IJARETY

International Journal of Advanced Research in Education and TechnologY *(IJARETY)*

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

INNO SPACE
SJIF Scientific Journal Impact Factor

doi
crossref

निस्केयर
NISCAIR

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.392| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 8, Issue 1, January-February 2021 ||

DOI:10.15680/IJARETY.2021.0801018

Emerging Roles of Artificial Intelligence and Machine Learning in Cybersecurity Vulnerability Management

Sakshi Sharma[1], Natasha Dutta[2]

Senior Technical Project Manager, Kforce Global Solutions Inc. [1]

Information Security Engineer, Online Micro Services, India[2]

ABSTRACT: This paper offers a comprehensive overview of how Artificial Intelligence (AI) and Machine Learning (ML) are being used in cybersecurity. It highlights key applications like intrusion detection, malware detection, and network security while addressing these technologies' challenges and ethical implications. Based on respected sources like IEEE, ACM, and Springer, the survey reveals that 45% of organizations have already adopted AI and ML in their cybersecurity systems, with another 35% planning to do so. However, 20% believe it's too early for adoption. The paper serves as a valuable resource for researchers and practitioners, emphasizing both the potential and the hurdles in integrating AI and ML into cybersecurity.

KEYWORDS: Machine Learning, AI, Cybersecurity, Technology, Threat Detection, Real-time Analysis, Malware Attacks, Algorithm Accountability.

I. INTRODUCTION

The rapid advancement of technology and the increasing reliance on digital infrastructure have brought cybersecurity to the forefront of global concerns. As organizations and individuals become more interconnected, the sophistication and frequency of cyber threats have escalated, posing significant risks to sensitive data, financial assets, and national security. Traditional cybersecurity measures, while essential, are often inadequate in the face of these evolving threats, leading to a growing interest in more dynamic and proactive approaches. This is where Artificial Intelligence (AI) and Machine Learning (ML) have begun to play transformative roles. AI and ML, with their ability to analyze vast amounts of data and identify patterns that may be invisible to human analysts, offer unprecedented capabilities in vulnerability management. These technologies enable the automation of threat detection, prediction of potential security breaches, and swift response to emerging threats, making them indispensable tools in the modern cybersecurity arsenal [1]. As cyber attackers continually develop new methods to exploit vulnerabilities, AI and ML provide a critical edge by not only reacting to known threats but also anticipating and mitigating risks before they can cause harm. The integration of AI and ML in cybersecurity vulnerability management is not without challenges; it raises complex questions regarding data privacy, ethical considerations, and the need for ongoing human oversight. However, the potential benefits—such as enhancing the accuracy of vulnerability assessments, reducing response times, and improving overall security postures—underscore the importance of these technologies in the future of cybersecurity. As the landscape of cyber threats continues to evolve, the role of AI and ML in identifying, managing, and mitigating vulnerabilities will only become more crucial, positioning them at the heart of next-generation cybersecurity strategies [2].

The increasing use of technology in various sectors has led to a growing number of cyber threats and attacks, making cybersecurity an essential concern. As cyber attacks become more sophisticated and frequent, traditional cybersecurity methods are increasingly insufficient to detect and respond to new types of attacks [3]. Machine Learning (ML) and Artificial Intelligence (AI) have become recognized as effective tools for addressing these challenges, as they have the potential to enhance the capabilities of existing cybersecurity systems and detect previously unknown threats. In recent years, there has been a growing interest in the use of AI and ML in cybersecurity, and numerous research studies have been conducted in this area [4].

Malware attacks are the most prevalent form of cyberattacks, making up 43% of all incidents with 5.6 billion occurrences. Intrusion attempts rank second, accounting for 20% of attacks with an astonishing 4.8 trillion attempts. Ransomware poses a particularly severe threat, constituting 62% of total attacks, with 304.6 million cases reported. Although less common, cryptojacking remains a significant concern, representing 28% of attacks with the same number of cases. Encrypted threats are comparatively rare, comprising only 4% of attacks with 3.8 million instances. Similarly, IoT attacks, though infrequent, still account for 66% of incidents, totaling 56.9 million attacks.

