security Operations Centers (SOCs) and Threat Intelligence Platforms, which have prepared reliable weapons for cyber defense systems.

Keywords: Cyber Security, Artificial Intelligence, Ethics, Machine learning, Cyber Threats, Virus, Malware, Syntactic Variations, Threat Detection, Bots, IT infrastructure.

INTRODUCTION

With the increasing sophistication of cyber threats and malicious actors, making cybersecurity infrastructure an integral part of our present situation has become a need that cannot be ignored now more than ever. Though they are good to some extent, traditional security tools are not strong enough to cope with the creative strategies of cyber hooligans. Hence, integrating AI technology has been considered an essential solution to the advanced threats emerging in the dynamic context, helping to identify the targets more precisely within a timely manner and even react to the threats in a quicker and real-time approach [2]. The positive sides of AI in the cybersecurity sector are undeniable; however, AI carries a plethora of challenges and ethical concerns, which calls for an unstinted examination. AI cybersecurity will be more effective in countering cyber crimes as long as the network of cybersecurity mechanisms is -from organizations to jurisdictions- duly deliberated and critically analyzed concerning their potentials and risks surrounding the approach. AI systems, especially algorithmic machine learning-based ones, can issue-based data screening, detecting patterns and anomalies that may reflect malicious actions of cyber-threats in a wide range [2,3]. AI-based cybersecurity solutions equipped with humans' cyber abilities have proven to be effective in fighting against malware and phishing and detecting unauthorized intrusion attempts more than that contributed to the height of digital infrastructure. However, the AI technology used in cybersecurity is full of difficulties; even these technologies can be fallible to menace and misuse by evil actors as others do [4].

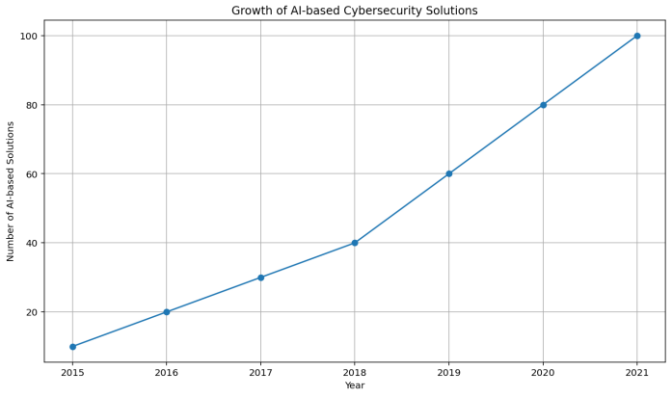

Fig. 1 Growth of AI-based Cyber Security solutions

AI technology, which is used for cybersecurity, imposes a superposition of ethics-related issues and its society, which need to be taken into account. The subject of fairness and morality is also present here because we cannot neglect the fact that AI algorithms might develop more than we want them to, checking the biases that can be applied to the data they are trained on [4]. Similarly, the opacity of AI decision-making processes may tempt the management of cybersecurity operations to become less transparent and make it easier for users to exercise their accountability. As AI technologies become the primary driver of more significant processes, we urgently find a way to cement high ethical standards and legal governance to address their control and mitigate the risks they entail. Through this paper, we will explore the impact of AI on cyber security, underscoring both the opportunities and the pitfalls resulting from using such technologies [5]. The ethical considerations will also be considered to determine the way forward to a safer and more ethical online environment.

RESEARCH PROBLEM

The research problem that this study addresses is on the role of AI-based cyber security systems, and their limitations in terms of ethical issues. Human-developed artificial intelligence can also be used to identify and prevent cyber threats. However, there are critical points in selecting AI algorithms, stopping adversarial attacks, and explaining AI systems. As a cybersecurity defense system, it will need to evolve rapidly for the sake of the responses to a constantly mutating threat [6]. The lack of reliability and consistency in cybercrime, AI algorithms, and their ability to neutralize the threats is quite evident one of the significant challenges in research in this area. There is still substantial doubt that they can work adequately in robust and general methods, especially when many attack scenarios and environments are considered [6]. Lastly, this type of AI technology is exposed to the vulnerability of adversarial attacks where strategically manipulated inputs can result in deception or subversion of such systems. This kind of AI algorithm poses some concerns regarding its dependability in the real world.

