World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

A comprehensive review of machine learning's role in enhancing network security and threat detection

Akoh Atadoga [1], Enoch Oluwademilade Sodiya [2, *], Uchenna Joseph Umoga [3] and Olukunle Oladipupo Amoo [4]

[1] *Independent Researcher, San Francisco, USA.*
[2] *Independent Researcher, UK.*
[3] *Independent Researcher, Seattle, Washington, USA.*
[4] *Department of Cybersecurity, University of Nebraska, Omaha, USA.*

World Journal of Advanced Research and Reviews, 2024, 21(02), 877–886

Publication history: Received on 03 January 2024; revised on 11 February 2024; accepted on 13 February 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.2.0501

Abstract

As network security threats continue to evolve in complexity and sophistication, there is a growing need for advanced solutions to enhance network security and threat detection capabilities. Machine learning (ML) has emerged as a powerful tool in this context, offering the potential to detect and mitigate threats in real-time by analyzing vast amounts of network data. This comprehensive review explores the role of machine learning in enhancing network security and threat detection. The review begins by providing an overview of the current landscape of network security threats and the challenges faced by traditional security approaches. It then delves into the fundamental principles of machine learning and its application to network security. Various machine learning techniques, including supervised learning, unsupervised learning, and deep learning, are discussed in detail, highlighting their strengths and limitations in the context of threat detection. Next, the review examines the application of machine learning in different aspects of network security, including intrusion detection, malware detection, anomaly detection, and behavioral analysis. Case studies and real-world examples are presented to illustrate the effectiveness of machine learning-based approaches in identifying and mitigating security threats. Furthermore, the review discusses the challenges and considerations associated with deploying machine learning in network security environments, such as data privacy, model interpretability, and adversarial attacks. Strategies for addressing these challenges and improving the robustness of machine learning models are explored. Finally, the review outlines future research directions and opportunities for leveraging machine learning to enhance network security. Areas such as federated learning, adversarial machine learning, and explainable AI are identified as promising avenues for further investigation. In summary, this comprehensive review provides insights into the potential of machine learning in enhancing network security and threat detection. By leveraging the capabilities of machine learning algorithms and techniques, organizations can strengthen their defenses against cyber threats and better protect their networks and sensitive data.

Keywords: Machine Learning; Network; Security; Threat; Detection

1. Introduction

In today's interconnected world, the prevalence of network security threats poses significant challenges to organizations across various sectors (Malhotra et al.,2021). From sophisticated cyberattacks to insider threats, the landscape of network security is constantly evolving, requiring robust defenses to safeguard sensitive data and infrastructure. As such, understanding the role of machine learning in enhancing network security and threat detection has become increasingly pertinent. Network security threats encompass a wide range of malicious activities aimed at compromising the confidentiality, integrity, and availability of network resources. These threats can manifest in various

[*] Corresponding author: Enoch Oluwademilade Sodiya

forms, including malware infections, phishing attacks, denial-of-service (DoS) attacks, and data breaches. With the proliferation of connected devices and digital technologies, the attack surface for potential threats has expanded, making effective security measures imperative (Djenna, 2021).

In modern environments, where digital assets play a crucial role in operations, ensuring robust network security is paramount (Muhammad et al.,2021). The consequences of security breaches can be severe, leading to financial losses, reputational damage, and legal repercussions. Moreover, in industries such as finance, healthcare, and critical infrastructure, the integrity and availability of network systems are essential for maintaining public trust and safety.

Machine learning has emerged as a powerful tool in the arsenal of cybersecurity professionals, offering the ability to detect and mitigate security threats in real-time (Shah, 2021). By leveraging algorithms and statistical models, machine learning techniques can analyze vast amounts of network data to identify patterns, anomalies, and potential security breaches. From intrusion detection to malware analysis, machine learning algorithms are increasingly being integrated into security solutions to augment human capabilities and enhance threat detection capabilities.

The purpose of this comprehensive review is to explore the role of machine learning in enhancing network security and threat detection (Asharf et al.,2020). By examining the fundamentals of machine learning, various techniques and methodologies, real-world applications, challenges, and future directions, this review aims to provide insights into how machine learning can be leveraged to bolster network security defenses. Through a thorough examination of existing literature and case studies, the review seeks to shed light on the potential of machine learning in addressing the evolving landscape of network security threats (Malhotra et al., 2021).

