International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Comparative Study of Artificial Intelligence and Machine Learning Algorithms for Cybersecurity

Sai Kiran Arcot Ramesh

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: The rapid expansion of cyberspace has been facilitated by a range of innovative networking and computing technologies, including software-defined networking, big data, and fog computing. Currently, cyber security has emerged as a paramount concern in the realm of cyberspace. The security of cyberspace has had significant effects on multiple essential infrastructures. The passive protection approach is no longer effective in safeguarding systems against emerging cyber risks, such as advanced persistent threats and zero-day assaults. So, the main objective of this study is to conduct a thorough examination of different implementations of artificial intelligence in the field of cybersecurity, encompassing activities such as identifying potential risks, responding to security incidents, and utilizing predictive analytics. The methodology employed in this study is qualitative research technique. The study emphasizes the efficacy of AI-powered solutions in strengthening the robustness of contemporary cybersecurity frameworks, based on current case studies and breakthroughs in machine learning algorithms. The paper critically examines the constraints and possible prejudices in AI systems used for cybersecurity, highlighting the significance of responsible AI methodologies. The study will be a contribution to the researchers, practitioners, and policymakers to know about the present condition of artificial intelligence (AI) in cybersecurity. It aims to encourage discussions on the efficient incorporation of AI technologies to tackle the continuously expanding challenges in the field of cyber threats.

Keywords: *Artificial Intelligence; Machine Learning; Cyber Security; Security Analysis; Risks; Threats.*

1. Introduction:

Cybersecurity encompasses a set of policies, strategies, technologies, and procedures that work together to protect the "confidentiality, integrity, and availability of computing resources, networks, software programmes, and data against malicious attacks". [1]. Cybersecurity measures can be applied across various levels, including application, network, devices, host, and data. A plethora of application tools and procedures, including "firewalls, antivirus software, intrusion detection systems (IDSs), and intrusion protection systems (IPSs)," are available for the deployment of cyber security [2]. These technologies exclusively function to prevent cyber-attacks and identify security vulnerabilities. The proliferation of internet-based technology & resolutions for real-world issues has led to an escalation in the likelihood of cyber-attacks [3]. In addition, as time progresses, organizations are faced with new types of cyber-attacks. It is imperative for them to be vigilant in order to monitor the state, identify the attacks, and mitigate them before they may impact the network or data [4].

The phrases AI and ML are sometimes used interchangeably in software development to refer to the same principles, as depicted in the Figure below.

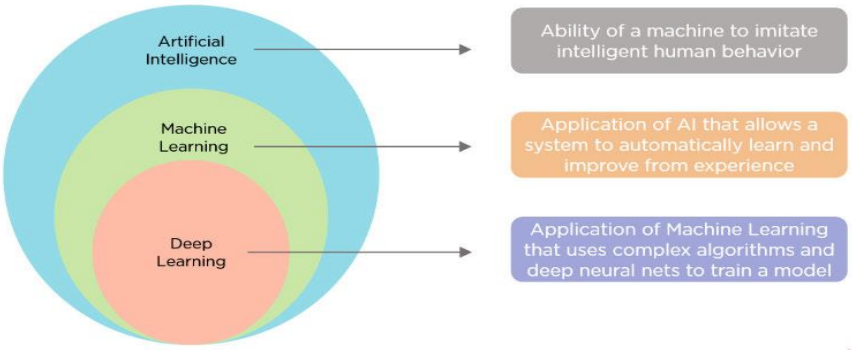

Fig 1: Relation between AI and ML [5]

Software Engineer, Department of Computer Science, Campbellsville University

The advantages of artificial intelligence in the field of cybersecurity are illustrated in the figure below.