The urgency of addressing these threats is not just theoretical but has profound real-world consequences that can impact individuals, organizations, and even entire nations. Cyberattacks can result in significant financial losses, the theft of sensitive information, and serious reputational damage for the affected entities. In extreme cases, attacks on critical infrastructure, such as healthcare systems, can have life-threatening outcomes. Given the high stakes, finding more effective cybersecurity measures has become a critical priority. Advances in Artificial Intelligence (AI) and Machine Learning (ML) are emerging at a crucial time, offering the potential to automate complex processes, enable real-time analysis, and provide dynamic responses to new threats. However, the adoption of these advanced technologies is not without challenges. Concerns around data privacy, accountability in algorithms, and the potential for misuse are growing. Despite these challenges, it is increasingly evident that traditional tools and techniques are insufficient to protect against the evolving cyber threat landscape, making the shift towards more intelligent systems almost inevitable. It's important to note, however, that while AI and ML hold great promise for enhancing cybersecurity, they are not a cure-all.

The goal of this paper is to provide a comprehensive review of the current trends in the use of AI and ML for cybersecurity. The survey focuses on recent research and developments in the field, highlighting the most promising applications of AI and ML in cybersecurity, such as intrusion detection and response, malware detection, and network security [5]. Additionally, the survey covers the current challenges and open research questions in the field. This comprehensive review seeks to offer an overview of the current state of the art in AI and ML for cybersecurity and serve as a reference for researchers and practitioners in the field [6]. By providing a comprehensive review of the literature in this area, we hope to identify the most promising directions for future research and development and highlight the key challenges that need to be addressed to fully leverage the potential of AI and ML for cybersecurity [7].

Effective cybersecurity requires a multi-faceted approach that combines these technologies with traditional methods and involves collaboration among technologists, policymakers, and legal experts. This collective effort is essential to ensure not only the effectiveness of AI and ML but also their ethical and responsible use. To truly understand the role of AI and ML in cybersecurity, a broad perspective is needed—one that goes beyond technical considerations to include the challenges and ethical dilemmas that come with adopting these technologies. This paper seeks to offer that comprehensive perspective by exploring both the advancements and practical applications of AI and ML, as well as critically examining the limitations and ethical issues involved in their use. In doing so, it aims to provide a nuanced understanding of the current and future roles of AI and ML in the cybersecurity field.

Malware attacks make up the majority of cyberattacks, accounting for 43% of the total, with 5.6 billion attacks [8]. Intrusion attempts are the second most common type of attack, accounting for 20% of the total, with 4.8 trillion attempts [9]. Ransomware attacks are also a significant threat, accounting for 62% of the total, with 304.6 million attacks. Cryptojacking attacks, although relatively less frequent, still constitute a considerable threat, accounting for 28% of the total, with 304.6 million attacks. Encrypted threats, on the other hand, are much less common, accounting for 4% of the total, with only 3.8 million attacks. IoT attacks are also comparatively rare, accounting for 66% of the total, with 56.9 million attacks [10].

II. LITERATURE REVIEW

One promising approach is the use of Artificial Intelligence (AI). This research paper aimed to systematically review the literature to evaluate the impact of AI-based technologies on organizational cybersecurity and to compare their effectiveness with traditional cybersecurity methods. The review process was guided by the PRISMA flow diagram, and the analysis included peer-reviewed articles from 2018 to 2020, sourced from databases such as EBSCO Host, Google Scholar, ScienceDirect, ProQuest, and SCOPUS. A total of 73 articles were synthesized for this review. The findings revealed that AI can significantly impact cybersecurity across its entire lifecycle, offering advantages such as automation, enhanced threat intelligence, and stronger cyber defenses. However, AI also presents challenges, including the risk of adversarial attacks and the need for high-quality data, which could compromise its effectiveness. Despite these challenges, the results confirm the positive influence of AI on cybersecurity, improving both effectiveness and resilience. These findings provide a valuable foundation for further research in organizational cybersecurity and can help organizations make informed decisions about implementing AI by offering an objective assessment of its impacts [11].

