EPiC Series in Computing

Volume 98, 2024, Pages 150–158

Proceedings of 39th International Conference on Computers and Their Applications

AI and Cybersecurity: Collaborator or Confrontation

Collin Orner[1] and Md Minhaz Chowdhury[2]

[1,2] East Stroudsburg University of Pennsylvania, Pennsylvania, USA.

[1]corner2@live.esu.edu, [2]mchowdhur1@esu.edu

Abstract

Artificial Intelligence (AI) is and has been rapidly transforming the landscape of cybersecurity as we know it, serving as a double-edged sword. On one side, AI systems can act as your ally, doing tasks like fortifying defense mechanisms and automating complex threat detection or intrusion detection systems. Machine learning models can sift through large amounts of data, identifying anomalies that could indicate a breach or malicious activity, which is often faster and more accurate than a human could be. This capability makes it possible to proactively counteract threats, minimizing any potential cyber issues. On the other hand, the power of AI can be easily weaponized by an adversary, becoming a potential threat actor. Sophisticated cybercriminals can use AI to craft advanced evasive malware and launch automated attacks. Techniques like using machine learning from an adversary perspective allow them to design inputs specifically intended to deceive AI-powered security systems. So as AI systems become smarter, do the tools and tactics used by adversaries looking to exploit them. This duality of AI in cybersecurity is an important relevance to professionals in the field. The discipline of a cybersecurity professional is constantly evolving in response to new strategies of the adversary. Professionals must be skilled at utilizing AI's capabilities and limiting its weaknesses as it becomes more and more integrated into security infrastructure. Not only must the newest technology be used, but it must also be understood in terms of its ramifications, potential risks, and the constantly shifting dynamics between defenders and attackers. Staying ahead of the competition on the AI-enhanced cyber-warfare battlefield requires constant learning, adaptation, and persistence. In this paper, the discussion pivots around a central question: Is AI in cybersecurity a friend, a foe, or perhaps both?

Keywords— ChatGPT; Google Bard; Natural Language Processing; Machine Learning; AI; Phishing; AI Model; Malware; Chatbot

1 Introduction

AI in cybersecurity has been instrumental in reinforcing cyber threat intelligence by enabling security professionals to search for characteristics of cyberattacks, strengthen their defenses, analyze data for user authentication, and discover clues to identify specific cyber attackers [1]. It helps address various cybersecurity issues through machine learning, deep learning, natural language processing, knowledge representation and reasoning, and knowledge or rule-based expert systems modeling [2]. Despite the significant strides AI has made in cybersecurity, it remains a buzzword as the promise of completely autonomous security solutions remains unfulfilled [3]. The core capabilities of AI in cybersecurity include detection systems, cybersecurity analytics solutions for enterprises, and supporting cybersecurity through accuracy in security models [4].

The cybersecurity landscape is ever evolving, necessitating innovative solutions to counteract the increasing complexity of cyber threats [1]. AI presents myriad advantages in cybersecurity, especially in a time where cyberattacks are fast-evolving and the multiplication of devices is rapid. AI and machine learning help keep pace with cyber criminals, automate threat detection, and respond more effectively compared to conventional software-driven or manual techniques [2]. Cyber attackers are also known as hackers [5] [6] [7] [8]. Such hackers are aiming to misuse AI and machine learning models. For example, generative AIs can be misused by hackers. The fear of this has become more severe with how easy it is to create malware by ChatGPT [9] [10] [11].

The potential misuse of AI in cybercrime is also a motivating factor, especially given a significant shortage of cybersecurity professionals globally. Thus, harnessing AI responsibly and securely is crucial to combat cyber threats. Advanced malware detection techniques through AI, such as machine learning and behavioral analysis, are pivotal in identifying and mitigating malware attacks, making AI an invaluable tool in contemporary cybersecurity measures [3].

Various methodologies and frameworks are employed in leveraging AI for cybersecurity. One such methodology classifies AI use cases based on a NIST cybersecurity framework using a thematic analysis approach, focusing on the implications of AI applications in cybersecurity scenarios [4]. Microsoft's AI security risk management framework exemplifies a structured approach towards securing AI systems, implementing best practices in AI security risk management for client systems [20]. The Zero Trust Security framework is another methodology that improves organizations' ability to anticipate and thwart breaches, essential in securing proliferating threat surfaces. Additionally, novel AI-based cybersecurity methods are being promoted to improve industrial security, encompassing new theories, concepts, and architectures for AI security, addressing challenges and solutions in big data security [12].

