IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MACHINE LEARNING IN CYBERSECURITY: HARNESSING AI FOR DEFENSE

[1]Anwar Hossain, [2]Roise Uddin, [3]Abdus Sobur, [4]Biswajit Chandra Das

[1]Graduate Student, [2]Graduate Student, [3] Graduate Student, [4]Bachelor Student

[1]Computer and Information Systems Security Cybersecurity Concentration
California State University San Bernardino, USA

[2]Computer and Information Systems Security Cybersecurity Concentration
California State University San Bernardino, USA

[3]Masters of Information Technology
Westcliff University, USA

[4]Department of Computer Science
Los Angeles City College,

Abstract: The escalating cost of cyberattacks demands a paradigm shift in cybersecurity strategies used by organizations. Traditional methods, often reactive and data-limited, struggle to keep up with the ever-growing sophistication of cyber threats and the vast volumes of data organizations produce. That's why the use of cutting-edge technologies such as Artificial Intelligence (AI) and Machine Learning (ML) if crucial to preventing cyberattacks in this day and age. By leveraging AI and ML, organizations can analyze massive datasets in real-time, identifying subtle patterns and anomalies indicative of imminent attacks. This proactive approach shifts the focus from simply reacting to breaches to predicting and preventing them altogether. AI and ML also enable the automation of time-consuming tasks, which gives security teams more time to focus on strategic initiatives and tasks that require critical thinking. AI and ML algorithms also go beyond detecting known threats as they can effectively detect and combat the newest malware variants. Despite the many benefits of integrating AI into security tools, security teams need to carefully consider its ethical and technical challenges. Addressing these challenges requires adopting practices such as using diverse and high-quality data for effective training and ensuring the interpretability of complex models. Additionally, navigating the legal and ethical landscape surrounding data privacy and governance regulations is essential.

Index Terms - Enhancing Cybersecurity by Artificial Intelligence, Monitoring Phishing Detection, Over control on Networking by AI.

I. INTRODUCTION

The cost of dealing with cyber-attacks has been escalating over the years, largely due to the increasing volume and value of data. The increasing value of data is the reason the cost of managing cybercrime has been escalating over the years. For instance, the global average cost of a data breach in 2023 was $4.45 million, marking a 15% increase compared to 2020 [1]. In the US, this cost was even higher at $9.48 million, primarily because attackers deem the data of US residents more valuable than that of most other countries [2].

The growing sophistication of cyber threats has revealed vulnerabilities in traditional defense mechanisms [3]. Traditional security solutions, which often rely on manual intervention and predefined rules, struggle to keep pace with the dynamic nature of today's cyber threats [3]. They are hindered by their inability to adapt

to new, unknown threats and their dependence on extensive human resources [3]. This is where Machine Learning (ML) and Artificial Intelligence (AI) come into play.

AI and ML offer a paradigm shift in how we approach cybersecurity [4]. By leveraging ML and AI, we can transition from a reactive to a proactive defense strategy. These technologies can learn from past incidents, adapt to evolving threats, and even predict future attacks, offering a robust and resilient defense mechanism [4]. A recent study by IBM shows that organizations that incorporate AI into their cybersecurity strategies can save an average of $1.76 million annually compared to those that don't [5].

The use of AI and ML in cybersecurity is even more critical today as we are now in the era of generative AI, which enables attackers to create more realistic phishing attacks [6]. Organizations need to devise ways to counter such attacks by using AI more effectively and aggressively than the attackers [6].

The purpose of this paper is to explore how organizations can harness the power of AI and ML to enhance their cybersecurity defenses. We aim to provide a comprehensive overview of how these advanced technologies can be utilized to fortify cyber defenses, analyze their strengths and weaknesses, and the best practices to get the best out of them.

Machine Learning (ML) and Artificial Intelligence (AI) offer a more dynamic approach to cybersecurity. The use of AI and ML in security tools such as Security Information and Event Management (SIEM) systems has been ongoing since at least 2015 [9]. Modern SIEMs, such as Splunk, leverage the power of AI and cloud resources to analyze massive amounts of logs in almost real time, allowing security teams to be notified about potential security incidents faster [9]. Besides SIEMs, several other security tools, such as Intrusion Detection Systems (IDS), also use AI to analyze behavioral patterns and detect anomalies [10].