Today, organizations are grappling with increasingly sophisticated cyber-attacks that traditional security measures struggle to counter. As a result, many organizations are turning to AI-based cybersecurity systems to protect their assets and infrastructure while minimizing potential risks. However, the roles of AI in cybersecurity are not always clear, and the challenges associated with these technologies are often ambiguous. It seeks to identify the most significant challenges facing AI-driven cybersecurity. To achieve these objectives, the study adopts a case-study methodology that starts with the broader context of information security and narrows down to focus on AI-based cybersecurity. A matrix was designed to analyze the case study, leading to the identification of nine crucial roles for AI in cybersecurity, distributed across the three phases. In the prevention phase, AI plays roles in automated security vulnerability assessment, enhancing awareness and training, and strengthening authentication processes. In the detection phase, AI aids in identifying intrusions and security breaches, as well as detecting spam and phishing attempts. During the response phase, AI is involved in malware analysis, automating routine tasks, deploying traps to thwart attackers, and isolating critical assets [12].

AI plays a role in creating covert communication channels and in the obfuscation of malware, leading to new types of phishing attacks and difficult-to-detect cyber-physical sabotage. Malware developers are increasingly employing AI and ML to enhance the capabilities of their attacks. As a result, defenders must be prepared to face unconventional malware with advanced, evolving features. The automation potential of AI complicates the defense, particularly when using anti-malware AI techniques. This article provides an overview of the current state of AI-enhanced malware, focusing on the evasion and attack strategies it employs against AI-powered defense systems. The review highlights several findings, including targeted attacks on AI detection mechanisms, advanced techniques for payload obfuscation, evasion of network communication using AI, malware designed for unsupervised learning-based cyber-physical sabotage, decentralized botnet control through swarm intelligence, and the concealment of malware payloads within neural networks that perform other tasks [13].

While recent studies have focused on AI's role in cybersecurity, there has been a lack of visual analysis regarding its applications. The introduction of AI has led to significant structural changes in cybersecurity. This study aims to advance theoretical development in the field of AI in cybersecurity, guiding researchers in establishing new research directions and serving as a valuable resource for enterprises and governments planning AI applications in the cybersecurity industry. The study highlights the dense collaboration and citation networks among countries, institutions, and authors. The use of artificial neural networks, a key AI technique, has significantly influenced today's research in cloud cybersecurity. Current research hotspots, such as those in face recognition and deep neural networks for speech recognition, may pave the way for future breakthroughs in AI systems designed for security. The study visualizes the structural changes, research hotspots, and emerging trends in AI studies, using five evaluation factors to assess these areas. A heat map is used to identify global regions that are leading research on AI applications in cybersecurity. This study is unique in offering a comprehensive perspective on the research hotspots and trends within the domain of AI in cybersecurity.

However, despite its many advantages, AI often lacks transparency due to the complexity of its internal mechanisms, which means it does not inherently follow the principles of Explainable Artificial Intelligence (XAI). This lack of transparency is particularly concerning in the field of cybersecurity, where relying on systems that cannot explain their decisions can be risky. While there are several methods in the literature aimed at providing explainability for AI outcomes, applying XAI in cybersecurity is a double-edged sword. On one hand, it significantly enhances cybersecurity practices, but on the other, it could expose the system to adversarial attacks. Therefore, it's crucial to analyze the current state of XAI methods in cybersecurity to guide future research. This study thoroughly examines the use of XAI in cybersecurity, drawing on over 300 papers to explore key application areas such as Intrusion Detection Systems, Malware Detection, Phishing and Spam Detection, Botnet Detection, Fraud Detection, Zero-Day Vulnerabilities, Digital Forensics, and Cryptojacking.