In this paper, the discussion pivots around a central question: Is AI in cybersecurity a friend, a foe, or perhaps both? The paper presents the usefulness of AI in providing better Cybersecurity and how AI is causing new vulnerabilities to be opened in Cybersecurity. This process is like the testing of a software system where we test the software to remove bugs, and in the process, we introduce new bugs in the software system. AI is very efficient in strengthening Cybersecurity and Minimizing Vulnerabilities, at the same time. The paper is organized as follows: section 2 describes how AI emerged as an essential tool for Cybersecurity, the dual nature of AI (good and bad), relationship between AI and Cybersecurity. Section 3 describes more on the dual AI's dual role in Cybersecurity, comparison with traditional methods, empirical analysis, evidence of AI's efficacy, challenges, and ethical considerations when AI is applied in Cybersecurity.

2 Background

In the intricate landscape of modern cybersecurity, Artificial Intelligence (AI) emerges as both a formidable ally and a potential adversary. This duality is rooted in AI's application in enhancing security measures and its potential misuse by cyber criminals.

The Rise of AI in Cybersecurity

AI's integration into cybersecurity has been revolutionary, marking a significant evolution from traditional, rule-based security systems. As organizations grapple with increasingly sophisticated cyber threats, AI has become a 'force multiplier', empowering security teams with enhanced capabilities for threat detection, rapid response, and predictive analysis [4]. This shift is particularly critical given the overwhelming volume and complexity of cyber threats that human analysts alone struggle to manage effectively.

The efficacy of AI in cybersecurity is exemplified by its ability to drive speed and precision in defenses, countering the inherently rapid and precise nature of cyber-attacks [20]. Moreover, mature AI capabilities are pivotal in addressing challenges like the skills shortage in cybersecurity and the deluge of data stemming from complex infrastructure [4].

A Double-Edged Sword

AI's role in cybersecurity is not without its challenges. On one side, AI's advanced data processing and anomaly detection capabilities have become indispensable in identifying and mitigating cyber threats. This includes AI's ability to learn from patterns and predict future attacks, enhancing initiative-taking defense mechanisms. The same features that make AI invaluable in defending against cyber threats also render it a powerful tool for adversaries. Cybercriminals can exploit AI to develop more effective attacks and identify system weaknesses. Such exploits include AI-driven phishing and malware, leading to a continuous escalation in cyber warfare tactics [13] [14] [15]. Phishing is becoming ever more popular in the cybersecurity space. Phishing attacks are possible through social engineering [16]. Phishing emails aid various cyber-attacks, e.g., ransomware attacks [17]. Time series analysis and artificial immune systems are a popular method for pattern recognition [18] [19]. The increasing use of AI, including machine learning, has created a complex threat availability, where cybercriminals employ sophisticated tactics to attack AI-powered systems [2] [3].

Addressing these challenges requires a holistic approach that encompasses various methodologies and frameworks. This includes AI-powered antivirus, cyber threat intelligence, forensics, malware analysis and detection, and enhanced cyber defense mechanisms [20]. Additionally, a proactive security posture, enabled by AI, can help organizations stay resilient during attacks, reducing the adversary's presence in the environment [12].

Relationship Between AI And Cybersecurity: Cybersecurity of AI And AI for Cybersecurity

The relationship between AI and cybersecurity can be viewed through a tridimensional lens: cybersecurity of AI, AI supporting cybersecurity, and the malicious use of AI [21]. In the first dimension, the focus is on protecting AI systems themselves from being compromised. The second dimension emphasizes AI's role in enhancing cybersecurity measures, such as threat detection and response. The third dimension underscores the potential misuse of AI by cyber criminals.

