International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I9P120

Volume 72 Issue 9, 131-136, September 2024
© 2024 Seventh Sense Research Group®

Original Article

Perspectives On Solving Cybersecurity Using AI Techniques

Radhika Kanubaddhi[1], Ramakanth Damodaram[1], Prasad Gandham[2], Ramu Pedada[3]

[1]*Technical Account Manager, Amazon Web Services, Dallas, Texas, USA.*
[2]*Principal Program Manager, Microsoft, Salt Lake City, Utah, USA.*
[3]*Lead Engineer, Northwestern Mutual, Milwaukee, Wisconsin, USA.*

[1]*Corresponding Author : baharsyah@unhas.ac.id*

Received: 03 August 2024 Revised: 01 September 2024 Accepted: 24 September 2024 Published: 30 September 2024

Abstract *- The increasing sophistication and frequency of cyberattacks, including incidents like those experienced by CrowdStrike, have propelled the need for innovative defenses in cybersecurity. These breaches, often resulting in substantial data loss and financial damage, pose significant risks to organizations globally, highlighting the urgent demand for advanced technological solutions. Artificial Intelligence (AI) and Large Language Models (LLMs) can play a critical role in transforming cybersecurity protocols by automating threat detection, improving incident response times, and analyzing vast datasets for anomaly identification. As traditional security measures often fail to keep pace with evolving threats, these technologies provide a means to stay ahead of cybercriminals who increasingly leverage AI for malicious purposes. Despite their potential, the integration of AI and LLMs into cybersecurity frameworks raises several challenges, including the need for continuous adaptation to new threats and the ethical implications associated with data handling and privacy concerns. This study provides an in-depth review of the different use cases using AI techniques and a way to modify those techniques to fit the purposes of different organizations.*

Keywords *- AI, LLM, Cybersecurity, CrowdStrike, Risk, Trust.*

1. Introduction

The rise of computer networks has significantly increased the surface area of any given company or organization, leading to an increased frequency and complexity of cyberattacks. These cyberattacks, which target computer systems, networks, or data, are often meticulously planned and executed, aiming to cause damage, unauthorized access, or service interruptions that result in severe data loss and financial repercussions.[1] One of the most alarming trends is the growth of insider threats, typically perpetrated by disgruntled or rogue employees who exploit their authorized access to harm their organization or steal sensitive data.[1] Understanding the landscape of cybersecurity breaches is crucial for organizations. A cybersecurity breach entails unauthorized access or manipulation of sensitive information, which may result in data disclosure to unauthorized parties. While incidents can be mere compromises, breaches represent confirmed data exposure and carry significant risks, including financial losses and reputational damage. High-profile cases, such as the Equifax breach, which exposed the personal data of over 147 million individuals, highlight the severe consequences of inadequate cybersecurity measures.[2] Moreover, cybercriminals continue to utilize sophisticated techniques, such as phishing, to exploit vulnerabilities within organizations. These techniques have evolved, especially with the advent of generative AI, which enables more convincing social engineering attacks.[3] This shift necessitates an understanding of various attack vectors, including the alarming statistic that compromised credentials account for 16% of data breaches.[4] To combat these rising threats, organizations must adopt comprehensive cybersecurity strategies that encompass risk management practices similar to general risk management frameworks, focusing on risk avoidance, transfer, and mitigation.[5] Implementing advanced technologies such as Artificial Intelligence (AI) and Large Language Models (LLMs) could play a pivotal role in enhancing cybersecurity defenses, potentially preventing incidents akin to those faced by organizations like CrowdStrike. By integrating these technologies, organizations can not only detect and respond to threats more effectively but also develop proactive measures to safeguard sensitive information.

2. Related work

2.1. Role of AI in Cybersecurity

AI in cybersecurity represents a revolutionary shift in the protection of digital assets, utilizing advanced techniques such as machine learning, deep learning, and natural language processing to bolster security defenses [6][7]. As cyber threats become increasingly sophisticated, traditional security measures often fall short, necessitating the integration of AI to stay ahead of potential attackers.

By enabling organizations to detect and mitigate threats proactively, AI enhances the accuracy of threat detection, reduces false positives, and accelerates response times [6][8].

