EasyChair Preprint

№ 14275

Artificial Intelligence in Cybersecurity

Ghadeer Zidan Suleiman

August 2, 2024

Artificial Intelligence In Cybersecurity

Ghadeer Zidan Suleiman
Prince Hussein bin Abdullah College of Information Technology
Irbed, Jordan
ghadeersuliman96@gmail.com

Abstract: This review paper examines the role of artificial intelligence (AI) in advancing cybersecurity. The text explores several AI methodologies, including machine learning, deep learning, and expert systems, and their applications in detecting risks, preventing disruptions, and ensuring data security. The analysis emphasizes the advantages of AI-driven cybersecurity solutions, such as the ability to efficiently process large amounts of data and identify patterns that indicate possible security weaknesses. Regardless, the material also discusses the limitations and ethical considerations associated with the use of AI in cybersecurity, highlighting the need for a balanced strategy that integrates technological advancement with human expertise and supervision.

Keywords: Cybersecurity, Artificial Intelligence (AI), Machine Learning (ML), Expert system (ES), Deep learning (DL), IOT, HLCSM, NIST

I. INTRODUCTION

Artificial intelligence (AI) is a branch of computer science that focuses on developing intelligent agents, to achieve this goal, machines need to learn precisely, which means they must be trained by learning algorithms. AI methods rely on algorithms but can also use big data and massive computing to learn through brute force. AI works in three ways: assisted intelligence, augmented intelligence, and autonomous intelligence. which are systems capable of independent reasoning, learning, and decision-making. Artificial intelligence has many applications in many domains such as healthcare, finance, manufacturing, and, more recently, cybersecurity [1].

In cybersecurity, Artificial intelligence (AI) is a fascinating technology that may offer advanced analysis and insight to defend against constantly changing assaults. It accomplishes this by rapidly processing large volumes of data and monitoring different types of cyber threats. technology is becoming more common to include technology into cybersecurity in order to automate security duties or assist human security teams[2].

Cybersecurity encompasses the use of many strategies, techniques, and resources to safeguard systems against potential risks and weaknesses, while efficiently delivering accurate services to consumers[3].

Cyber security aims to mitigate dangers to the greatest extent feasible and promptly and efficiently fulfill the demands of detecting, responding to, and recovering from incidents [3].

Expert system (ES): also known as knowledge-based systems, consist of a repository of information and an inference engine that enables logical reasoning and problem-solving. Their problem-solving talents consist of two separate methodologies: case-based reasoning, which entails utilizing previous problems and applying their solutions to new ones, and rule-based reasoning, which depends on expert-defined standards to handle challenges. Case-based reasoning involves evaluating previous scenarios and adjusting answers as needed, whereas rule-based reasoning utilizes rules that consist of a condition and a corresponding action. Rule-based systems do not possess the capacity to autonomously acquire new rules or modify existing ones, in contrast to case-based systems. Expert systems (ESs) can be employed to offer decision-making support in the field of cyberspace by analyzing modified data from security systems to determine the existence of hostile network or system activity. They possess the capacity to perform live monitoring in digital environments and deliver alert notifications and relevant information for security professionals to select appropriate measures [1].

Machine learning (ML): refers to a collection of techniques that enable computers to acquire knowledge and improve their performance without the need for explicit instructions or programming. It facilitates the identification and formalization of data principles inside systems, enables learning from data, and enhances performance based on experience. Machine learning employs statistical techniques to extract information, identify patterns, and make inferences. It may be categorized into three main types: supervised learning, unsupervised learning, and reinforcement learning. Common machine learning techniques used in cybersecurity are decision trees, support vector machines, Bayesian algorithms, and ensemble learning [1].

Machine learning algorithms have the ability to evaluate large amounts of data in real-time, allowing them to detect possible security breaches. Successful cybersecurity relies on the essential elements of collaboration, technical innovation, and user awareness. Nevertheless, the use of AI and ML technologies brings both progress and novel risks, as unscrupulous individuals exploit them for the purpose of launching attacks and engaging in phishing activities. Ensuring the ethical application of AI in cybersecurity is crucial for preventing its exploitation. Artificial intelligence (AI) aids researchers in comprehending the intricacies of ecosystem dynamics and providing valuable insights for conservation initiatives. Artificial intelligence (AI) integrated transportation systems enhance route optimization, minimize emissions, and enhance operational efficiency [4].