3 Analysis

The integration of Artificial Intelligence (AI) in cybersecurity marks a critical juncture in the evolution of digital defense mechanisms. This development presents a multifaceted landscape where AI's capabilities are as promising as they are challenging. AI in cybersecurity is not just a technological advancement; it is a change in thinking, redefining the rules of digital security and cyber warfare. This expanded conclusion aims to explore AI's comprehensive impact on cybersecurity, highlighting its dual nature, comparisons with traditional methods, empirical evidence, challenges, ethical considerations, and prospects. As AI technology continues to advance, its role in cybersecurity is set to become even more central. Future AI systems are expected to be more sophisticated, capable of even more advanced threat detection, automated response, and the ability to predict analytics. These developments hold the promise of a more secure digital world but also necessitate continuous vigilance and adaptation to new AI-driven threats.

AI’s Dual Role in Cybersecurity

AI has become an indispensable tool in the realm of cybersecurity, offering unparalleled processing speeds and analytical capabilities. By utilizing machine learning algorithms, AI can swiftly process and analyze large amounts of data, detecting intricate patterns and anomalies that are indicative of cyber threats, a task that is nearly impossible for humans to perform with the same efficiency [22]. This level of automation and capability far exceeds the scope of traditional cybersecurity methods, which often struggle to adapt to the rapidly evolving landscape of digital threats.

Deception in cyberspace is a common scenario [23] [24] [25] [26] [27]. Deception not only can victimize humans but also AI models. AI's growing prominence in cybersecurity also presents unique challenges. Cybercriminals, leveraging an understanding of AI's functionalities, are devising increasingly sophisticated strategies to bypass AI-driven security measures. These tactics include the development of malware and cyberattacks specifically engineered to deceive AI systems, leading to incorrect threat assessments and potentially significant breaches in security defenses [28]. This adversarial use of AI creates ongoing vigilance and continuous evolution of AI strategies to maintain robust cybersecurity defenses.

The dynamic nature of AI in cybersecurity underscores the necessity for continuous development and adaptation. As AI technologies evolve, do the methodologies and tactics employed by cybercriminals, necessitating a perpetual cycle of advancement and refinement in cybersecurity strategies. This evolving landscape requires cybersecurity professionals to remain constantly vigilant and adapt their strategies to harness AI's full potential while mitigating its vulnerabilities [29] [30].

In summary, AI-powered cybersecurity is a double-edged sword. While AI strengthens defense mechanisms, it also gives rise to more advanced and elusive cyber threats. AI-driven cyber-attacks are not only more sophisticated but also more difficult to detect and counteract, requiring constant updates and refinements in AI-based cybersecurity measures [14] [15].

Comparison with Traditional Methods

The contrast between AI and traditional cybersecurity methods is stark. Traditional approaches, often limited by their static nature, are increasingly insufficient against modern, sophisticated cyber-attacks. AI, with its dynamic and adaptive learning capabilities, not only detects but also anticipates threats, offering a more comprehensive and preemptive security posture. This adaptability is crucial in an environment where cyber threats are not only growing in number but also in complexity [13] [14] [15].

Traditional cybersecurity methods often lag in their ability to effectively combat the continuously evolving tactics employed by cybercriminals. Relying primarily on static databases of known threats and predefined rules, these traditional methods can be inadequate in identifying and countering novel or complex cyber-attacks [22] [28]. This limitation often results in slower reaction times and reduced efficacy in threat mitigation, hindering the overall security posture.

AI, however, represents a paradigm shift in cybersecurity. Unlike traditional methods that remain static, AI systems are designed to learn and adapt continually. This constant evolution enables AI to identify and respond to emerging threats more effectively, ensuring a more dynamic and proactive approach to cybersecurity [28]. By constantly updating its understanding of threat patterns, AI can stay ahead of cybercriminals, offering a more robust and resilient defense against cyber-attacks.

The integration of AI into cybersecurity operations significantly enhances resource allocation efficiency. Traditional cybersecurity approaches often require extensive human intervention for threat detection, analysis, and response, leading to potential delays and increased workload on cybersecurity teams. In contrast, AI's ability to automate these processes allows for more strategic deployment of human resources, focusing on complex and nuanced cybersecurity challenges that require human insight and decision-making [29] [30].