2.2. Applications of AI in Cybersecurity

AI's ability to process vast amounts of data in real-time is crucial for identifying and responding to cyber threats effectively. It helps organizations discover new attack vectors and manage the evolving threat landscape [7]. AI-powered systems can analyze data from multiple sources, including network traffic, user behaviors, and system logs, to identify patterns that indicate potential security risks [9][10]. This capability allows security teams to focus on high-priority incidents, streamlining the triage process and improving overall security posture [8][9].

2.3. Threat Detection and Prevention

One of the most prominent applications of AI in cybersecurity is threat detection and prevention. AI systems can continuously monitor user behavior, recognizing anomalies that may suggest malicious activities, such as unauthorized access attempts or unusual data retrieval from unexpected locations [11]. Furthermore, AI can automate responses to certain threats, isolating affected systems and mitigating damage without human intervention [12].

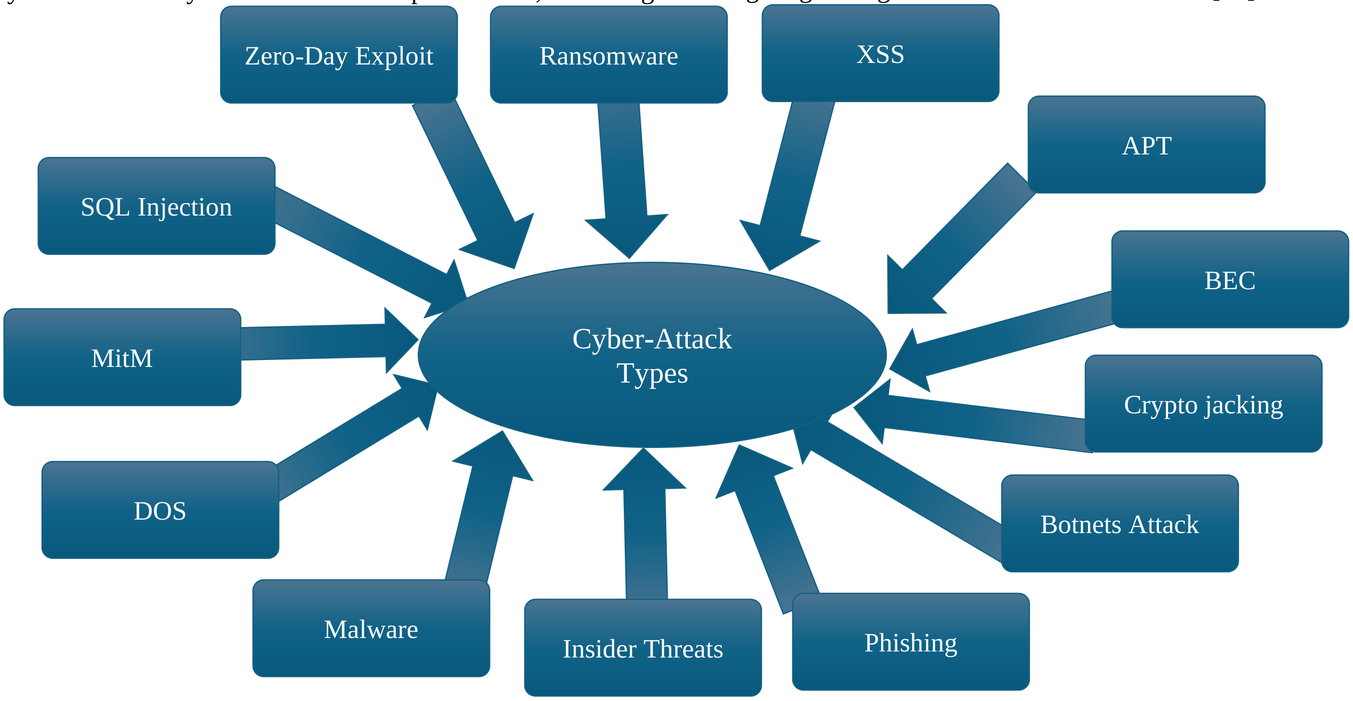

Fig. 1 Types of cyber attacks

2.4. Automation and Efficiency

The ongoing shortage of skilled cybersecurity professionals has amplified the need for automation in security processes. AI enables organizations to enhance their security investments and operations, allowing teams to manage their resources more effectively [7]. By automating repetitive tasks, AI frees up human experts to focus on more complex security challenges, thus improving operational efficiency [6][8].