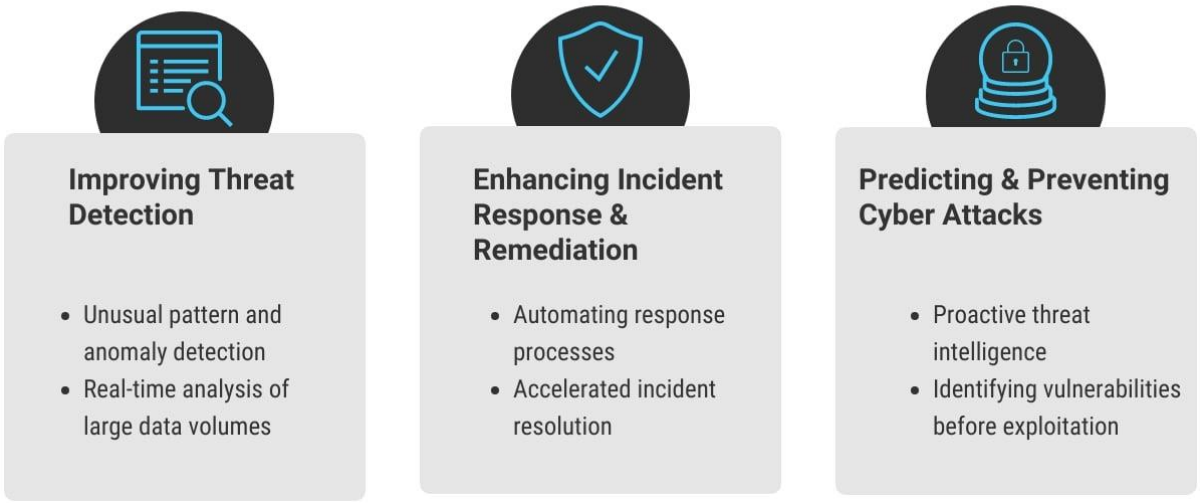

Fig 2: Benefits of AI in cybersecurity[1]

Recently, prominent cyber-attacks have highlighted the seriousness of the difficulties encountered by both organizations and people. Cybercriminals employ advanced approaches, continuously adapting their methods to surpass traditional security mechanisms. Cyber-attacks have consequences that go beyond only financial losses. They can affect national security, individual privacy, and the reliability of digital infrastructure. With the continuous advancement of technology, the potential targets for attacks increase, "highlighting the need for cybersecurity measures to stay on par with, or perhaps beyond, the cleverness of cyber adversaries. The increasing threat posed by the evolving threat landscape requires a fundamental change in cybersecurity methods. Conventional methods, while necessary, frequently fail to adequately deal with the ever-changing and intricate characteristics of contemporary cyber risks. The integration of AI into cybersecurity appears as a transformational force within this framework. AI has the capability to improve the effectiveness of current security measures and also anticipate and adjust to new threats as they arise in real-time. This study explores the uses, difficulties, and future directions of artificial intelligence in cybersecurity, with the goal of adding to the ongoing discussion on strengthening our digital protections against changing cyber threats.

2. Literature Review:

The subsequent part provides detailed information on previous publications pertaining to the utilization of AI and machine learning algorithms for cybersecurity.

Table 1: Related Works

AUTHORS AND YEARS	METHODOLOGY	FINDINGS
Husák et al., (2021) [6]	This study compared three methods in a shared intrusion detection platform, demonstrating predictive analysis's potential for cybersecurity research and operations.	Both prediction and projection approaches are useful for predictive blacklisting, with the former offering more thorough output and the latter being more adaptable.
Vemuri et al., (2023) [7]	This research showed a distinct AI system for cyber security based on this basic foundation. This study also addressed AI ethics, risk, and cyber security failure accountability.	This study recommended association between cyber security specialists, system developers, & politicians for system integration.

[1] https://www.stanfieldit.com/the-role-of-ai-and-ml-in-business-cyber-security/

Rangaraju (2023) [8]	In this paper, AI-driven security solutions were examined as a key to improving product resilience across industries.	This article showed real-world examples of how AI-driven security solutions improved product security & resilience. AI-centric security systems offer several advantages, such as improved accuracy in detecting threats, quicker response times, and increased adaptability to emerging cyber threats.
Labu & Ahammed (2024) [9]	The primary aim of this study was to investigate methods for identifying and reducing cyber risks in the future, with a particular focus on the utilization of AI and ML.	The study found that "Feedzai's AI-based software and random forest algorithms" can help financial institutions detect fraud in real-time & accurately identify lawful transactions. The Random Forest framework was most accurate at 83.94%.
Kasowaki & Emre (2024) [10]	The study examined how to strengthen cyber defences with technology advances, strong security standards, personnel training, and strict access limits.	The paper stated that a comprehensive and adaptable cybersecurity system that adapts to new threats is needed. It recommends a proactive and dynamic strategy to cyber security to combat growing cyber threats.