Empirical Analysis and Evidence of AI’s Efficacy

An empirical analysis of AI in cybersecurity can encompass various performance metrics, such as the reduction in response times to security incidents, accuracy in threat detection, and effectiveness in distinguishing false positives from genuine threats [29]. By quantifying these metrics, researchers can provide concrete evidence of AI's impact on enhancing cybersecurity efficiency and effectiveness.

Data reflecting AI's impact on cybersecurity demonstrates substantial improvements in response times to security threats, often reducing the time from hours to mere minutes. This rapid response capability is crucial in mitigating the impact of cyber-attacks, as timely intervention can significantly limit the damage caused by security breaches [22] [28]. Furthermore, AI's advanced analytical abilities can lead to more accurate threat identification, reducing the incidence of false alarms and ensuring that security resources are deployed more effectively.

Another significant aspect of empirical analysis is the cost-benefit analysis of implementing AI in cybersecurity. By averting significant security breaches or swiftly containing them, AI not only prevents potential data loss and system downtime but also saves organizations from the substantial financial losses associated with these incidents. This cost-saving aspect, coupled with the efficiency gains from AI deployment, underscores the financial viability and strategic advantage of integrating AI into cybersecurity strategies [30].

Empirical studies and real-world applications underscore AI's transformative impact on cybersecurity. AI's rapid data processing and pattern recognition capabilities significantly shorten response times, a critical factor in limiting the damage from cyber-attacks. Additionally, AI's precision in identifying real threats enhances the effectiveness of security measures, leading to a more efficient allocation of cybersecurity resources and a reduction in the rate of false alarms [13] [14] [15].

Challenges and Ethical Considerations

The integration of AI in cybersecurity is laden with challenges and ethical dilemmas. The potential for biases in AI algorithms poses significant ethical concerns, as these biases can lead to erroneous threat assessments. Additionally, the rapid progression in AI technology raises the risk of over-dependence, potentially leading to a skills gap in human cybersecurity expertise. A balanced approach, emphasizing ethical AI use and maintaining human oversight, is critical [14] [15].

The integration of AI in cybersecurity, while beneficial, is not without its challenges. One of the primary concerns is the emergence of adversarial AI tactics, where cybercriminals develop advanced AI tools to create attacks that are specifically tailored to evade detection by AI-based security systems [29] [22]. This constant cat-and-mouse game between security professionals and cybercriminals necessitates ongoing updates and refinements to AI systems to ensure their effectiveness in identifying and mitigating novel cyber threats.

Ethical considerations in the use of AI in cybersecurity are also of paramount importance. Biases inherent in AI algorithms, often a result of biased training data, can lead to skewed threat assessments and discriminatory practices. This issue is particularly concerning as it can result in the misidentification of benign activities as malicious or the overlooking of genuine threats, thus compromising the integrity and effectiveness of cybersecurity measures [28] [30]. Ensuring fairness and objectivity in AI systems is therefore a critical aspect of ethical AI deployment in cybersecurity.

The risk of over-reliance on AI is another significant challenge. While AI systems offer numerous advantages in terms of efficiency and effectiveness, an over-dependence on these systems can lead to a degradation of human analytical skills in cybersecurity. This potential skills gap, resulting from an overemphasis on automated systems, may leave organizations vulnerable in situations where AI systems are less effective or fail altogether [22]. Balancing the use of AI with the cultivation of human expertise is therefore essential in developing a comprehensive and resilient cybersecurity strategy.

The role of AI in cybersecurity is undeniably complex, serving as both an invaluable ally and a potential source of new challenges [29] [28]. While AI significantly enhances the capabilities of cybersecurity systems, it also introduces complexities that require careful management and oversight. The balance between leveraging AI's strengths and mitigating its potential drawbacks is a critical aspect of modern cybersecurity strategies.

As we look toward the future of AI in cybersecurity, a balanced approach that combines the strengths of AI with an awareness of its limitations and potential risks will be essential [30]. This approach should include continuous adaptation of AI systems to evolving cyber threats, as well as a commitment to ethical considerations and the development of human expertise.

Ultimately, the effective harnessing of AI in cybersecurity will depend on a blend of automated and human-driven strategies. This combination will enable organizations to create robust, adaptable, and resilient cybersecurity infrastructures, capable of responding to both current and future cyber threats with agility and precision [22] [30].