3. Materials and Methods

This study focuses on three perspectives: prevention, challenges, and case studies.

3.1. Anatomy of Prevention Strategies using AI

Cybersecurity breaches can be defined as confirmed data disclosures to unauthorized third parties, encompassing various threats that target sensitive information within computer systems, networks, or applications [2]. The first step in preventing these breaches is to understand the types of cyber threats and their potential impacts. A robust defense strategy combines proactive and reactive tools, such as cybersecurity awareness training and effective security operations centers [2].

3.1.1. Data Protection Measures

Implementing data protection measures is crucial in minimizing the risk of breaches. This includes utilizing AI-driven cybersecurity automation, which helps set security protocols to counter cyberattacks and safeguard sensitive information [19]. Organizations should focus on data breach protection through predictive forecasting using machine learning models to identify weak points and common tactics employed by cybercriminals, allowing for enhanced defenses against potential breaches [20].

3.1.2. Threat Detection and Anomaly Detection

Employing advanced threat detection technologies is essential. AI and machine learning can be leveraged to spot unusual behavior and detect variations in network traffic that may signal an impending breach [19][1]. For instance, behavioral patterns can be analyzed to identify anomalies, which enhances the organization's ability to respond swiftly to potential threats.

3.1.3. User Behavior Analysis and Access Control

AI can significantly improve user access control by analyzing typical user behaviors and flagging any deviations that may indicate unauthorized access [21]. By assessing the risk of each login attempt, organizations can enhance security measures without imposing excessive barriers on verified users. This not only strengthens security but also improves the user experience [21].

3.1.4. Continuous Security Assessments and Training

Conducting regular security assessments is paramount in maintaining an effective cybersecurity posture. Organizations should train employees on best practices, ensuring that they remain vigilant against common threats such as phishing attacks, which often serve as entry points for cybercriminals [22]. Creating a security-conscious culture through ongoing training can mitigate human errors that lead to breaches [2].

3.1.5. Collaborative Cybersecurity Efforts

Collaboration with cybersecurity experts can enhance an organization's defenses. Tailoring security solutions to specific needs, based on a comprehensive understanding of potential threats, allows businesses to stay ahead of evolving cyber risks [22]. The integration of advanced technologies, such as large language models (LLMs) and AI, can support cybersecurity professionals in identifying vulnerabilities and predicting future threats [18].

3.1.6. Threat Modeling and Asset Inventory

Organizations identify potential vulnerabilities associated with LLMs and generative AI [23]. Maintaining an inventory of AI assets ensures that organizations understand the tools and services they are utilizing, facilitating better security management [5]. This proactive approach aids in safeguarding connections to AI platforms from internal systems, thereby minimizing the risk of exploitation. By employing these strategies, organizations can build a comprehensive defense mechanism against cybersecurity breaches, leveraging the capabilities of AI and LLMs to enhance security measures effectively.

3.2. Challenges of Prevention using AI

The deployment of AI and large language models (LLMs) in cybersecurity, particularly in preventing incidents similar to those experienced by CrowdStrike, faces several significant challenges and limitations.

3.2.1. Resource Demands

One of the foremost challenges is the substantial computational resources required for training and running AI algorithms. These demands pose difficulties, especially in resource-limited environments, where organizations may struggle to maintain the necessary infrastructure for effective AI implementation [17].

3.2.2. Data Preprocessing Needs

The complexity and time required for data preprocessing can hinder the swift deployment of AI systems. Effective preprocessing is essential to ensure the quality of input data for AI algorithms, thereby complicating the implementation process [1].

3.2.3. Adaptation to New Threats

Another challenge lies in the necessity to adapt AI models to evolving cyber threats continuously. As new attack vectors emerge, existing models may require retraining or significant adjustments, which can lead to a decline in their accuracy over time. This adaptability is crucial for maintaining effective defense mechanisms [1].

3.2.4. Ethical Considerations

Ethical concerns also complicate the application of AI in cybersecurity. Issues related to user privacy, data surveillance, and potential biases can arise from the extensive data collection required for threat detection. Striking a balance between robust security measures and the preservation of individual privacy rights remains a complex challenge [24][25].