2. Fundamentals of Machine Learning

Machine learning (ML) has become increasingly prominent in the field of cybersecurity, offering innovative solutions for enhancing network security and threat detection (Shaukat et al.,2020). This section provides an in-depth exploration of the fundamentals of machine learning, including its definition, principles, types of algorithms, applications across various domains, and its relevance to network security and threat detection.

Machine learning is a subset of artificial intelligence (AI) that focuses on developing algorithms and statistical models that enable computers to learn from and make predictions or decisions based on data (Tyagi and Chahal, 2022.). Unlike traditional programming, where explicit instructions are provided to achieve a specific task, machine learning algorithms learn iteratively from data and improve their performance over time. The fundamental principles of machine learning include: Machine learning algorithms rely on data to identify patterns, relationships, and insights that can be used to make predictions or decisions. Machine learning models improve their performance by learning from past experiences and adjusting their parameters accordingly. Machine learning algorithms are designed to generalize from training data to make predictions on unseen or new data. Machine learning involves optimizing algorithms to minimize errors or maximize performance metrics through techniques such as gradient descent and backpropagation (Haji and Abdulazeez, 2021).

Machine learning algorithms can be categorized into several types based on their learning approach and application domain, Supervised Learning: In supervised learning, algorithms are trained on labeled data, where each input is associated with a corresponding output or target variable (Antoniadis ,2021). Common supervised learning algorithms include linear regression, logistic regression, decision trees, random forests, support vector machines (SVM), and neural networks. Unsupervised learning algorithms are trained on unlabeled data, and the goal is to uncover hidden patterns or structures within the data. Clustering algorithms, such as K-means clustering and hierarchical clustering, and dimensionality reduction techniques, such as principal component analysis (PCA) and t-distributed stochastic neighbor embedding (t-SNE), are examples of unsupervised learning. Semi-supervised learning combines elements of supervised and unsupervised learning by leveraging a small amount of labeled data in conjunction with a large amount of unlabeled data. This approach is particularly useful when labeled data is scarce or expensive to obtain. Reinforcement learning is a type of machine learning where an agent learns to interact with an environment by taking actions and receiving feedback in the form of rewards or penalties. The agent learns to maximize cumulative rewards over time through trial and error. Algorithms such as Q-learning and deep Q-networks (DQN) are commonly used in reinforcement learning. Deep learning is a subfield of machine learning that focuses on training deep neural networks with multiple layers of interconnected neurons. Deep learning algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated remarkable success in tasks such as image recognition, natural language processing, and speech recognition (Torfi et al.,2020).

Machine learning has found applications across a wide range of domains, including healthcare, finance, retail, marketing, transportation, and cybersecurity (Sarker, 2021). Some common applications of machine learning include: Machine learning algorithms are used to predict future outcomes or trends based on historical data. This includes applications such as sales forecasting, customer churn prediction, and disease diagnosis. Machine learning techniques are applied to analyze and understand human language, enabling tasks such as sentiment analysis, language translation, and text summarization. Machine learning algorithms are used to interpret and analyze visual data, such as images and videos. Applications include object detection, image classification, and facial recognition. Machine learning is used to develop autonomous systems that can perceive and interact with their environment, such as self-driving cars, drones, and robotic systems (Soori ,2023).

In the context of network security and threat detection, machine learning plays a crucial role in augmenting traditional security measures and enabling proactive defense mechanisms (Bouchama and Kamal, 2021). Machine learning techniques are used to analyze large volumes of network data, detect patterns indicative of malicious activity, and identify emerging threats in real-time. By leveraging machine learning, organizations can enhance their ability to detect, prevent, and respond to cyber threats more effectively. Additionally, machine learning enables adaptive and dynamic security measures that can evolve in response to changing threat landscapes, providing a more resilient defense against cyberattacks (Babu, 2024).

This section has provided an overview of the fundamentals of machine learning, including its definition, principles, types of algorithms, applications across various domains, and relevance to network security and threat detection (Dasgupta ,2022). Understanding these fundamental concepts lays the groundwork for exploring the role of machine learning in enhancing network security in subsequent sections of this review.

3. Machine Learning Techniques for Network Security

In the realm of network security, the adoption of machine learning techniques has revolutionized the way organizations detect and mitigate threats (Rawindaran ,2021). This section explores various machine learning techniques applied to network security, including intrusion detection systems (IDS), malware detection, anomaly detection, and behavioral analysis. Each technique encompasses distinct methodologies aimed at bolstering network defenses and safeguarding against evolving cyber threats. Intrusion detection systems play a critical role in identifying unauthorized access attempts, malicious activities, and potential security breaches within a network. Machine learning techniques enhance IDS capabilities by enabling automated detection and response mechanisms.