Research Gap: Prior research has demonstrated the importance of integrating AI technologies such as ML, natural language processing, and anomaly detection into cybersecurity frameworks to enhance the robustness of digital defensive structures. This study explores the diverse uses of AI in the field of cybersecurity, focusing on the intricate ways in which these technologies are transforming the cybersecurity environment. Furthermore, it addresses the difficulties that arise throughout this process, taking into account aspects such as the interpretability of the model, adversarial attacks, and ethical considerations. This paper examines the interdependent connection between AI and cybersecurity, shedding light on how AI goes beyond being a mere tool and instead acts as a catalyst for transforming our methods of safeguarding the digital domain.

3. Methodology:

The study employs a qualitative research methodology. Qualitative research methods are intended specifically to reveal the behaviour and viewpoint of a target audience in respect to a certain topic. Several qualitative research approaches are frequently utilised, such as "in-depth interviews, focus groups, ethnographic research, content analysis, and case study research". This research mostly utilized case studies to achieve its purpose. This text discusses real-world case studies and examples where the introduction of AI-driven security solutions has greatly enhanced the security and resilience of products. The text emphasizes the concrete benefits of implementing AI-focused security solutions, such as greater precision in detecting threats, decreased response times, and improved ability to adapt to new cyber threats.

4. Results and Discussions:

The utilization of AI and ML in the field of cybersecurity has gained significant prominence in recent times. These technologies are employed to identify potential security breaches by detecting threats, anomalies, and patterns, resulting in faster and more precise identification. Advanced Threat Intelligence: Cyber threat intelligence has advanced to offer proactive insights into prospective threats, allowing firms to predict and prepare for attacks with greater effectiveness. Ensuring adherence to regulations and protecting privacy: Stringent rules, such the "General Data Protection Regulation (GDPR)" and the "California Consumer Privacy Act (CCPA)", have compelled enterprises to give top priority to data privacy and compliance in their cybersecurity strategy. Cybersecurity is continually evolving due to advancements in technology, shifts in the threat landscape, and the necessity for enhanced defences to protect digital assets. Organizations are continuously modifying their cybersecurity strategy to effectively respond to developing threats and safeguard against developing threats.

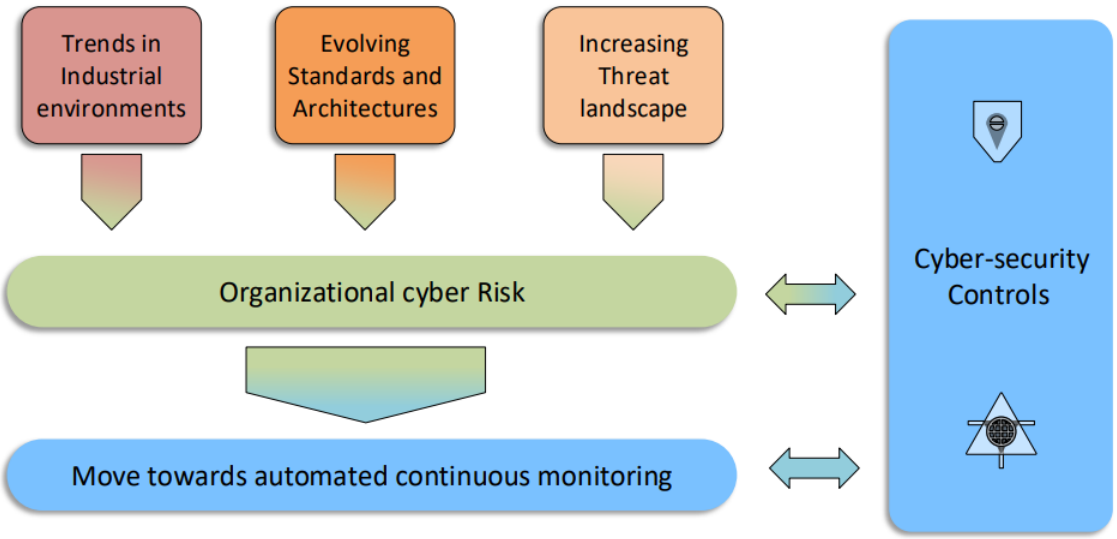

Fig 3: Evolution of Cyber Security (Rangaraju, 2023)