This paper will further explore the use of AI and ML in cybersecurity, including a comprehensive overview of its benefits, shortcomings, and the best practices organizations can implement to achieve the best results from these technologies. We will also explore how new technologies, such as generative AI, can be leveraged to further enhance the security posture of organizations. We hope that this paper will contribute to the ongoing discourse on this important topic and inspire further research in this area.

BACKGROUND

The evolution of technologies, such as the Internet, has brought several benefits, including increased connectivity, access to information, and improved efficiency across various sectors. However, it has also given rise to new challenges, particularly in the realm of cybersecurity [7]. As our reliance on digital technologies grows, so does the volume of data we generate and store online.

This data, often sensitive and valuable, has become a prime target for cybercriminals who are willing to do whatever it takes to gain access to it [8]. Traditional security solutions cannot keep up with the ever-increasing volumes of data and the increasingly sophisticated cyber threats [3]. These measures are mainly effective against known threats but struggle when faced with new, unknown threats. The use of AI and ML in cybersecurity has helped address most of the shortcomings of these older technologies [6].

AI AND MACHINE LEARNING

Gartner defines AI as the application of advanced analysis and logic-based computing techniques to interpret events, support and automate decisions, and take action [11]. AI-powered systems are capable of performing complex tasks that historically only a human could do, such as reasoning, making decisions, or solving problems. The term "AI" is used as an umbrella term that encompasses a wide variety of technologies, including machine learning, deep learning, and natural language processing (NLP).

According to Gartner, ML is an analytical discipline that applies mathematical models to data to extract knowledge and find patterns that humans would likely miss [11]. It is a subfield of artificial intelligence that uses algorithms trained on data sets to create models that enable machines to perform tasks that would otherwise only be possible for humans. In cybersecurity, such tasks include anomaly detection, behavior analysis, malware analysis network logs analysis, and more.

THE ROLE OF AI AND ML IN CYBERSECURITY

Phishing Detection

Phishing involves the attacker impersonating a trustworthy entity to deceive victims into providing sensitive information or clicking on malicious links [12]. Traditional phishing detection methods often rely on rules-based filtering or blacklisting, which can only identify and block known phishing emails [12]. AI and ML offer a more dynamic and proactive approach to blocking phishing attacks in the following ways;

- **Content and Structure Analysis:** AI-based phishing detection solutions use machine learning algorithms to analyze the content and structure of emails [13]. These algorithms are trained on a vast amount of data, which includes both phishing and non-phishing emails. Based on this training, they can easily learn to detect patterns and anomalies in the email data that are indicative of a phishing attack.
- **Behavior Analysis:** AI-based solutions can also analyze user behavior when interacting with emails [14]. For instance, if a user clicks on a suspicious link or enters personal information in response to a known or suspected phishing email, AI-based solutions can flag that activity and alert security teams to take action.

Malware Detection

Unlike traditional antivirus software that relies on signature-based detection, ML and AI can identify both known and unknown malware threats [15]. The AV-TEST Institute registers over 450,000 new malware and potentially unwanted applications (PUA) every day [16]. A significant chunk of this malware may not be detected by traditional anti-virus tools in real-time. This is where using AI and ML-powered security tools becomes crucial. Here is how AI-powered detect malware.

Signature-Based Detection vs. AI-Based Detection

With signature-based detection, a file is compared to a database of known malware signatures to determine if it contains malware. If there's a match, the file is flagged as malicious. This technique, however, is only effective against known malware variants and can be easily bypassed by slightly modifying the malware to evade detection [17].

On the other hand, AI-based solutions use machine learning algorithms to analyze large amounts of data and identify patterns and anomalies that are indicative of malicious behavior [17]. This allows AI to detect new and unknown malware variants that may be missed by traditional antivirus software. The only drawback with using this technique is that it can sometimes yield lots of false positives. However, the accuracy of these tools is starting to improve as ML algorithms continue to get smarter.