Signature-based detection relies on predefined patterns or signatures of known attacks to identify malicious activities (Díaz et al.,2022; Uddin et al., 2022). Machine learning algorithms can effectively match network traffic patterns against a database of signatures, enabling rapid detection of known threats. Anomaly-based detection identifies deviations from normal network behavior, indicating potential security breaches. Machine learning algorithms learn the baseline behavior of the network and flag anomalies that deviate significantly from the norm, allowing for the detection of novel and zero-day attacks. Hybrid intrusion detection systems combine both signature-based and anomaly-based detection techniques to leverage the strengths of each approach. Machine learning algorithms play a crucial role in analyzing network data, identifying patterns, and distinguishing between normal and malicious activities to enhance detection accuracy (Rabbani et al.,.2021; Adegoke et al., 2023).

Malware poses a significant threat to network security, encompassing various forms of malicious software designed to disrupt operations, steal sensitive information, or gain unauthorized access (Ngo ,2020). Machine learning techniques are employed in malware detection to identify and mitigate these threats effectively. Key methodologies, Static analysis examines the code and characteristics of files to identify potential malware threats without executing them. Machine learning algorithms analyze file attributes, such as file size, metadata, and code structure, to classify files as benign or malicious. Dynamic analysis involves executing files in a controlled environment to observe their behavior and identify malicious activities. Machine learning algorithms analyze runtime behavior, system calls, and network traffic generated by the executable to detect and classify malware. Behavior-based detection focuses on monitoring the behavior of software or processes to identify malicious activities. Machine learning algorithms analyze patterns of behavior and classify them as either benign or suspicious, enabling the detection of previously unseen malware variants (Aslan and Yilmaz, 2021; Ikechukwu et al., 2019).

Anomaly detection techniques aim to identify abnormal or unusual patterns in network traffic, indicating potential security threats or malicious activities (Coker et al., 2023; Ali et al.,2020). Machine learning algorithms are instrumental in detecting anomalies and distinguishing them from legitimate network behavior. Common approaches include Statistical anomaly detection relies on mathematical models to identify deviations from expected patterns in network data. Machine learning algorithms, such as Gaussian mixture models and autoencoders, analyze network traffic statistics to detect anomalies indicative of security breaches. Clustering algorithms group network data into clusters based on similarity, enabling the identification of outliers or anomalies. Machine learning algorithms, such as k-means clustering and DBSCAN, cluster network traffic data and flag clusters with unusual characteristics as potential anomalies. Deep learning techniques, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), excel at learning complex patterns and features from raw network data. These algorithms analyze network traffic sequences or data streams to detect anomalies and identify potential security threats with high accuracy (Bouchama and Kamal, 2021; Ikwue et al., 2023).

Behavioral analysis focuses on monitoring and analyzing user behavior, network traffic patterns, and endpoint activities to detect and mitigate security threats (Sivanathan, 2020). Machine learning techniques play a crucial role in behavioral analysis by identifying suspicious behavior and flagging potential security incidents. Key areas of focus include Machine learning algorithms analyze user activities, login patterns, and access privileges to detect anomalous behavior indicative of insider threats or unauthorized access attempts. Machine learning techniques analyze network traffic patterns, protocols, and communication behaviors to detect anomalies, intrusion attempts, and malicious activities, such as denial-of-service (DoS) attacks or data exfiltration. Machine learning algorithms monitor endpoint devices, such as desktops, laptops, and servers, to identify abnormal activities or deviations from normal behavior. Endpoint behavior analysis enables the detection of malware infections, unauthorized access attempts, and suspicious system modifications (Oguejiofor et al., 2023; Arfeen et al.,2021).

Machine learning techniques play a pivotal role in enhancing network security and threat detection by enabling automated detection, analysis, and response mechanisms (Venkatesan and Rahayu, 2024). From intrusion detection to malware analysis and anomaly detection, machine learning algorithms leverage advanced analytics and pattern recognition to identify and mitigate security threats effectively. By leveraging machine learning in network security, organizations can bolster their defenses, detect emerging threats, and safeguard sensitive data and assets against evolving cyber threats.