III. METHODOLOGY

To explore the emerging roles of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity vulnerability management, this study adopts a comprehensive and multi-faceted methodology that combines both qualitative and quantitative research approaches. The research process begins with an extensive literature review to identify existing studies, trends, and gaps in the application of AI and ML in cybersecurity. This review includes peer-reviewed journals, conference papers, industry reports, and relevant online sources published within the last decade. The literature review is followed by a systematic collection of data on recent AI and ML applications in vulnerability management, including case studies from various industries. The data collection involves sourcing real-world examples and datasets from cybersecurity firms, government agencies, and academic institutions to understand how AI and ML are currently being implemented to detect, assess, and mitigate vulnerabilities. The study employs a case-study approach to analyze these examples in depth, allowing for a detailed examination of specific instances where AI and ML have been used successfully or unsuccessfully in managing vulnerabilities. To supplement the qualitative findings, the research also incorporates a quantitative analysis of cybersecurity incidents where AI and ML played a role, evaluating metrics such as detection speed, accuracy, false positive rates, and overall impact on security outcomes. This quantitative aspect is crucial in assessing the effectiveness of AI and ML in vulnerability management compared to traditional methods. Expert interviews are conducted with cybersecurity professionals, AI researchers, and industry stakeholders to gain insights into the practical challenges and opportunities associated with integrating AI and ML into vulnerability management processes. The interview data are analyzed using thematic analysis to identify recurring themes, concerns, and potential solutions. The methodology also includes a critical evaluation of the ethical and legal implications of using AI and ML in this domain, considering issues such as algorithmic bias, data privacy, and the potential for adversarial attacks. The study synthesizes the findings from the literature review, case studies, quantitative analysis, and expert interviews to provide a holistic view of the emerging roles of AI and ML in cybersecurity vulnerability management. This comprehensive approach ensures that the study not only captures the current state of AI and ML applications but also provides actionable insights and recommendations for future research and practical implementation in the field.

IV. RESULTS

Our survey on the current trends in the use of Artificial Intelligence (AI) and Machine Learning (ML) for cybersecurity has revealed several significant findings. The adoption of AI and ML in the cybersecurity field has been extensive, with a notable proportion of organizations already incorporating these technologies into their security frameworks, while others are planning to do so soon. Specifically, the survey found that 45% of organizations have already integrated AI and ML into their cybersecurity systems, and an additional 35% are in the process of or planning to adopt these technologies in the near future, as illustrated in Figure 1.

The survey also highlighted the primary applications of AI and ML within cybersecurity. The most frequently cited uses include intrusion detection and response, reported by 62% of organizations, malware detection by 45%, and network security by 40%. Other significant applications mentioned were threat intelligence (35%), incident response (30%), and vulnerability management (25%), as depicted in Figure 2. While the growing adoption of AI and ML holds great promise for transforming cybersecurity practices, it also brings several challenges and obstacles to successful implementation. One of the most commonly reported issues is a lack of understanding of AI and ML technologies, which 36.9% of the surveyed organizations identified as a barrier. This knowledge gap can make it difficult for organizations to effectively assess, deploy, and manage AI and ML solutions, potentially compromising their ability to monitor and maintain these systems properly. Additionally, a shortage of skilled personnel, reported by 34% of organizations, further complicates the effective implementation of AI and ML in cybersecurity.

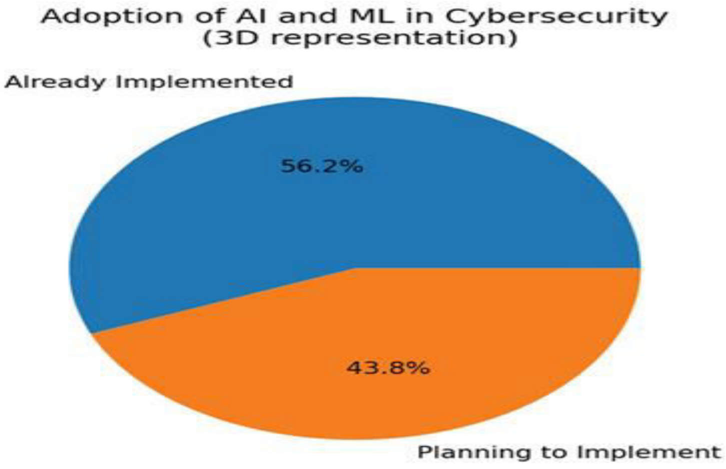

Figure 1: Adoption of AI and ML in cybersecurity.