LITERATURE REVIEW

A. ADVANCEMENTS IN AI-POWERED THREAT DETECTION

Progress in AI is changing cybersecurity practices dramatically; now, organizations can find and respond to cyber threats with an exceptionally higher speed and accuracy. Machine learning models that use deep learning and other neural networks perform well at capturing crucial information in cybersecurity data for attack detection. For example, a study by [8] has shown how deep learning models can recognize unknown malware based on the representation of malicious behavior obtained from historical data. Moreover, threat report

demonstrations such as machine learning algorithms can detect even the slightest deviations in the network traffic, indicating that the new cyber threats could be stealthy and advanced. By utilizing AI-assisted threat detection technologies proactively, organizations can reduce the without delay incidents of cyber threats from important to severe security threats, as a result of which their cybersecurity posture is being enhanced.

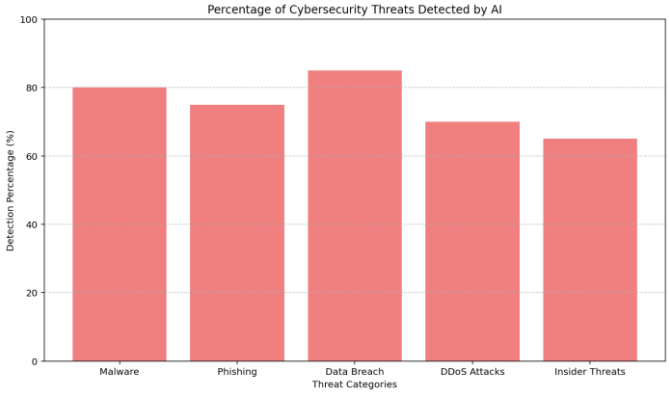

Fig. 2 Percentage of Cyber Security Threats Detection by AI

B. CHALLENGES IN ADVERSARIAL AI AND DEFENSE EVASION

AI-based threat detection is the best technology that helps organizations in cyberspace security. They can act on the identified threats with unusual speed and good precision. Deep learning makes machine learning much more profound, so the algorithms can analyze large datasets and spot attack patterns that might not be recognizable by other algorithm types, such as using deep learning to detect previously undetected malware by learning from historical data and recognizing the representation of malicious behaviors. Similarly, the McAfee Labs Threat Report [10] indicates that machine learning algorithms can spot subtle anomalies in network traffic that may indicate the existence of sophisticated cyber threats, such as advanced persistent threats (APTs) and insider threats.Organizations and enterprises can proactively uncover threats and mitigate them before they develop further into significant security events which means to be secured in this case.

C. ETHICAL CONSIDERATIONS IN AI-DRIVEN CYBERSECURITY

The deployment of AI-powered cybersecurity is not devoid of challenges as the hackers utilize ploys of adversarial attacks or evasion methods. Adversarial AI attacks are one of the most threatening scenarios for AI-driven cybersecurity solutions where malicious attackers exploit the weaknesses of the machine learning algorithms by deceiving AI models thereby compromising their integrity and dependability. Artificial intelligence has been proven to be vulnerable to adversarial examples through which hackers can trick models into incorrect predictions thus leading to false threats detection and raising critical interception issues. Furthermore, adversarial attacks have been proven to escape from AI-based detection systems, including intrusion detection systems and malware classifiers, thereby showing the dire need for the implementation of solid defense mechanisms against adversarial AI techniques. The solutions to these challenges include designing robust AI models, which, in turn, reinforce the adversarial defenses and adopting training AI techniques to make the cyber systems against attacks more resilient.

D. ETHICAL CONSIDERATIONS IN AI-DRIVEN CYBERSECURITY

AI advancements have shifted security methods, with SOAR platforms and automated security systems becoming mainstream. SOAR adoption comprises machine learning and natural language processing to represent a fully automated incident response workflow; the security operations are streamlined, and the threat

detection and response times improve. For example, Cisco Systems research [11] shows that AI-driven SOAR platforms can prioritize concerns from various sources and do people's regular work by automating them. In addition, these autonomous security systems, which AI powers to take the role of analyzing, detecting, and responding to cybersecurity threats in real-time, reduce the need for manual intervention and give the capability to cut down human error, thereby enhancing effective cybersecurity. For instance, research by [12] has been dedicated to exploring the AI robots' surveillance and mitigating cyber risk capacity, improving security resilience and efficiency.