4. Applications and Case Studies

The application of machine learning techniques in network security has revolutionized the way organizations detect, prevent, and respond to cyber threats (Shaukat et al.,2020). This section explores various real-world applications and case studies that demonstrate the effectiveness of machine learning in enhancing network security and threat detection. Through the implementation of machine learning algorithms, organizations can achieve proactive defense mechanisms and mitigate security risks effectively.

Machine learning techniques are widely deployed across diverse real-world scenarios to enhance network security and detect potential threats (Evtimov et al.,2020; Oyetunde et al., 2016). Some common applications include: Machine learning algorithms are utilized in IDS to identify and respond to unauthorized access attempts, anomalous behaviors, and potential security breaches. By analyzing network traffic patterns and identifying abnormal activities, machine learning-based IDS can effectively detect and mitigate threats in real-time. Machine learning techniques play a crucial role in malware detection by analyzing file attributes, code structures, and behavioral patterns to identify and classify malicious software. Through static and dynamic analysis, machine learning-based malware detection systems can accurately detect and mitigate various types of malware threats, including viruses, worms, and ransomware. Machine learning algorithms are employed in anomaly detection systems to identify deviations from normal network behavior, indicating potential security threats or malicious activities. By learning the baseline behavior of the network and flagging anomalies, machine learning-based anomaly detection systems can effectively detect and respond to emerging threats in real-time. Machine learning techniques are used in behavioral analysis to monitor and analyze user activities, network traffic patterns, and endpoint behaviors. By identifying suspicious behavior and abnormal activities, machine learning-based behavioral analysis systems can detect insider threats, unauthorized access attempts, and malicious activities targeting network infrastructure.

Several case studies highlight the effectiveness of machine learning in enhancing network security and threat detection across different industries and organizational settings (Chen ,2021; Oguejiofor et al., 2023). Some notable examples. In a large financial services organization, machine learning-based anomaly detection systems were implemented to identify fraudulent transactions and suspicious activities in real-time. By analyzing transactional data, user behaviors, and network traffic patterns, the system successfully detected and prevented fraudulent activities, resulting in significant cost savings and improved security posture. In a healthcare environment, machine learning-based malware detection systems were deployed to protect sensitive patient data and critical infrastructure from cyber threats. By analyzing file attributes, network traffic, and endpoint behaviors, the system effectively detected and mitigated malware infections, ensuring the integrity and confidentiality of patient information. In an e-commerce platform, machine learning-based IDS were employed to safeguard customer data, prevent unauthorized access, and mitigate security risks. By analyzing user activities, login patterns, and transactional data, the system successfully detected and responded to security incidents, ensuring a secure and trustworthy shopping experience for customers.

Numerous successful applications of machine learning for threat detection exist across various industries and domains (Khalil et al.,2021). Machine learning algorithms are used to analyze network traffic patterns, detect anomalous behaviors, and identify potential security threats, such as unauthorized access attempts, malware infections, and denial-of-service (DoS) attacks. Machine learning techniques are employed in email security solutions to identify and block phishing attempts, spam emails, and malicious attachments. By analyzing email content, sender reputation, and attachment files, machine learning-based email security systems can effectively detect and prevent email-based threats. Machine learning algorithms are utilized in endpoint security solutions to protect devices from malware infections, ransomware attacks, and other security threats. By monitoring endpoint activities, analyzing system behaviors, and detecting malicious software, machine learning-based endpoint security systems can prevent data breaches and protect sensitive information.

The implementation of machine learning techniques in real-world scenarios has demonstrated significant effectiveness in enhancing network security and threat detection (Nassar and Kamal, 2021). Through the deployment of machine learning-based intrusion detection systems, malware detection solutions, anomaly detection systems, and behavioral analysis tools, organizations can achieve proactive defense mechanisms and mitigate security risks effectively. Case studies and examples from various industries highlight the versatility and efficacy of machine learning in addressing diverse security challenges and safeguarding critical assets against evolving cyber threats. As organizations continue to embrace machine learning technologies, the role of machine learning in network security will become increasingly prominent, driving innovation and resilience in cybersecurity practices (Olowononi ,2020).

5. Challenges and Considerations

The integration of machine learning (ML) techniques in network security and threat detection brings about various benefits, but it also introduces several challenges and considerations (Haider et al.,2020). This section discusses key challenges and considerations associated with the use of ML in enhancing network security and threat detection, including data privacy and security concerns, model interpretability and explainability, adversarial attacks and robustness, scalability and computational complexity, and regulatory compliance and ethical considerations.