Deep learning: also known as deep neural learning, utilizes data to train computers to accomplish tasks that humans can do. Deep learning algorithms mimic the cognitive processes of the human brain to evaluate data and produce patterns that influence decision-making. They have the ability to carry out iterative tasks, making alterations to the job to enhance the outcomes. Cybersecurity utilizes deep learning techniques to handle the vast volumes of data that are gathered daily. Deep learning methods enable the implementation of supervised,

unsupervised, and reinforcement learning approaches. Xu et al. conducted a case study to assess the efficacy of deep learning in identifying network intrusions. This showcases the capabilities of AI-driven technologies to do instantaneous analysis and precisely detect harmful network traffic [1,6].

IOT: The term "Internet of Things" encompasses the interconnected network of devices and the technology that enables communication between these devices and the cloud, as well as between the devices themselves. An essential aspect of the future of cybersecurity centers on the Internet of Things (IoT). The Internet of Things (IoT) consists of an extensive network of networked objects, ranging from intelligent appliances and wearable gadgets to industrial systems and essential infrastructure. Although the Internet of Things (IoT) offers unparalleled ease and automation, it also brings about weaknesses that may be easily exploited by malevolent individuals. Inadequate security measures, weak authentication mechanisms, and subpar device management can render IoT systems susceptible to attacks. To counter these risks, future cybersecurity strategies must prioritize robust encryption protocols, regular software updates, and enhanced security measures tailored specifically for IoT devices [2].

A. *The Human-in-the-Loop Cyber Security Model*

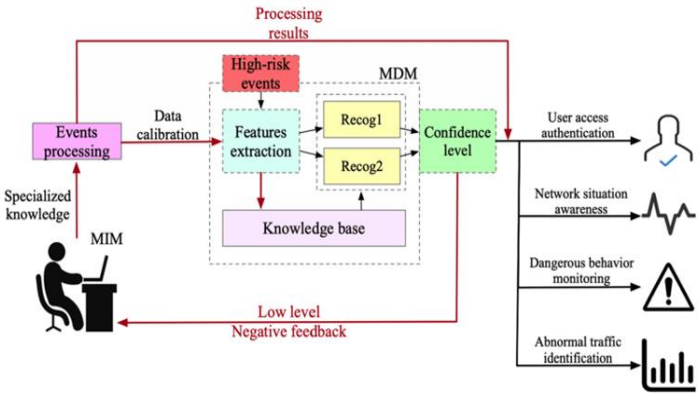

Figure 1: Human-in-the-Loop Cyber Security Model (HLCSM)

Figure 1 shows The Human-in-the-Loop Cyber Security Model (HLCSM) is a novel approach that seeks to combine human experience with machine intelligence in the realm of cyber security. Artificial intelligence (AI) technology provides significant advantages in several applications, despite its inherent constraints. The model is divided into two subordinate modules: the Machine Detection Module (MDM) and the Manual Intervention Module (MIM). The main role of MDM is to proactively avoid and detect cyber issues, while also ensuring data readiness and extracting pertinent attributes. MIM functions as a supplementary entity, overseeing events by the application of experienced knowledge. The Confidence Level Module (CLM) is designed to build a smooth link between MDM and MIM, enabling efficient collaboration. The CLM combines the results and determines the Confidence Level, therefore maximizing human resources and reducing the time needed for identification. However, when the Confidence Level is low, experts carefully examine the information to minimize the likelihood of errors. The primary goal of the HLCSM is to augment the proficiency and reliability of cyber security systems by combining human knowledge with machine intelligence. However, it is essential to recognize that the best results can only be achieved by integrating AI with human-in-the-loop technology [3].

B. *NIST : The National Institute of Standards and Technology*

Figure 2: NIST cybersecurity framework.

Figure 2 shows The National Institute of Standards and Technology (NIST) is a voluntary framework that aims to assist enterprises in comprehending, controlling, and mitigating cybersecurity risks. The framework comprises four components: Functions, Categories, Subcategories, and Informative references. The initial two tiers of the framework, comprising of 5 cybersecurity functions and 23 solution categories, offer a complete perspective on cybersecurity management. The suggested taxonomy incorporates an additional tier that delineates AI-driven applications that align with each level of the framework. This taxonomy offers a precise and straightforward classification of current research on AI for the field of cybersecurity, making it easy to understand and navigate [2].