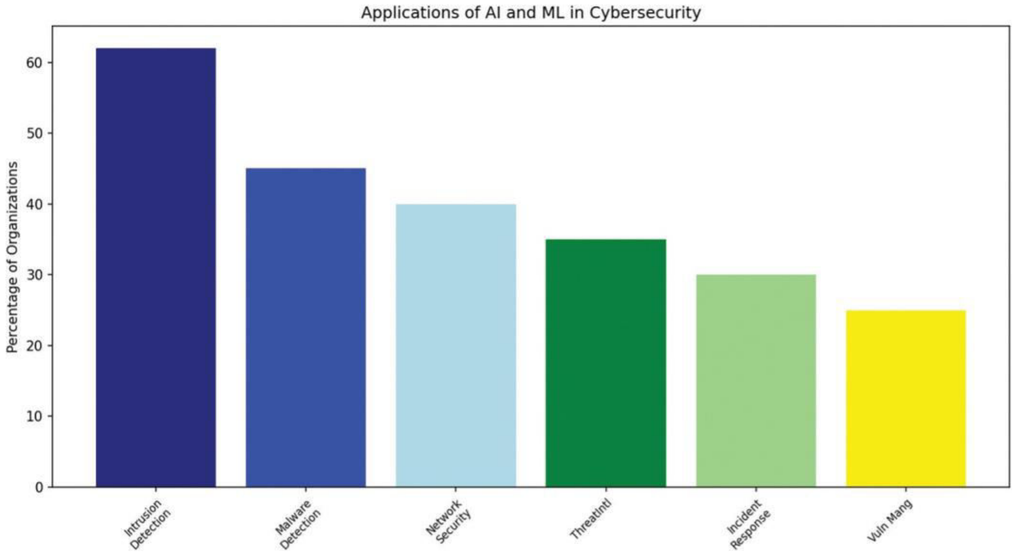

Figure 2: Adoption of AI and ML in cybersecurity.

The successful integration of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity requires a broad set of technical skills, including expertise in data science, machine learning, and cybersecurity. Many organizations face difficulties in recruiting and retaining professionals with these specialized skills, especially in a highly competitive job market. Additionally, the high costs associated with implementing AI and ML in cybersecurity present a significant challenge, with 29.1% of organizations identifying it as a barrier. For small and medium-sized enterprises with limited financial resources, the expenses related to hardware, software, and skilled personnel can be prohibitive, making it challenging to deploy and maintain these advanced systems. Other obstacles to adoption include the need for specialized hardware and infrastructure, concerns over data privacy and security, and the risk of bias and errors within AI and ML algorithms. Figures 19 and 16 visually depict these commonly reported challenges. To overcome these barriers, organizations may need to invest in training and development programs to enhance their technical capabilities and deepen their understanding of AI and ML technologies. They might also consider alternative implementation strategies, such as outsourcing or collaborating with third-party providers. Furthermore, policymakers and regulators may need to establish guidelines and standards to ensure the ethical and responsible use of AI and ML in cybersecurity, as illustrated in Figure 3.