One of the primary challenges in applying ML to network security is ensuring the privacy and security of sensitive data used for training and testing ML models (Liu et al.,2020). Network security datasets often contain confidential information, such as IP addresses, user credentials, and network configurations, which could be exploited if not adequately protected. Moreover, sharing or transferring datasets between organizations may pose risks of data breaches or unauthorized access. Addressing data privacy and security concerns requires implementing robust data encryption, access control mechanisms, and anonymization techniques to safeguard sensitive information while enabling effective ML model training.

ML models used for network security often exhibit complex behaviors and decision-making processes, making it challenging to interpret and understand their predictions (Azam and Huda, 2023). Lack of model interpretability and explainability can hinder trust and transparency in ML-based security systems, especially in critical applications where human oversight is necessary. Therefore, ensuring the interpretability of ML models is crucial for identifying potential biases, errors, or vulnerabilities and for providing actionable insights to security analysts. Techniques such as feature importance analysis, model visualization, and rule extraction algorithms can enhance the interpretability of ML models and facilitate human understanding of their decision-making processes.

Adversarial attacks pose significant threats to ML-based security systems, as attackers may exploit vulnerabilities in ML models to manipulate or evade detection mechanisms (Alotaibi and Rassam, 2023; Ukoba and Jen, 2023). Adversarial attacks can manifest in various forms, including data poisoning, evasion attacks, and model inversion attacks, aiming to deceive ML models and compromise network security. Ensuring the robustness of ML-based security systems requires employing defense mechanisms such as adversarial training, model diversification, and robust optimization techniques to mitigate the impact of adversarial attacks and enhance the resilience of ML models against manipulation and exploitation (Silva and Najafirad, 2020).

ML algorithms used for network security often require significant computational resources and processing power, particularly when dealing with large-scale datasets and complex network environments (Anamu et al., 2023; Sarker et al.,2023). Scalability and computational complexity issues can arise when deploying ML-based security solutions in real-world settings, especially in high-volume network traffic scenarios or resource-constrained environments. Therefore, optimizing ML algorithms for scalability and efficiency is essential for ensuring the practicality and feasibility of deploying ML-based security systems in diverse network environments.

The use of ML in network security raises various regulatory compliance and ethical considerations related to data protection, privacy rights, and algorithmic fairness (Fabian et al., 2023; Dhirani et al.,2023). Organizations must adhere to relevant data protection regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), to ensure lawful and ethical use of personal data for ML model training and deployment. Additionally, addressing algorithmic biases and ensuring fairness and transparency in ML-based security systems is essential for upholding ethical standards and mitigating potential discriminatory impacts on individuals or groups.

Addressing the challenges and considerations associated with the use of ML in enhancing network security and threat detection is essential for realizing the full potential of ML-based security systems (Koay et al.,2023; Uchechukwu et al., 2023). By prioritizing data privacy and security, enhancing model interpretability and explainability, mitigating adversarial attacks, optimizing scalability and computational complexity, and adhering to regulatory compliance and ethical standards, organizations can effectively harness the benefits of ML while minimizing risks and vulnerabilities in network security operations. As ML technologies continue to evolve, ongoing research and collaboration across academia, industry, and regulatory bodies are necessary to address emerging challenges and ensure the responsible and ethical use of ML in network security practices (Ahmad et al.,2022).

6. Future Directions and Research Opportunities

Network security practices play a crucial role in safeguarding digital assets, protecting sensitive information, and ensuring the integrity and availability of network resources (Arogundade, 2023). This section explores future directions and research opportunities in network security practices, focusing on emerging trends and advancements in machine learning (ML) for enhancing network security, areas for further research and development, and strategies for addressing current challenges and limitations.

The integration of ML techniques in network security has witnessed significant advancements and innovations, paving the way for more effective and adaptive security solutions (Stasevych and Zvarych, 2023). Deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are increasingly being applied to network intrusion detection systems (NIDS) for detecting and mitigating sophisticated cyber threats. Deep learning models can effectively analyze network traffic patterns, identify anomalous behaviors, and classify malicious activities with high accuracy and efficiency. Federated learning enables collaborative model training across distributed network environments without centralized data aggregation, preserving data privacy and security. By leveraging federated learning techniques, organizations can collectively train ML models on locally stored data from multiple network nodes, facilitating the development of robust and privacy-preserving security solutions. Explainable AI techniques aim to enhance the interpretability and transparency of ML models used in network security operations. By providing insights into the decision-making processes of ML models, explainable AI techniques enable security analysts to understand, validate, and trust the recommendations and predictions generated by ML-based security systems (Kumar et al.,2023).