3.2.5. Transparency and Explainability

The lack of transparency and explainability in AI algorithms can impede user trust and adoption. Users and stakeholders must understand how AI systems make decisions to ensure accountability and fairness, particularly in sensitive security contexts [25].

3.2.6. Bias and Fairness

AI systems are susceptible to biases, which can lead to unfair targeting or misidentification of individuals as insider threats. This lack of context and understanding may result in significant ethical dilemmas, necessitating human oversight to validate AI outputs and guide responsible decision-making [26][27].

3.2.7. Cost of Implementation

Incorporating AI technology into cybersecurity can be expensive, requiring significant investment in infrastructure, specialized hardware, and skilled personnel. Organizations must carefully evaluate the total cost of ownership to avoid unexpected financial burdens associated with AI solutions [27][28].

3.3. Real-World Application of AI in Dealing with Cybersecurity

Real-world applications of Artificial Intelligence (AI) in cybersecurity have demonstrated significant improvements in data protection and threat mitigation. One notable case study involved a Fortune 500 telecommunications provider that utilized Snorkel Flow to enhance the classification of encrypted network data flows. By addressing challenges related to slow and costly manual labeling processes, as well as the limitations of static rules-based systems, they achieved a remarkable 26.2% improvement in accuracy over their baseline model [29].

3.3.1. Digital Forensics and Large Language Models

In the realm of digital forensics, the potential of Large Language Models (LLMs) is being explored to assist in cybercriminal prosecutions. Research by Scanlon et al. (2023) evaluated LLM performance in various forensic scenarios, such as file identification and evidence retrieval. While the findings indicated that LLMs cannot yet serve as standalone forensic tools, they can function as valuable supplementary aids in specific cases, thereby enhancing investigative capabilities [17].

3.3.2. Threat Detection and Prevention

Recent studies have highlighted the integration of AI into threat detection and prevention strategies. For instance, Best Buy reported that its machine learning-based cybersecurity system improved the accuracy of detecting phishing emails to 96% [3]. This level of precision is essential as cyber threats become increasingly sophisticated, utilizing techniques such as natural language and deep fake multimedia that are difficult to identify without advanced solutions.

3.3.3. Enhancements in Cyber Resilience

The dynamic capabilities of AI enable organizations to implement real-time anomaly detection and adjust access policies based on behavioral analysis.

For example, when a potentially risky account attempts to access data from an unusual location, AI can automate data security measures such as data masking to mitigate risks effectively [30]. This proactive approach is crucial in today's rapidly evolving digital landscape, where 76% of companies are allocating budget towards AI and machine learning in their IT expenditures, reflecting a broader trend of embracing automation as a fundamental component of cybersecurity strategies [20].

4. Discussion

This review identified and discussed various use cases as well as limitations of applying AI in cybersecurity. The integration of Artificial Intelligence (AI) and Large Language Models (LLMs) in cybersecurity is rapidly evolving, presenting both opportunities and challenges. The ongoing development in these areas aims to enhance defense mechanisms against increasingly sophisticated cyber threats.

4.1. Continuous Improvement of LLMs

The OWASP Top 10 for LLM Applications is expected to undergo periodic updates, reflecting the dynamic nature of the industry and the growing community's involvement in pushing the state of the art forward [31].

This iterative approach ensures that the frameworks remain relevant as new vulnerabilities and attack vectors emerge. As LLMs are incorporated into more consumer-facing products, the complexity of vulnerabilities will expand, necessitating continuous research and adaptation in security measures [32].

4.1.1. Rise in Research and Publications

There has been a significant uptick in research focused on LLMs for cybersecurity. From just a few papers in 2020, the number surged to 109 in 2023, indicating a heightened interest in leveraging LLMs for security applications [17]. This trend suggests that cybersecurity professionals are increasingly turning to advanced AI techniques to address the evolving landscape of cyber threats.

4.1.2. Enhanced Cyber Defense Mechanisms

AI technologies such as machine learning and deep learning are being employed to bolster cybersecurity defenses. By analyzing vast datasets, these systems can identify anomalies and predict potential threats more accurately and swiftly than traditional methods [7][33]. The concept of "possibility synthesis," which utilizes machine learning to anticipate vulnerabilities, is becoming integral to proactive cybersecurity strategies [20].