4 Conclusion

The paper presented the usefulness of AI in providing better Cybersecurity and how AI is causing new vulnerabilities to be opened in Cybersecurity. This process is like the testing of a software system where we test the software to remove bugs, and in the process, we introduce new bugs in the software system. AI is very efficient in strengthening cybersecurity and minimizing vulnerabilities, at the same time.

AI’s role in cybersecurity will become increasingly complex and multifaceted as AI continues to evolve. Organizations must navigate this landscape with a balanced perspective, recognizing AI as both a powerful ally in enhancing cybersecurity and a potential threat vector that needs to be guarded against. The future of AI in cybersecurity will likely be characterized by continuous innovation, refinement, and an ongoing battle between its beneficial applications and its potential for misuse. AI in cybersecurity presents a paradoxical scenario of being both a friend and a foe. Its capabilities to significantly improve threat detection and response are countered by its potential exploitation by cybercriminals. This necessitates a nuanced understanding and approach towards AI in cybersecurity, emphasizing the development of robust strategies and frameworks to harness AI's benefits while mitigating its risks. AI will require constant vigilance, innovation, and adaptation to ensure it remains more of an ally than an adversary in the realm of cyber defense, as AI's role in cybersecurity continues to evolve. AI's integration into cybersecurity represents a dynamic and evolving landscape. It brings significant benefits in threat detection and response but also introduces new complexities and challenges. The effective use of AI in cybersecurity will depend on a combination of AI technological power and human expertise, ethical considerations, and the ability to adapt to an ever-changing threat landscape. AI in cybersecurity is both a powerful ally in the fight against cyber threats and a source of new challenges, requiring a specific and dynamic approach to ensure digital security and integrity.

As future research on AI and cyber security interactions, we need to improve AI capabilities in providing better and more effective cybersecurity capabilities, and how to use AI to reduce/remove vulnerabilities in cybersecurity protections.

References

[1] “How Artificial Intelligence (AI) Can Help with Cybersecurity Threats.” Fortinet, www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity.

[2] Sarker, Iqbal H. “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions - SN Computer Science.” SpringerLink, Springer Singapore, 26 Mar. 2021, link.springer.com/article/10.1007/s42979-021-00557-0.

[3] AI in cybersecurity 101 | Infosec. (n.d.). Retrieved January 31, 2024, from https://resources.infosecinstitute.com/topics/machine-learning-and-ai/ai-in-cybersecurity/

[4] Kaur, Jagreet. “Artificial Intelligence in Cybersecurity: The Advanced Guide.” Real Time Data and AI Company, Xenonstack Inc, 18 July 2023, www.xenonstack.com/blog/artificial-intelligence-cyber-security.

[5] Smith, L., M. M. Chowdhury, and S. Latif. "Ethical Hacking: Skills to Fight Cybersecurity Threats. EPiC Series in Computing, 82, 102–191." (2022).

[6] K. Guers, M. M. Chowdhury and N. Rifat, "Card Skimming: A Cybercrime by Hackers," 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 575-579, doi: 10.1109/eIT53891.2022.9813890.

[7] S. Vandervelden, M. M. Chowdhury and S. Latif, "Managing the Cyber World: Hacker Edition," 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 2021, pp. 1-6, doi: 10.1109/ICECCME52200.2021.9590870.

[8] R. Vanness, M. M. Chowdhury and N. Rifat, "Malware: A Software for Cybercrime," 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 513-518, doi: 10.1109/eIT53891.2022.9813970.

[9] Chowdhury, M. M., Rifat, N., Ahsan, M., Latif, S., Gomes, R., & Rahman, M. S. (2023). ChatGPT: A Threat Against the CIA Triad of Cyber Security. IEEE International Conference on Electro Information Technology, 2023-May, 478–483. https://doi.org/10.1109/EIT57321.2023.10187355

[10] Chowdhury, M., Rifat, N., Latif, S., Ahsan, M., Rahman, M. S., & Gomes, R. (2023). ChatGPT: The Curious Case of Attack Vectors’ Supply Chain Management Improvement. IEEE International Conference on Electro Information Technology, 2023-May, 499–504. https://doi.org/10.1109/EIT57321.2023.10187385.