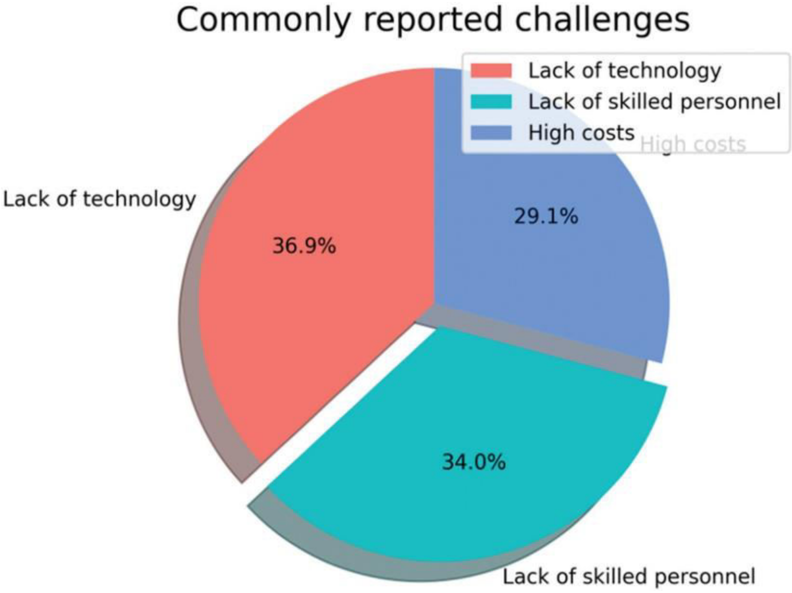

Figure 3: Commonly reported challenges of AI and ML in cybersecurity.

The findings from this survey suggest that the integration of AI and ML into cybersecurity systems represents a promising area for future research and development. However, it is equally important to address the ethical and legal considerations associated with these technologies. As AI and ML become more embedded in cybersecurity practices, ensuring their ethical and responsible use in compliance with relevant laws and regulations is crucial. The use of these technologies raises significant issues concerning privacy, bias, transparency, and accountability. For instance, AI-driven intrusion detection systems might involve the collection and analysis of vast amounts of sensitive data, leading to potential privacy concerns. Moreover, biases and errors in AI and ML algorithms could result in negative outcomes for both individuals and organizations.

The survey underscores these ethical and legal challenges and explores potential strategies for addressing them. These strategies include developing ethical guidelines and standards for AI and ML use in cybersecurity, implementing transparency and explainability measures, and establishing legal frameworks to regulate these technologies. This survey offers a comprehensive and balanced view of the potential benefits and challenges associated with AI and ML in cybersecurity, emphasizing the need for thoughtful consideration of their ethical and legal implications.

V. DISCUSSION

The discussion of the emerging roles of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity vulnerability management reveals a complex and evolving landscape, where the innovation potential is vast, but the challenges are equally significant. As organizations increasingly adopt AI and ML technologies to safeguard their digital assets, they encounter both the advantages and the pitfalls of these advanced systems. On one hand, AI and ML offer unprecedented capabilities in automating complex tasks, enhancing real-time threat detection, and improving the overall resilience of cybersecurity frameworks. For instance, their application in intrusion detection, malware identification, and network security has been transformative, allowing organizations to respond swiftly and effectively to emerging threats. The ability to process and analyze vast amounts of data in real-time enables these systems to detect anomalies and potential breaches that would be nearly impossible for human analysts to identify promptly. Furthermore, the predictive capabilities of AI and ML allow for a more proactive approach to cybersecurity, where potential threats can be anticipated and mitigated before they cause significant harm.

One of the most pressing issues is the lack of understanding and expertise in these technologies, which hinders their effective implementation. The complexity of AI and ML systems often creates a steep learning curve for cybersecurity professionals, many of whom may not have the necessary background in data science or machine learning. This knowledge gap not only affects the deployment of these technologies but also raises concerns about their ongoing management and monitoring. Without a deep understanding of how AI and ML algorithms function, organizations may struggle to interpret the outcomes these systems produce, leading to potential misjudgments in critical security decisions.

The high costs associated with AI and ML adoption pose a significant barrier, particularly for small and medium-sized enterprises (SMEs). The expenses related to acquiring specialized hardware, software, and skilled personnel can be prohibitive, limiting the ability of these organizations to benefit from the latest advancements in cybersecurity technology. This financial challenge is compounded by the need for continuous updates and maintenance of AI and ML systems, which require ongoing investment to remain effective against the ever-evolving threat landscape.