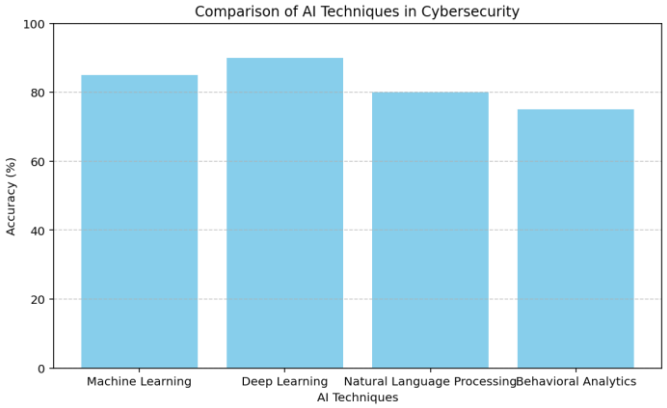

Fig. 3 Comparison of AI Techniques in Cyber Security

E. POLICY IMPLICATIONS AND REGULATORY FRAMEWORKS

Implementing the policy and regulatory system is integral to AI applications in the cybersecurity sphere of development and governance. Governments and regulators in several countries are increasingly paying attention to the ethical, legal, and societal impact of AI and security issues. The European Commission [13] presented regulations and provisions to encourage adopting responsible and ethical behavior using AI machines along with data protection, transparency, and accountability. Moreover, NIST (2020) has developed guidelines and standards that help organizations accept and implement AI cybersecurity solutions through risk management and continuous monitoring. By adopting such industry standards and regulations, companies can attain the required compliance with legal and ethical standards and get the maximum benefits of AI technology deployment for protecting their cybersecurity [14].

SIGNIFICANCE AND BENEFITS TO THE U.S

AI application in cybersecurity has proven viability in the United States and provides benefits and advantages in the future to address the increasing threats of cyberattacks. Primarily, AI-based cybersecurity provides the capability to implement adaptive security that withstands modern cyberattacks, the national security infrastructure, and combat system infiltration. By exploiting AI programs in threat detection, response to a security problem, and vulnerability management, the US can safeguard its digital resources, comprising government systems, military installations, and essential services, from cyber threats or cyber-attacks [15]. Furthermore, AI-based cybersecurity solutions provide the same economic gains by enabling the efficiency and effectiveness of cybersecurity operations, cutting down the expenditure incurred from cyber breaches and cybercrime. Such a sense of security makes businesses feel more secure in advancing, investing, and competing regionally and internationally, as this benefits the economy and job creation in the cybersecurity sector.

Moreover, AI-equipped cybersecurity technologies spur US leadership in technological innovation and competitiveness in the global marketplace. The US can maintain a competitive edge in developing innovative AI and cybersecurity technologies with the support of research and development programs that promote it [16]. Also, the US is bound to implement cyber defenses powered by artificial intelligence because it will help reinforce the bonds it shares with its allies on cybersecurity matters globally considering that these issues are increasingly transnational.

FUTURE IN THE U.S

The employment of AI in cyber security in the United States is expected to continue to grow and advance even more as AI progresses, more advanced technologies are developed, and strategic investments are made. With the advancement and maturity of AI technologies, more AI-supported cybersecurity solutions will be integrated into critical infrastructure, government institutions, and private sectors [17]. For example, the development of AI-driven intelligent robotic defense systems can quickly detect, analyze, and react to cybercrimes in real time; thus, human intervention and errors are reduced [17,18]. Additionally, the future of AI cybersecurity in the United States will depend on improvements in areas such as explainable AI, federated learning, and secure AI, which will be used to address challenges relating to transparency and security regarding privacy and adversarial attacks. The application of explainable [18] AI approaches makes it possible to observe and understand AI decision-making processes, which leads to transparency and responsibility in cybersecurity procedures. Using federated learning approaches enables good parties to cooperate in AI intelligence training without disclosing sensitive data, thereby ensuring privacy and confidentiality [19]. Secure AI approaches attempt to improve the reliability and resilience of AI models against attacks that aim to misuse them and undermine their impact.