4.1.3. AI-Driven Threat Evolution

While AI presents new opportunities for enhancing security, it also enables cybercriminals to adopt advanced strategies. Hackers are leveraging AI-driven techniques to breach robust protection programs, indicating a shift in the cybersecurity landscape [34]. Consequently, organizations must not only adopt AI solutions for defense but also prepare for the potential adversarial use of these technologies.

4.1.4. Training and Skill Development

As AI tools become more prevalent, there is a growing demand for skilled professionals capable of implementing these advanced systems effectively. Online cybersecurity training programs are increasingly vital in equipping specialists with the necessary skills to meet industry demands and successfully combat emerging threats [6].

References

[1] Aya H. Salem et al., “Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques,” *Journal of Big Data*, vol. 11, pp. 1-38, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Understanding Cybersecurity Breaches: Types, Common Causes and Potential Risks, Infosec, 2023. [Online]. Available: https://www.infosecinstitute.com/resources/general-security/understanding-cybersecurity-breaches-types-common-causes-and-potential-risks/

[3] Insights, Why Understanding AI’s Role in Data Breach Prevention is Key to Cyber Resilience, UST. [Online]. Available: https://www.ust.com/en/insights/why-understanding-ai-role-in-data-breach-prevention-is-key-to-cyber-resilience#:~:text=In%20cybersecurity%2C%20AI%2Dpowered%20tools,or%20blocking%20malicious%20IP%20addresses.

[4] What is a Data Breach?, IBM, 2024. [Online]. Available: https://www.ibm.com/topics/data-breach#:~:text=A%20data%20breach%20is%20any,intellectual%20property%2C%20financial%20information).

[5] Alessandro Mazzoccoli, and Maurizio Naldi, “An Overview of Security Breach Probability Models,” *Risks*, vol. 10, no. 11, pp. 1-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Karin Kelley, AI in Cybersecurity: A Comprehensive Guide, Caltech, 2024. [Online]. Available: https://pg-p.ctme.caltech.edu/blog/cybersecurity/ai-in-cybersecurity

[7] What is AI in Cybersecurity?, SOPHOS. [Online]. Available: https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity#:~:text=AI%20powered%20cybersecurity%20can%20monitor,common%20kinds%20of%20cyber%20attacks.

[8] How Can Generative AI Be Used in Cybersecurity? 10 Real-World Examples, Secureframe, 2024. [Online]. Available: https://secureframe.com/blog/generative-ai-cybersecurity

[9] AI in Cybersecurity: How It’s Used + 8 Latest Developments, Secureframe, 2024. [Online]. Available: https://secureframe.com/blog/ai-in-cybersecurity

[10] Enhancing Cybersecurity through AI: A Look Into the Future, ISC2, 2023. [Online]. Available: https://www.isc2.org/Insights/2023/09/Enhancing-Cybersecurity-through-AI-A-Look-into-the-Future

[11] Examples of Artificial Intelligence (AI) Use Cases In Cyber Security, zcybersecurity.com. [Online]. Available: https://zcybersecurity.com/using-artificial-intelligence-in-cyber-security/

[12] Artificial Intelligence (AI) Cybersecurity, IBM, 2024. [Online]. Available: https://www.ibm.com/ai-cybersecurity

[13] AI Security Threats: Challenges & Solutions for LLMs, Zero Point Labs, 2024. [Online]. Available: https://zeropointlabs.ai/ai-security-threats-challenges-solutions-for-llms/

[14] Arjun, LLM Risks: Insights & Real-World Case Studies, Akto.io. [Online]. Available: https://www.akto.io/blog/llm-risks-insights-real-world-case-studies

[15] Dinil Mon Divakaran, and Sai Teja Peddinti, “LLMs for Cyber Security: New Opportunities,” *arXiv*, pp. 1-10, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Aleena Noor, Large Language Models in Cybersecurity: Pioneering Trends in AI, Cirrus Labs. [Online]. Available: https://www.cirruslabs.io/additionalresources/large-language-models-in-cybersecurity-pioneering-trends-in-ai#:~:text=LLMs%20are%20typically%20trained%20on,relationships%20and%20context%20behind%20them.