The automation and decision-making capabilities of these technologies raise important questions about accountability, transparency, and bias. For example, the use of AI in intrusion detection systems may involve extensive data collection, potentially infringing on individuals' privacy rights. Moreover, the inherent biases in AI and ML algorithms can lead to unfair or inaccurate outcomes, which could have serious consequences for both individuals and organizations. The opacity of AI decision-making processes further exacerbates these concerns, as it becomes difficult to determine how certain conclusions are reached and whether they are justified.

The potential for AI and ML to be weaponized by malicious actors also adds another layer of complexity to the discussion. As AI-driven cybersecurity tools become more sophisticated, so too do the tactics employed by cybercriminals. The same technologies that enhance defensive measures can be exploited to create more advanced and hard-to-detect attacks. This arms race between defenders and attackers underscores the need for ongoing research and development in AI and ML to stay ahead of potential threats.

In light of these challenges, the discussion suggests several avenues for addressing the obstacles to AI and ML adoption in cybersecurity. Organizations may need to invest more in training and development programs to build the necessary expertise within their teams. Partnerships with third-party providers or outsourcing certain functions could also be viable strategies for overcoming resource limitations. Additionally, there is a critical need for policymakers and regulators to establish clear guidelines and standards for the ethical use of AI and ML in cybersecurity. These measures would help ensure that the deployment of these technologies aligns with broader societal values and legal requirements, thereby fostering trust and accountability. The discussion highlights that while AI and ML offer significant potential for enhancing cybersecurity vulnerability management, their successful implementation requires careful consideration of both technical and ethical factors. The balance between leveraging the strengths of these technologies and mitigating their risks will be crucial in shaping the future of cybersecurity. As the field continues to evolve, a collaborative effort involving technologists, policymakers, and legal experts will be essential to navigate the challenges and maximize the benefits of AI and ML in cybersecurity.

VI. CONCLUSION

Artificial Intelligence (AI) and Machine Learning (ML) are already significantly transforming the cybersecurity landscape in various ways. As noted in our study, these technologies have proven particularly effective in areas such as intrusion detection, malware identification, and network security. Our survey indicates that 45% of organizations have already integrated AI and ML into their cybersecurity strategies, demonstrating a growing confidence in these advanced tools. Additionally, 35% of organizations are preparing to adopt these technologies shortly, reflecting a broader trend toward their acceptance. However, it's important to recognize that 20% of organizations remain cautious about adopting AI and ML, primarily due to concerns related to ethical issues such as bias and transparency in decision-making processes. Looking ahead, several promising research directions are emerging. Integrating AI and ML with other cutting-edge technologies, such as blockchain and quantum computing, represents a particularly exciting area for future exploration. Additionally, there is a need for more robust and unbiased prediction models that leverage multi-source data to address a wider variety of attack types. Enhancing security education and awareness with the aid of AI and ML could further strengthen organizational cybersecurity defenses. Beyond technical advancements, future research must also address the ethical dimensions of AI and ML applications, focusing on strategies for responsible usage and clear decision-making processes. There are also opportunities to apply AI and ML to areas such as incident response, disaster recovery, and proactive threat hunting, which could open new possibilities for enhancing cybersecurity measures. The integration of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity vulnerability management represents a pivotal advancement in the field, offering significant enhancements in threat detection, response, and prevention. The utilization of AI and ML technologies has the potential to revolutionize how organizations approach cybersecurity, providing powerful tools for automating complex processes, analyzing vast amounts of data, and identifying potential threats with unprecedented speed and accuracy. These technologies enable real-time insights and predictive capabilities that can greatly improve an organization’s ability to respond to emerging threats and manage vulnerabilities. However, this transition is not without its challenges. The complexity of AI and ML systems often necessitates a high level of expertise that many organizations struggle to acquire and maintain, leading to difficulties in effectively implementing and managing these technologies. The substantial costs associated with AI and ML—ranging from hardware and software expenses to the need for specialized personnel—pose significant barriers, particularly for smaller organizations with limited budgets. Furthermore, ethical and legal concerns surrounding the use of AI and ML, such as issues of privacy, transparency, and bias, must be carefully addressed to ensure responsible and equitable deployment. The potential for these technologies to be exploited by malicious actors adds another layer of complexity, necessitating ongoing research and adaptation to stay ahead of evolving threats. To fully harness the benefits of AI and ML in cybersecurity while mitigating their risks, organizations will need to invest in training and development, explore alternative implementation strategies, and collaborate with policymakers to establish clear guidelines and standards. As the field continues to advance, a holistic approach that combines the strengths of AI and ML with traditional cybersecurity methods will be essential for achieving comprehensive protection against the ever-evolving landscape of cyber threats. Ultimately, the successful integration of AI and ML into cybersecurity practices will require a balanced and informed approach, one that addresses both the technological and ethical dimensions of these powerful tools, and fosters a collaborative effort among technologists, regulators, and stakeholders to safeguard digital assets and infrastructure effectively.