Static Analysis and Dynamic Analysis

Static analysis involves debugging by examining source code before a program is run. It's done by analyzing a set of code against a set (or multiple sets) of coding rules [18]. The static analysis addresses weaknesses in source code that might lead to vulnerabilities. In the context of malware, static analysis involves examining the characteristics of a file without executing it. It looks at features such as file size, file structure, and embedded code to identify patterns and anomalies that might indicate the file is malicious.

On the other hand, dynamic analysis involves testing and evaluation of a program based on execution [18]. In the context of malware detection dynamic analysis involves observing the behavior of a file when it is executed. It can monitor system-level activities, such as file system modifications, network traffic, and changes to the system registry to identify patterns and anomalies that might indicate the file is malicious. Dynamic analysis is particularly useful for detecting unknown malware variants.

Endpoint Security

Endpoint security involves the protection of endpoints, or end-user devices like computers, laptops, and mobile devices, within a network [19]. These endpoints serve as points of access to an enterprise network and create points of entry that can be exploited by malicious actors. AI and ML security solutions secure end-point devices using the following techniques:

- **Behavior Analysis:** AI-based endpoint security solutions use machine learning algorithms to analyze endpoint behavior and detect potential threats [9]. These algorithms can learn from vast amounts of data to detect patterns and anomalies that indicate a threat. For example, if a device starts sending out large amounts of data to an unknown server, the AI system could flag this as potential data exfiltration and alert the security team in real-time.
- **Adaptability:** One of the key advantages of AI-based endpoint security solutions is their ability to adapt and evolve over time. As cyber threats become more sophisticated, AI algorithms can learn from new data and identify new patterns that indicate potential threats [19]. This enables AI-based endpoint security solutions to provide better protection against new and unknown threats than traditional antivirus software.
- **Preventing Unauthorized Access:** AI-based endpoint security solutions can also block unauthorized access attempts and prevent attackers from gaining access to sensitive data [19]. They can identify suspicious login attempts, such as multiple failed login attempts or logins from unusual locations or devices, and take action to block these attempts.

Network Security

AI and ML are increasingly being used to enhance network security. They offer several advantages over traditional methods, including the ability to analyze large volumes of data, identify patterns, and make predictions in real time. Security tools that use AI and ML secure networks in the following ways;

- **Monitoring Networks for Suspicious Activity**: AI algorithms can be trained to monitor networks for suspicious activity. This includes identifying unusual traffic patterns and detecting devices that are not authorized to be on the network [20]. For example, if a new device is detected on the network that hasn't been authorized by the IT department, the AI system can flag it as a potential security risk and block it or send an alert to the security team.

- **Anomaly Detection**: Anomaly detection involves analyzing network traffic to identify patterns that deviate from the norm. By analyzing historical traffic data, AI algorithms can learn what is normal for a particular network and identify suspicious traffic [20]. This can include unusual port usage, unusual protocol usage, or traffic from suspicious IP addresses.

Handling Duplicative Processes

AI-powered cybersecurity tools can handle monotonous and repetitive security, which can be tedious and time-consuming for human analysts. For example, AI can be used to automate the process of scanning logs for signs of suspicious activity, a task that would be extremely time-consuming for a human analyst using traditional security tools [21]. AI can also detect and prevent basic security threats regularly. It can be trained to recognize patterns associated with different types of threats and can automatically take action to prevent these threats from causing harm. This includes tasks such as identifying and blocking malicious IP addresses, detecting and quarantining malware, and identifying potential security holes in a network.

Eliminating Time-Consuming Tasks

AI can also eliminate time-consuming tasks that are typically done manually by human experts. For example, AI can scan vast amounts of data to identify potential threats. This includes analyzing network traffic, user behavior, and system logs to identify patterns that may indicate a security threat [22]. AI can also reduce false positives by filtering out non-threatening activities. False positives, or alerts that turn out to be harmless, can be a major source of frustration for cybersecurity teams. They can lead to wasted time and resources and can cause teams to become desensitized to alerts, potentially leading them to overlook real threats. By accurately distinguishing between threatening and non-threatening activities, AI can help teams focus their attention on the most serious threats.