II. RESEARCH METHODOLOGY

This review paper's methodology involves conducting a comprehensive analysis of contemporary literature published between 2020 and 2024. The research will include an analysis of the benefits, limitations, strengths, and risks of AI-based cybersecurity approaches. explores the use of artificial intelligence (AI) in cybersecurity, specifically in the areas of user access authentication, network state knowledge, hostile activity monitoring, and anomalous traffic recognition. This paper examines the application of artificial intelligence (AI) in intrusion detection systems (IDS) and examines the ethical consequences linked with it. The research categorizes AI approaches such as machine learning and deep learning, along with their applications in threat detection, intrusion detection systems (IDS), and real-time data processing.

What is the crucial function of Artificial Intelligence (AI) in cybersecurity, specifically looking at how it is used in areas such as identifying threats, assessing vulnerabilities, responding to incidents, and doing predictive analyses [4]?

What is the paradoxical nature of using AI in cybersecurity, where AI can be used both for public good and for harm [5]?

What is the potential of Artificial Intelligence (AI), specifically sophisticated language models such as ChatGPT, in improving the capacity of Intrusion Detection Systems (IDS) to recognize, categorize, and detect abnormal network traffic and cyber-attacks [6]?

What is the significance of ML in the field of cybersecurity, with a special emphasis on the identification of threats and the implementation of protective measures [7]?
What are the impacts and limitations of artificial intelligence in cybersecurity [8]?

III. LITERATURE REVIEW

The study by Katanosh Morovat and Brajendra Panda,2020 explains that the growing complexity of cyberattacks has required the creation of sophisticated cybersecurity methods. AI technologies have been employed to protect systems from a range of threats, including effective defensive capabilities to identify and respond to malware attacks, network intrusions, phishing and spam emails, and data breaches. AI techniques, including learning algorithms, expert systems, machine learning, deep learning, and biologically inspired computation, are crucial topics in the field of cybersecurity. Artificial Intelligence (AI) can effectively analyze vast quantities of data and derive insights from previous security breaches to anticipate forthcoming cyber threats. Nevertheless, artificial intelligence (AI) is constrained by factors such as the need for extensive data, frequent occurrence of false alarms, and susceptibility to possible assaults. Scientists have devised techniques to categorize and identify malicious software by utilizing approaches such as data mining and machine learning. Current research has mostly concentrated on using deep learning architectures to identify sophisticated malicious software. Artificial intelligence can greatly enhance data and application security in the future. However, there are ongoing worries over the dependability and potential risks linked with AI.[1]

A study conducted by Nicolas Camacho,2024 Artificial intelligence systems can rapidly evaluate large amounts of data to detect unusual patterns that may indicate possible security breaches. These technologies allow enterprises to take proactive measures to prevent hazards and protect sensitive information. Nevertheless, the utilization of AI in cybersecurity also presents ethical and privacy concerns, requiring a measured approach to its adoption. This study provides a thorough analysis of the advantages, restrictions, and ethical considerations of artificial intelligence (AI) in the field of cybersecurity. It highlights the need of achieving a harmonious equilibrium between technological advancement and ethical obligations. The trajectory of cybersecurity is shaped by the widespread use of digital technology, such as the Internet of Things (IoT), which exposes potential weaknesses that may be exploited by malevolent individuals. Future cybersecurity policies should give top priority to implementing strong encryption methods, ensuring frequent software upgrades, and implementing better security measures designed particularly for Internet of Things (IoT) devices. Effective collaboration among manufacturers, developers, and cybersecurity specialists is crucial to guarantee that IoT devices are developed with security as a primary consideration right from the beginning.[4]

A study conducted by Roba Abbas and colleagues, 2023 highlights the contradictory characteristics of AI in cybersecurity, presenting several challenges, such as its inherent fallibility, its role within a larger socio-technical framework, the potential negative consequences of unregulated AI, and concerns over the accuracy and fairness of data. Understanding the complex socio-technical system and the potential risks associated with AI in cybersecurity is crucial, as mentioned in the conclusion of the research. The statement emphasizes the need for highly skilled professionals in the areas of cybersecurity and risk management, while also emphasizing the need to maintain a balance between technology, ethics, and regulation. When integrating AI into cybersecurity, it is essential to thoroughly evaluate the characteristics of the data, potential risks, and the probability of unforeseen consequences [5].