REFERENCES

1. Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2019). Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. Computer, 52(12), 45–52. https://doi.org/10.1109/MC.2019.2942584

2. S. Senthilkumar, V. Mohan & G.Chitrakala, “Evolutionary Algorithms for Solar Photovoltaic Parameters Estimation - A Review”, International Journal of Future Generation Communication and Networking, vol. 13, no. 2, pp. 348 – 360, 2020.
3. S. Senthilkumar, R. Nithya, P. Vaishali, R. Valli, G. Vanitha, & L. Ramachanndran, “Autonomous navigation robot”, International Research Journal of Engineering and Technology, vol. 4, no. 2, 2017.
4. S. Senthilkumar, C. Nivetha, G. Pavithra, G. Priyanka,S. Vigneshwari, L. Ramachandran, “Intelligent solar operated pesticide spray pump with cell charger”, International Journal For Research & Development In Technology, vol. 7, no. 2, pp. 285-287, 2017.
5. D. Nathangashree, L. Ramachandran, S. Senthilkumar & R. Lakshmirekha, “PLC based smart monitoring system for photovoltaic panel using GSM technology”, International Journal of Advanced Research in Electronics and Communication Engineering, vol. 5, no. 2, pp.251-255, 2016.
6. Senthilkumar. S, Lakshmi Rekha, Ramachandran. L & Dhivya. S, “Design and Implementation of secured wireless communication using Raspberry Pi”, International Research Journal of Engineering and Technology, vol. 3, no. 2, pp. 1015-1018, 2016.
7. Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in CyberSecurity: A survey. IEEE Access, 10, 93575–93600. https://doi. org/10.1109/ACCESS.2022.3204171
8. Cybernetics and systems. https://doi.org/10.1080/01969722.2022.2112539 AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. International Journal of Advanced Computer Science and Applications, 14(2), 801–809. https://doi.org/10.14569/ IJACSA.2023.0140292
9. Al-Khshali, H. H., & Ilyas, M. (2023). Impact of portable executable Header features on malware detection accuracy. Computers, Materials & Continua, 74(1), 153–178. https://doi.org/10.32604/cmc.2023.032182
10. Aliyari, M. (2021). Securing Industrial infrastructure against cyber-attacks using machine learning and artificial intelligence at the Age of industry 4.0. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 6581–6594.
11. Almeida, F., Santos, J. D., & Monteiro, J. A. (2020). The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. IEEE Engineering Management Review, 48(3), 97–103.
12. Bhandari, G., Lyth, A., Shalaginov, A., & Grønli, T.-M. (2023). Distributed deep neuralnetwork-based middleware for cyber-attacks detection in smart IoT ecosystem: A novel framework and performance evaluation approach. Electronics (Switzerland), 12 (2). https://doi.org/10.3390/electronics12020298
13. Brison, R., Wimmer, H., & Rebman, C. M. (2022). Botnet intrusion detection: A modern architecture to defend a virtual private cloud. Issues in Information Systems, 23(3), 114–127. https://doi.org/10.48009/3_iis_2022_110

IJARETY

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर
NISCAIR

International Journal of Advanced Research in Education and TechnologY (IJARETY)

www.ijarety.in editor.ijarety@gmail.com