Compliance with regulations

AI and ML tools can also enable organizations to effortlessly comply with cybersecurity-related regulations in their jurisdiction in the following ways;

- **Automating compliance tasks:** AI can automate many compliance tasks that are labor-intensive and time-consuming [23]. Such tasks can include analyzing and accurately interpreting regulatory documents to decipher their applicability to an organization. This help reduce costly compliance errors by providing a more systematic and efficient approach to compliance management.
- **Assessing Impact and Implementing Changes:** AI tools can be used to compare requirements of regulations to internal policies, standards, and procedures, accelerating gap assessments and compliance analyses [23]. It can also be used to update the policies, standards, and procedures to comply with new regulatory requirements.
- **Timely updates on regulatory changes:** AI tools can be programmed to continuously monitor and scan a wide array of regulatory databases, websites, and official gazettes [23]. These tools can then provide real-time alerts on regulatory changes. As soon as a new regulation or amendment is published, the AI system can notify the relevant teams within the organization to ensure they are always up-to-date with their compliance status and can quickly address any issues that arise.

Challenges of using AI and ML in cybersecurity

Despite offering several benefits over traditional security solutions, AI and ML have some shortcomings that organizations need to be aware of and address. Here are some of these challenges;

Data Quality and Availability

Effective machine learning applications in cybersecurity depend on the availability of diverse and high-quality datasets [24]. However, the quality of data fed into these models is often not guaranteed and can lead to undesirable results. For instance, when developing an AI-based system to detect phishing emails, a large dataset of emails, including both phishing and non-phishing examples is needed.

If the organization only has access to a small number of phishing emails, or if the phishing emails in their dataset are all very similar, the AI system might not learn to accurately identify phishing emails in the real world. In the end, this can limit the system's ability to detect some phishing attacks that might go unnoticed by the security team. Training the ML models of insufficient data can also lead to lots of false positives.

Interpretability and Explainability

Understanding the predictions made by machine learning models is crucial in cybersecurity. However, the complexity of these models often leads to a lack of interpretability, making it challenging to trust the decisions they make [25]. This issue becomes even more critical when the model's decisions have significant implications on people's lives and privacy. For instance, an AI system could flag certain patterns of network traffic as potential threats based on its training data. However, due to the complexity of the AI model, it might be challenging for the cybersecurity team to understand why certain patterns of network traffic were flagged as threats.

Computational Resources and ROI

Training and deploying complex AI models requires substantial cloud computational power, which can pose a challenge for organizations with limited resources. The ever-changing threat landscape requires continuous model updates, further taxing computational resources. Evaluating the ROI of these computation costs can be a challenge to organizations [26]. That's why it is crucial for organizations must carefully weigh the potential benefits and costs before investing in AI cybersecurity solutions.

Legal and Ethical Concerns

Striking a balance between security and user privacy can be challenging, and organizations often face numerous legal and ethical dilemmas when using AI-powered security tools [27]. The need for robust data protection measures and adherence to data governance norms is crucial for maintaining user trust and compliance with existing laws, ensuring the ethical use of technology.

For instance, organizations operating in Europe must comply with regulations such as the GDPR, which requires that user data is collected with consent, stored securely and used for the appropriate purposes. Such regulations may make it harder to collect enough data that ML models need to gain the understanding required to solve complex security problems.

Skills and Expertise

Implementing and managing AI for cybersecurity requires a team with some level of understanding in technical fields, such as AI, data science, and cybersecurity [28]. Hiring and retaining these skilled professionals can be a challenge for many organizations. The demand for such skills is very high, making it very costly for organizations to hire and maintain teams that possess them.