Despite significant progress, several areas in network security practices warrant further research and development to address emerging threats and enhance resilience against evolving cyber risks. Advancing techniques for adversarial machine learning to improve the robustness and resilience of ML-based security systems against adversarial attacks, evasion techniques, and model manipulation strategies. Developing privacy-preserving ML algorithms and protocols to protect sensitive data and ensure confidentiality while enabling collaborative model training and information sharing across networked environments. Designing context-aware security solutions that leverage contextual information, such as network topology, user behavior, and environmental factors, to adaptively respond to dynamic security threats and mitigate risks in real-time (Rangaraju, 2023).

To overcome current challenges and limitations in network security practices, organizations can adopt several strategies: Foster collaboration and knowledge-sharing among researchers, industry practitioners, and academia to address complex security challenges, exchange best practices, and accelerate innovation in network security. Invest in training and education programs to equip security professionals with the necessary skills, knowledge, and expertise to effectively deploy and manage ML-based security solutions and respond to emerging cyber threats. Adhere to industry best practices, standards, and guidelines for network security, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to ensure comprehensive risk management, regulatory compliance, and adherence to security principles.

The future of network security practices holds immense potential for leveraging ML techniques to enhance threat detection, incident response, and risk mitigation strategies (Hassan, and Ibrahim, 2023). By embracing emerging trends in ML, exploring new research avenues, and implementing proactive strategies to address current challenges and limitations, organizations can strengthen their defense mechanisms, adapt to evolving cyber threats, and safeguard network infrastructure against sophisticated attack s (Safitra ,2023). Collaborative efforts, continuous innovation, and a commitment to excellence are essential for advancing network security practices and building resilient and secure digital ecosystems in the face of evolving cyber risks (Muhammad et al.,2022)

7. Conclusion

In conclusion, this comprehensive review has highlighted the significant role of machine learning (ML) in enhancing network security and threat detection. Through an exploration of fundamental concepts, methodologies, applications, challenges, and future directions, several key findings and insights have emerged. The review elucidated the fundamentals of ML, including its principles, algorithms, and applications across various domains. Specifically, it examined how ML techniques such as intrusion detection systems, malware detection, anomaly detection, and behavioral analysis contribute to bolstering network security measures. Furthermore, the review underscored the importance of interpretability, scalability, and ethical considerations in ML-based security solutions.

The insights gleaned from this review have significant implications for network security practices. By leveraging ML technologies, organizations can fortify their defenses against sophisticated cyber threats, improve incident response capabilities, and enhance overall security posture. ML-based approaches offer the potential to detect previously unseen threats, adapt to evolving attack vectors, and minimize false positives, thereby augmenting the effectiveness of security operations.

To further advance the role of ML in network security and threat detection, several recommendations are proposed. Firstly, continued research and development efforts should focus on refining ML algorithms, enhancing model interpretability, and addressing challenges related to scalability and adversarial attacks. Additionally, fostering interdisciplinary collaboration between academia, industry, and regulatory bodies can accelerate innovation and knowledge-sharing in the field of ML-based security. Moreover, organizations should prioritize investment in training and education initiatives to equip security professionals with the necessary skills and expertise to deploy and manage ML-driven security solutions effectively.

In conclusion, the integration of ML holds immense promise for bolstering network security practices. By embracing the insights garnered from this review and implementing proactive strategies, organizations can navigate the evolving threat landscape with confidence, resilience, and adaptability, safeguarding critical assets and infrastructure in an increasingly digital world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adegoke, A., (2023). Patients' Reaction to Online Access to Their Electronic Medical Records: The Case of Diabetic Patients in the US. International Journal of Applied Sciences: Current and Future Research Trends, 19 (1), pp 105-115

[2] Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J. and Al-Fuqaha, A., 2022. Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, p.100452.

[3] Ali, W.A., Manasa, K.N., Bendechache, M., Fadhel Aljunaid, M. and Sandhya, P., 2020. A review of current machine learning approaches for anomaly detection in network traffic. *Journal of Telecommunications and the Digital Economy*, *8*(4), pp.64-95.