The integration of AI algorithms has resulted in a substantial revolution in the realm of cybersecurity, allowing enterprises to identify and address both familiar and developing threats with exceptional swiftness, precision, and effectiveness. AI systems improve threat detection in several ways:

Pattern Recognition and Anomaly Detection: Artificial intelligence algorithms demonstrate exceptional proficiency in identifying established patterns and detecting anomalies, allowing them to recognize existing risks and identify developing threats that depart from typical behaviour. Machine learning models utilize extensive data analysis, encompassing network traffic, system logs, and user behaviour, to build benchmarks of typical activities. Anomalies are identified when there are deviations from these baselines, signalling possible security vulnerabilities that require additional examination. AI-driven anomaly detection systems can accurately identify both established and emergent risks in real-time by constantly acquiring knowledge and adjusting to new patterns and behaviours.

Behavioural Analysis and User Profiling: AI algorithms utilize behavioural analysis techniques to analyse user activity and detect abnormal activities that may indicate security issues. AI-driven systems can identify abnormal behaviour patterns, such as atypical login times, unauthorized access to sensitive information, or departures from typical activity levels, by studying human interactions with digital systems. AI algorithms can proactively mitigate security risks by matching diverse data sources and detecting behavioural anomalies, thus spotting potential insider threats, compromised accounts, or unauthorized access attempts.

Predictive Analytics and Threat Intelligence Integration: AI algorithms utilize predictive analytics and integrate threat intelligence to identify and manage emerging threats before they escalate into large-scale cyber-attacks. AI-driven systems can detect developing trends, vulnerabilities, and attack vectors by analysing historical threat data, threat intelligence feeds, and external indications of compromise (IOCs). Organizations can use machine learning algorithms to forecast potential dangers by analysing historical data and threat intelligence. This enables them to take proactive measures and fix vulnerabilities before cyber attackers can exploit them.

Zero-Day Threat Detection and Adaptive Defences: AI algorithms are essential for identifying previously unknown security vulnerabilities and adjusting defensive measures in real-time to effectively respond to new and evolving threats. AI-driven threat detection systems can detect previously unidentified or zero-day vulnerabilities and exploits by monitoring code behaviour, system interactions, and network traffic patterns. AI systems can identify abnormal actions that suggest zero-day attacks by utilizing advanced methods like deep learning and heuristic analysis. This allows enterprises to promptly implement countermeasures and reduce the likelihood of serious cyber-attacks.

AI algorithms improve threat detection by utilizing pattern recognition, anomaly detection, behavioural analysis, predictive analytics, and the integration of threat intelligence. AI-driven systems enhance the overall resilience of cybersecurity defences by continuously learning and adapting to new threats, enabling companies to detect & respond to both known and emergent threats in real-time. The subsequent part presents many real-

world case studies that illustrate the efficacy of artificial intelligence in threat detection.

CylancePROTECT: An endpoint security solution, CylancePROTECT employs AI and ML algorithms to detect and halt malware threats in real-time. CylancePROTECT is capable of detecting and preventing both familiar and previously unknown malware threats by examining file properties and analysing behavioural patterns, therefore stopping them from running on endpoints. A financial services firm adopted CylancePROTECT and conducted a case study. The study found that the organization had a notable decrease in malware incidents. Specifically, 99.9% of threats were stopped before they could be executed, showcasing the efficacy of artificial intelligence in detecting threats at the endpoint level.