Best Practices for Using AI And ML Security Solutions

Sure, let's delve into these best practices for using AI and ML security solutions:

- **Data encryption:** Implementing end-to-end encryption is crucial to protect sensitive data during transmission. Encrypting data at rest safeguards information stored on servers or databases. A promising technology in this regard is homomorphic encryption (HE), which allows AI computation on encrypted data, enabling models to use this data without decrypting it [29].
- **Access control:** Strong access controls ensure that only authorized personnel can access AI systems and their data. Implementing multi-factor authentication also adds an extra layer of security.
- **Regular updates and patching:** Keeping AI security software and frameworks up-to-date with the latest security patches is essential to address vulnerabilities. Regularly updating libraries, dependencies, and operating systems helps maintain system integrity.
- **Compliance with relevant regulations:** Adherence to data protection regulations and standards such as GDPR, HIPAA, or others relevant to your industry is mandatory. For instance, organization need to anonymize or pseudonymize data to protect user privacy.
- **Vendor Security Assessment:** If using third-party AI tools or services, conducting thorough security assessments of vendors is necessary. Ensuring that vendors follow best security practices and adhere to necessary compliance standards is important.
- **Careful Data Collection and Ingestion:** Establishing clear data standards, collecting the data responsibly, and validating it thoroughly at the point of entry are key steps. Data profile tools such as Talend Open Profiler and Open Refine can be utilized to identify and address missing values, outliers, inconsistencies, and duplicates [30].
- **Backing up data:** Implementing data backup and recovery mechanisms ensures resilience against data loss or corruption. The process of collecting and organizing data use by ML model is very costly, which is why investing in an effective backup solution.

Conclusion

This paper has explored the potential of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing the cybersecurity defenses of organizations. The primary use of AI and ML is to address the limitations of traditional tools, such as their inability to process and interpret the vast amounts of data that are crucial for identifying threats and vulnerabilities. AI-powered tools also have the ability to detect unknown threats through techniques such as behavior-based analysis.

The integration of AI into cybersecurity solutions comes with several benefits, including the ability to analyze vast amounts of data in real-time, identify patterns and anomalies that might signify a security threat, and automate responses to detected threats. AI-powered security tools can significantly enhance an organization's ability to defend against both known and unknown cyber threats, which is crucial in this era of increasingly sophisticated attacks.

Despite the numerous benefits, the integration of AI into security solutions also comes with several challenges, such as the need to ensure data quality, interpretability of complex models, the requirement for computational resources to train models, legal and ethical concerns, and a shortage of skills. Organizations need to be aware of these challenges and devise necessary solutions to address them before adopting AI security tools in their ecosystem.

Implementing best practices such as data encryption, keeping security tools up-to-date, adhering to data protection regulations, and responsible data collection is essential to the success of using AI in cybersecurity. Adopting these practices while using AI-powered security tools could be costly and may slow down some processes, but it is worth it in the long run.