[17] Hanxiang Xu et al., “Large Language Models for Cyber Security: A Systematic Literature Review,” *arXiv*, pp. 1-47, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jie Zhang et al., “When LLMs Meet Cybersecurity: A Systematic Literature Review,” *arXiv*, pp. 1-36, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Tejdeep Desai, Top 4 AI Security Tools for 2023, ITSecurityWire, 2023. [Online]. Available: https://itsecuritywire.com/featured/top-4-ai-security-tools-for-2023/

[20] Akash Takyar, AI in Cybersecurity: Use Cases, Implementation, Solution and Development, Leeway Hertz. [Online]. Available: https://www.leewayhertz.com/ai-in-cybersecurity/

[21] AI in Cybersecurity, Sekoia.io. [Online]. Available: https://www.sekoia.io/en/glossary/ai-in-cybersecurity/#:~:text=AI%20can%20handle%20routine%20data,resilient%20response%20to%20evolving%20threats.

[22] AI-Powered Cyber Attacks: Understanding and Mitigating the Risks, BDO USA, 2023. [Online]. Available: https://www.bdo.com/insights/digital/ai-powered-cyber-attacks-understanding-and-mitigating-the-risks

[23] Chris Hughes, Keeping up with AI: OWASP LLM AI Cybersecurity and Governance Checklist, CSO, 2024. [Online]. Available: https://www.csoonline.com/article/1313475/keeping-up-with-ai-the-owasp-llm-ai-cybersecurity-and-governance-checklist.html

[24] What is AI Security?, IBM, 2024. [Online]. Available: https://www.ibm.com/think/topics/ai-security#:~:text=Short%20for%20artificial%20intelligence%20(AI,enhance%20an%20organization’s%20security%20posture.

[25] Data Science Dojo Staff, AI in Cybersecurity: Revolutionizing Threat Detection and Defense, Data Science Dojo, 2023. [Online]. Available: https://datasciencedojo.com/blog/ai-in-cybersecurity/

[26] Altay Ataman, AI Cybersecurity: Real-Life Examples & Limitations, AIMultiple, 2024. [Online]. Available: https://research.aimultiple.com/ai-cybersecurity/

[27] What are the Risks and Benefits of Artificial Intelligence (AI) in Cybersecurity?, Paloalto Networks. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity

[28] Tiedrich, Celine Caira, and Yaniv Benhamou, The AI Data Challenge: How do we Protect Privacy and Other Fundamental Rights in an AI-Driven World?, OECD.AI, 2023. [Online]. Available: https://oecd.ai/en/wonk/the-ai-data-challenge-how-do-we-protect-privacy-and-other-fundamental-rights-in-an-ai-driven-world

[29] AI Case Studies and Success Stories, Accubits. [Online]. Available: https://accubits.com/ai-case-studies-and-success-stories/

[30] Rachelle Blair-Frasier, Top Cybersecurity Trends of 2023, Security Magazine, 2023. [Online]. Available: https://www.securitymagazine.com/articles/100156-top-cybersecurity-trends-of-2023

[31] OWASP Top 10: LLM & Generative AI Security Risks, Owasp. [Online]. Available: https://genai.owasp.org/

[32] Cybersecurity in the AI Era: How the Threat Landscape Evolved in 2023, Kaspersky, 2023. [Online]. Available: https://www.kaspersky.com/about/press-releases/cybersecurity-in-the-ai-era-how-the-threat-landscape-evolved-in-2023

[33] What Is the Role of AI in Threat Detection?, Paloalto Networks. [Online]. Available: https://www.paloaltonetworks.in/cyberpedia/ai-in-threat-detection#:~:text=In%20network%20security%2C%20AI%20threat,and%20provide%20real%2Dtime%20alerts.

[34] Dewayne Hart, How AI-Driven Cyberattacks Will Reshape Cyber Protection, Forbes, 2024. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2024/03/19/how-ai-driven-cyber-attacks-will-reshape-cyber-protection/#:~:text=Invoking%20AI%20into%20the%20risk,on%20patterns%20and%20computational%20errors.