[11] N. Atanassov and M. M. Chowdhury, "Mobile Device Threat: Malware," 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, 2021, pp. 007-013, doi: 10.1109/EIT51626.2021.9491845.

[12] Hindawi. “Artificial Intelligence-Based Cybersecurity Methodologies for Attack and Defense.” Hindawi, www.hindawi.com/journals/scn/si/621837/.

[13] Sridhar Muppidi, IBM Fellow, and CTO IBM Security. “AI in Cybersecurity: Yesterday’s Promise, Today’s Reality.” MIT Technology Review, MIT Technology Review, 17 Nov. 2023, www.technologyreview.com/2023/05/24/1073395/ai-in-cybersecurity-yesterdays-promise-todays-reality/.

[14] Craig, Dr. Jerry. “How Ai Will Affect Cybersecurity in 2023.” Ntiva, Ntiva, 21 Sept. 2023, www.ntiva.com/blog/how-ai-will-affect-cybersecurity-in-2023.

[15] “Ai in Cybersecurity: A Comprehensive Overview of 2023.” Machine Labs Ai, 17 June 2023, machinelabs.ai/ai-uses/ai-in-cybersecurity/.

[16] M. Mattera and M. M. Chowdhury, "Social Engineering: The Looming Threat", IEEE International Conference on Electro Information Technology, vol. 2021, pp. 56-61, May 2021.

[17] M. A. Mos and M. D. M. Chowdhury, "The Growing Influence of Ransomware", IEEE International Conference on Electro Information Technology, vol. 2020, 2020, July.

[18] Shamsi, Silvey, and Mian Adnan, "A Least Deviation Estimation Approach for Time Series Models." In Joint Statistical Meetings Proceedings. 2019.

[19] M. Minhaz Chowdhury, J. Tang and, K. E. Nygard, "An artificial immune system heuristic in a smart grid", 28th International Conference on Computers and Their Applications 2013 CATA 2013, pp. 129-132, 2013.

[20] Kumar, Ram Shankar Siva. "Best Practices for AI Security Risk Management." Microsoft Security Blog, 26 Sept. 2023, www.microsoft.com/en-us/security/blog/2021/12/09/best-practices-for-ai-security-risk-management/.

[21] AI in cybersecurity: Friend or foe? - Back End News. (n.d.). Retrieved January 31, 2024, from https://backendnews.net/ai-in-cybersecurity-friend-or-foe/

[22] Ramanpreet Kaur, et al. "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions." Information Fusion, Elsevier, 7 Apr. 2023, www.sciencedirect.com/science/article/pii/S1566253523001136.

[23] M. M. Chowdhury and K. E. Nygard, "Deception in cyberspace: An empirical study on a con man attack", IEEE International Conference on Electro Information Technology, pp. 410-415, 2017.

[24] M. Chowdhury and K. E. Nygard, "Machine learning within a con resistant trust model", Proceedings of the 33rd International Conference on Computers and Their Applications CATA 2018, vol. 2018, 2018, March.

[25] M. M. Chowdhury, K. E. Nygard, K. Kambhampaty and M. Alruwaythi, "Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm", Proceedings - 2017 International Conference on Computational Science and Computational Intelligence CSCI 2017, pp. 25-30, 2018.

[26] Chowdhury, Minhaz. "Deception in Cyberspace: Con-Man Attack in Cloud Services." PhD diss., North Dakota State University, 2018.

[27] Md Minhaz Chowdhury, K. E. N. "An Empirical Study on Con Resistant Trust Algorithm for Cyberspace." In The 2017 World Congress in Computer Science, Computer Engineering, & Applied Computing. 2017.

[29] Das, R., & Sandhane, R. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series, 1964(4), 042072. https://doi.org/10.1088/1742-6596/1964/4/042072.

[28] Sarker, Iqbal H., et al. "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions - SN Computer Science." SpringerLink, Springer Singapore, 26 Mar. 2021, link.springer.com/article/10.1007/s42979-021-00557-0.

[30] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2). https://doi.org/10.1080/23311916.2023.2272358.