Darktrace Enterprise Immune System: This utilizes artificial intelligence technologies, such as unsupervised machine learning and probabilistic modelling, to identify and address cybersecurity risks in various digital contexts. Darktrace identified a complex internal attack campaign aimed at compromising critical customer data in a case study involving a multinational telecoms business. Darktrace detected abnormal behaviour patterns and recognized the compromised login information of a high-level user. As a result, it successfully stopped the unauthorized transfer of sensitive data. This demonstrates the effectiveness of artificial intelligence in detecting internal security risks and reducing the impact of data breaches.

Vectra Cognito: Vectra Cognito is a network detection and response technology that uses AI and ML algorithms to quickly identify and react to cyber assaults as they happen. A hospital firm implemented Vectra Cognito, as part of a case study undertaken by Vectra, to identify and address cybersecurity risks inside its network architecture. Vectra Cognito detected abnormal network activities that suggest a ransomware attack aimed at vital systems. Vectra Cognito successfully prevented the assault from causing extensive harm by isolating the compromised devices and shutting the ransomware communication channels. This demonstrates the efficacy of artificial intelligence in identifying and reducing sophisticated threats in intricate network environments.

Splunk User Behaviour Analytics (UBA): Splunk User Activity Analytics (UBA) use machine learning algorithms to examine user activity and identify insider threats, misuse of credentials, and unusual actions within organizational environments. Splunk UBA identified abnormal user actions linked to unauthorized login attempts and the unauthorized extraction of data in a case study involving a major financial institution. Splunk UBA utilized advanced data analysis techniques to connect different data sources and detect suspicious trends. This allowed the business to take proactive measures in investigating and addressing potential insider threats. This highlights the importance of using AI-powered user behaviour analytics in cybersecurity.

Although there are potential advantages, incorporating artificial intelligence (AI) into conventional incident response methods poses numerous problems and factors to consider. The factors encompassed in this category are: Data Quality and Availability, Interoperability and Integration. Issues related to ethics, privacy, and the collaboration between humans and machines.

5. Conclusion:

"Secure by Artificial Intelligence" signifies a significant change in strengthening product security by using AI-powered security measures. Integrating Artificial Intelligence provides numerous benefits in improving the identification of risks, capacity to respond, and overall ability to withstand emerging cyber threats. This summarizes the importance and consequences of implementing AI-powered security solutions and their revolutionary effect on the security of products. The implementation of AI-powered security solutions radically transforms the conventional reactive approach to cybersecurity. Through the utilization of “machine learning, predictive analytics, and automated response systems, organizations may proactively identify, avoid, and mitigate possible dangers” before they become a reality. By taking a proactive approach, response times are greatly reduced and the effect of security incidents is limited. This helps protect digital assets and maintain user trust.

AI-driven security measures that incorporate privacy-preserving solutions are designed to satisfy the crucial requirement of safeguarding sensitive user data. These solutions guarantee strong security measures while also adhering to privacy standards, thereby promoting user trust in the reliability and secrecy of their evidence. The variety and efficiency of AI-driven security measures are demonstrated by their capacity to accommodate to varying security needs across numerous sectors, regardless of industry.

References

[1] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.

[2] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In *2018 10th international conference on cyber Conflict (CyCon)* (pp. 371-390). IEEE.

[3] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *Ieee access*, *6*, 35365-35381.

[4] Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*(10), 2823-2836.

[5] Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine learning and deep learning approaches for cybersecurity: A review. *IEEE Access*, *10*, 19572-19585.

[6] Husák, M., Bartoš, V., Sokol, P., & Gajdoš, A. (2021). Predictive methods in cyber defense: Current experience and research challenges. *Future Generation Computer Systems*, *115*, 517-530.

[7] Vemuri, N., Thaneeru, N., & Tatikonda, V. M. (2023). Securing Trust: Ethical Considerations in AI for Cybersecurity. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 167-175.

[8] Rangaraju, S. (2023). Secure by Intelligence: Enhancing Products with AI-Driven Security Measures. *EPH-International Journal of Science And Engineering*," *9*(3), 36-41.

[9] Labu, M. R., & Ahammed, M. F. (2024). Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning. *Journal of Computer Science and Technology Studies*, *6*(1), 179-188.

[10] Kasowaki, L., & Emre, B. (2024). *Fortifying Cyber Defenses: Tactics for Secure Digital Environments* (No. 11702). EasyChair.