CONCLUSION

The purpose of the present paper was to discursively analyze the role of AI in cybersecurity and the consequences of using it to protect cyberspace. An extensive review of literature and research was undertaken with a focus on the ability of AI technologies to reinforce cybersecurity systems, mitigate cyber threats, and secure critical infrastructure from malicious actors. By merging the results of academic studies, industry reports, and real-life implementations, we clarified the opportunities and challenges of AI-based cybersecurity solutions. Following our research, we addressed generative AI for cybersecurity, adversarial AI and defense evasion software, ethical sides of AI-driven cyber security, technology trends in AI-based security processes, and regulatory frameworks. An exploration of these individual elements reveals how machine learning affects cybersecurity platforms. This paper indicates the impact of AI on the alignment of cybersecurity defenses. It reiterates the need for a complex perspective on cybersecurity that envisages the integration of technological innovations with moral, legal, and policy principles. Generally, the relevance and profitability of AI in cybersecurity outstrip the country's boundaries, leading the USA to the forefront as the cybersecurity innovation and resilience leader.

REFERENCES

1. J.Pejas and A.Piegat, Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems. Springer Science & Business Media, 2006.
2. S. G. Kanade, Dijana Petrovska-Delacrétaz, and B. Dorizzi, Enhancing information security and privacy by combining biometrics with cryptography. San Rafael, Calif.: Morgan & Claypool, 2012.

3. K. Saeed, Jerzy Pejas, and Romuald Mosdorf, Biometrics, Computer Security Systems, and Artificial Intelligence Applications. Springer Science & Business Media, 2007.
4. R. Jiang, Somaya Al-Maadeed, A. Bouridane, Prof Danny Crookes, A Beghdadi, and SpringerLink (Online Service, Biometric Security, and Privacy: Opportunities & Challenges in The Big Data Era. Cham: Springer International Publishing, 2017.
5. Jaswal, Vivek Kanhangad, and R. Ramachandra, AI and Deep Learning in Biometric Security. CRC Press, 2021.
6. Sai et al., Computational Intelligence, Cyber Security and Computational Models: Proceedings of ICC3, 2013. New Delhi Springer India Imprint: Springer, 2014.
7. S.Balusamy, et al., Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation: Third International Conference, ICC3 2017, Coimbatore, India, December 14-16, 2017, Proceedings. Singapore: Springer Singapore, 2018.
8. Herrero, E. Corchado, Carlos Redondo Gil, Ángel Alonso Alvarez, and SpringerLink (Online Service, Computational Intelligence in Security for Information Systems 2010: Proceedings of the 3rd International Conference on Computational Intelligence in Security for Information Systems (CISIS'10). Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.
9. Jerzy Sołdek, Leszek Drobiazgiewicz, and Springerlink (Online Service, Artificial Intelligence and Security in Computing Systems : 9th International Conference, ACS ’2002 Międzyzdroje, Poland October 23-25, 2002 Proceedings. New York, NY: Springer Us, 2003.
10. B. W. D’andrade, Software engineering: artificial intelligence, compliance, and security. New York: Nova Science Publishers, Inc., 2021.
11. N. Bhargava, R. Bhargava, Pramod Singh Rathore, and R. Agrawal, Artificial Intelligence and Data Mining Approaches in Security Frameworks. John Wiley & Sons, 2021.
12. Karimipour, P. Srikantha, H. Farag, and J. Wei-Kocsis, Security of Cyber-Physical Systems Vulnerability and Impact. Cham: Springer International Publishing : Imprint: Springer, 2020.
13. R. E. Pino, Network Science and Cybersecurity. New York, NY Springer, 2014.
14. Adams Niall M, Heard Nicholas A, and R. Patrick, Data Science For Cyber-security. World Scientific, 2018.
15. Joseph Migga Kizza, Guide To Computer Network Security. 2020.
16. M. A. Maloof and SpringerLink (Online Service, Machine Learning and Data Mining for Computer Security: Methods and Applications. London: Springer London, 2006.
17. B. B. Gupta and Q. Z. Sheng, Machine Learning for Computer and Cyber Security. CRC Press, 2019.
18. A.E. Hassanien, S. Bhattacharyya, Satyajit Chakrabarti, A. Bhattacharya, and S. Dutta, Emerging Technologies in Data Mining and Information Security. Springer Nature, 2021.
19. P. S. Yu and J. J. P. Tsai, Machine Learning in Cyber Trust: Security, Privacy, and Reliability. Boston, Ma: Springer-Verlag Us, 2009.