References

1. IBM, "Cost of a Data Breach Report 2023." Available online: https://www.ibm.com/reports/data-breach
2. Statista, "Average cost of a data breach in the United States from 2006 to 2023." Available online: https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/
3. Mark M., Eric B., "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence," July 2021. Available online: https://www.ndu.edu/News/Article-View/Article/2684986/cyber-threats-and-vulnerabilities-to-conventional-and-strategic-deterrence/
4. Lucia S., "How Machine Learning (ML) & Cybersecurity: How Is ML Used In Cybersecurity?" November 2023. Available online: https://www.crowdstrike.com/cybersecurity-101/machine-learning-cybersecurity/
5. IBM, "Research shows extensive use of AI contains data breaches faster and saves significant costs," August 2023. Available online: https://www.ibm.com/blog/research-shows-extensive-use-of-ai-contains-data-breaches-faster-and-saves-significant-costs/
6. Anna F., "Generative AI in Cybersecurity: How It's Being Used + 8 Examples," October 2023. Available online: https://secureframe.com/blog/generative-ai-cybersecurity
7. Preethiga N., "Most Extensive Cyber Security Challenges & Solutions in 2024," December 2023. Available online: https://www.knowledgehut.com/blog/security/cyber-security-challenges#what%C2%A0is-cyber-security%C2%A0and-its-importance?%C2%A0
8. John M.J., "How cybercriminals turn 'harmless' stolen or leaked data into dollars," June 2021. Available online: https://www.csoonline.com/article/570759/how-cybercriminals-turn-harmless-stolen-or-leaked-data-into-dollars.html
9. Exabeam, "AI SIEM: How SIEM with AI/ML is Revolutionizing the SOC." Available online: https://www.exabeam.com/explainers/siem/ai-siem-how-siem-with-ai-ml-is-revolutionizing-the-soc/
10. Shruti P., Vijayakumar V., Siddiqui M.M., Abdulwodood S., Nihal A., Onkar S., Satish K., Kailash S., Ketan K., "Explainable Artificial Intelligence for Intrusion Detection System," September 2022. Available online: https://www.mdpi.com/2079-9292/11/19/3079
11. Gartner, "What Is Artificial Intelligence?" Available online: https://www.gartner.com/en/topics/artificial-intelligence
12. Kutub T., Md L.A., Muath A., Obaidat, Abu K., "A Systematic Review on Deep-Learning-Based Phishing Email Detection," November 2023. https://www.mdpi.com/2079-9292/12/21/4545
13. Gilchan P., Julia M.T., "Towards Text-Based Phishing Detection." Available online: https://arxiv.org/pdf/2111.01676.pdf
14. Casey I.C., Baruch F., Alex D., "Quantifying Phishing Susceptibility for Detection and Behavior Decisions." Available online: https://www.cmu.edu/epp/people/faculty/research/Fischhoff-HF%20Canfield%20phishing%202016.pdf
15. Achraf B., "Machine learning for malware detection," March 2017. Available online: https://resources.infosecinstitute.com/topics/machine-learning-and-ai/machine-learning-malware-detection/
16. AVTEST, "Malware statistics." Available online: https://www.av-test.org/en/statistics/malware/
17. Muhammad S.A., Tao F., "Malware Analysis and Detection Using Machine Learning Algorithms," November 2022. Available online: https://www.mdpi.com/2073-8994/14/11/2304
18. Christopher C., "Dynamic and Static Malware Analysis," June 2022. Available online: https://www.cybermaxx.com/resources/dynamic-and-static-malware-analysis/

19. Abdus Sobur, Md Humayun Kabir, Md Zakir Hossain, Anwar Hossain, Md Imran Chowdhury Rana, “Enhanching Tomato Leaf Disease Detection in Varied Climates: A Comparative Study of Advanced Deep Learning Models with a Novel Hybrid Approach” February 2024.
Available online:
http://ijcrt.org/viewfull.php?&p_id=IJCRT2402150
https://doi.one/10.1729/Journal.37820
20. CISCO, “What Is Artificial Intelligence in Networking?” Available online:
https://www.cisco.com/c/en/us/solutions/artificial-intelligence/artificial-intelligence-machine-learning-in-networking.html
21. Abdus Sobur, Md Imran Chowdhury Rana, Md Zakir Hossain, Anwar Hossain, Md Firoz Kabir, “Advancing Cancer Classification with Hybrid Deep Learning: Image Analysis for Lung and Colon Cancer Detection” February 2024.
Available online:
http://ijcrt.org/viewfull.php?&p_id=IJCRT2402237
https://doi.one/10.1729/Journal.37861
22. Almahdi M., Almahdi E., Najiya B.A., “Artificial Intelligence in Cybersecurity: Opportunities and Challenges.” June 2023. Available online:
https://ijo-bs.com/doi.org/2023/06/10.30566ijo-bs.2023.06.111.pdf?_t=1688705883
23. Md Abdus Shobur, Kazi Nazrul Islam, Md Humayun Kabir, Anwar Hossain, “A CONTRADISTINCTION STUDY OF PHYSICAL VS. CYBERSPACE SOCIAL ENGINEERING ATTACKS AND DEFENSE”, September 2023.
Available online:
http://ijcrt.org/viewfull.php?&p_id=IJCRT2309500
https://doi.org/10.5281/zenodo.10670510
24. Charlie I., “How to Estimate ROI for AI and ML Projects,” February 2022. Available online:
https://www.phdata.io/blog/how-to-estimate-roi-for-ai-ml-projects/
25. Mathura, “The Ethical Dilemmas of AI in Cybersecurity,” Available online:
https://www.isc2.org/Insights/2024/01/The-Ethical-Dilemmas-of-AI-in-Cybersecurity