This study by Michal Markevich and Maurice Dawson, 2023, examines the potential of Artificial Intelligence (AI) to improve intrusion detection systems (IDS) in the cybersecurity domain. This demonstrates that artificial intelligence (AI) is a crucial asset in enhancing the accuracy of intrusion detection systems (IDS) in recognizing and responding to cyber-attacks. However, the study also highlights the limitations and challenges of integrating artificial intelligence (AI) into intrusion detection systems (IDS), such as the complexity of calculations and the potential for biases in the training data. Deploying sophisticated language models like ChatGPT can enhance cybersecurity measures, but it is crucial to tackle these issues to offer a more robust defense against complex cyber threats. The study indicates that artificial intelligence (AI) can improve the precision of intrusion detection systems (IDS). However, it also faces challenges like as inaccurate positive and negative results, intricate computational demands, limitations in resources, and worries about data privacy [6].

Another research by Ugochukwu Okoli et al,2024 examines the importance of Machine Learning (ML) in cybersecurity, specifically its applications in threat detection and defense systems. The versatility of machine learning enables it to detect nuanced patterns in extensive datasets, rendering it highly valuable in the realm of cyber warfare. The paper highlights the necessity of adopting a holistic strategy that integrates technology with ethical issues, blending human expertise with machine intelligence. Additionally, it explores the difficulties and advantages of ensuring cybersecurity in power grids and maritime industries, as well as the influence of the Internet of Things (IoT) on cyber threats. The report asserts that the integration of machine learning into cybersecurity is essential for organizations to effectively counteract the ever-changing threats [7].

The latest research in this article by Miraj Ansari and colleagues,2022 examines the significant impact of AI on cybersecurity as it enables intelligent systems and robots to mimic human behavior. AI platforms enable the deployment

of machine learning and deep learning models in businesses, therefore enhancing data security, reducing reliance on cybersecurity experts, and lowering costs associated with maintenance and auditing. Artificial Intelligence (AI) improves the effectiveness of network intrusion detection, vulnerability management, and data center security. During the ongoing COVID-19 pandemic, there has been a consistent increase in investments in artificial intelligence (AI), which allows for the continuous monitoring of vulnerability databases in real-time. However, artificial intelligence (AI) does have limitations, including the potential for manipulation by unscrupulous persons, the impossibility to completely replace human expertise, and difficulties in adapting to constantly evolving threats. The high costs involved in implementing AI-powered cybersecurity solutions and the possibility of hostile actors reverse engineering AI systems highlight the need for continuous improvements in system security [8].

IV. CONCLUSION

The integration of artificial intelligence (AI) technologies within cybersecurity has demonstrated significant potential in enhancing security measures, automating detection processes, and improving response times. Machine learning, deep learning, and expert systems are sophisticated techniques that may be used to analyze and address new cyber risks. Nevertheless, it is important to utilize artificial intelligence in this field using ethical and responsible methodologies. This needs a meticulously designed strategy that combines human knowledge with artificial intelligence. In order to enhance the cybersecurity landscape, it is essential for humans and AI-driven systems to work together in a synergistic manner to protect crucial infrastructure and sensitive information from advanced threats.

REFERENCES

[1] Morovat, K., & Panda, B. (2020, December). A survey of artificial intelligence in cybersecurity. In *2020 International conference on computational science and computational intelligence (CSCI)* (pp. 109-115). IEEE.

[2] kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion , 97* , 101804

[3] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25.

[4] Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.

[5] Michael, K., Abbas, R., & Roussos, G. (2023). AI in cybersecurity: The paradox. IEEE Transactions on Technology and Society, 4(2), 104-109.

[6] Markevych, M., & Dawson, M. (2023, July). A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). In *International conference Knowledge-based Organization* (Vol. 29, No. 3, pp. 30-37).

[7] Okoli, U.I., Obi, O.C., Adewusi, A.O., & Abrahams, T.O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews , 21* (1), 2286-2295.

[8] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: a literature review. *International Journal of Advanced Research in Computer and Communication Engineering*.