[4] Alotaibi, A. and Rassam, M.A., 2023. Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. *Future Internet*, *15*(2), p.62.

[5] Anamu, U.S., Ayodele, O.O., Olorundaisi, E., Babalola, B.J., Odetola, P.I., Ogunmefun, A., Ukoba, K., Jen, T.C. and Olubambi, P.A., 2023. Fundamental design strategies for advancing the development of high entropy alloys for thermo-mechanical application: A critical review. *Journal of Materials Research and Technology*.

[6] Antoniadis, A., Lambert-Lacroix, S. and Poggi, J.M., 2021. Random forests for global sensitivity analysis: A selective review. *Reliability Engineering & System Safety*, *206*, p.107312.

[7] Arfeen, A., Ahmed, S., Khan, M.A. and Jafri, S.F.A., 2021, November. Endpoint detection & response: A malware identification solution. In *2021 International Conference on Cyber Warfare and Security (ICCWS)* (pp. 1-8). IEEE.

[8] Arogundade, O.R., 2023. Network Security Concepts, Dangers, and Defense Best Practical. *Computer Engineering and Intelligent Systems*, *14*(2).

[9] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W. and Wahab, A., 2020. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics*, *9*(7), p.1177.

[10] Aslan, Ö. and Yilmaz, A.A., 2021. A new malware classification framework based on deep learning algorithms. *Ieee Access*, *9*, pp.87936-87951.

[11] Azam, Z., Islam, M.M. and Huda, M.N., 2023. Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree. *IEEE Access*.

[12] Babu, C.S., 2024. Adaptive AI for Dynamic Cybersecurity Systems: Enhancing Protection in a Rapidly Evolving Digital Landscap. In *Principles and Applications of Adaptive Artificial Intelligence* (pp. 52-72). IGI Global.

[13] Bouchama, F. and Kamal, M., 2021. Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. *International Journal of Business Intelligence and Big Data Analytics*, *4*(9), pp.1-9.

[14] Chen, D., Wawrzynski, P. and Lv, Z., 2021. Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities and Society*, *66*, p.102655.

[15] Coker, J.O., Uzougbo, N.S., Oguejiofor, B.B. and Akagha, O.V., 2023. The Role Of Legal Practitioners In Mitigating Corporate Risks In Nigeria: A Comprehensive Review Of Existing Literature On The Strategies And Approaches Adopted By Legal Practitioners In NIGERIA TO MITIGATE CORPORATE RISKS. *Finance & Accounting Research Journal*, *5*(10), pp.309-332.

[16] Dasgupta, D., Akhtar, Z. and Sen, S., 2022. Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, *19*(1), pp.57-106.

[17] Dhirani, L.L., Mukhtiar, N., Chowdhry, B.S. and Newe, T., 2023. Ethical dilemmas and privacy issues in emerging technologies: a review. *Sensors*, *23*(3), p.1151.

[18] Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R. and Madinabeitia, G., 2022. On the detection capabilities of signature-based intrusion detection systems in the context of web attacks. *Applied Sciences*, *12*(2), p.852.

[19] Djenna, A., Harous, S. and Saidouni, D.E., 2021. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), p.4580.

[20] Evtimov, I., Cui, W., Kamar, E., Kiciman, E., Kohno, T. and Li, J., 2020. Security and machine learning in the real world. *arXiv preprint arXiv:2007.07205*.

[21] Fabian, A.A., Uchechukwu, E.S., Okoye, C.C. and Okeke, N.M., (2023). Corporate Outsourcing and Organizational Performance in Nigerian Investment Banks. *Sch J Econ Bus Manag, 2023Apr*, *10*(3), pp.46-57.

[22] Haider, N., Baig, M.Z. and Imran, M., 2020. Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends. *arXiv preprint arXiv:2007.04490*.

[23] Haji, S.H. and Abdulazeez, A.M., 2021. Comparison of optimization techniques based on gradient descent algorithm: A review. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(4), pp.2715-2743.

[24] Hassan, S.K. and Ibrahim, A., 2023. The role of artificial intelligence in cyber security and incident response. *International Journal for Electronic Crime Investigation*, *7*(2).

[25] Ikechukwu, I.J., Anyaoha, C., Abraham, K.U. and Nwachukwu, E.O., 2019. Transient analysis of segmented Di-trapezoidal variable geometry thermoelement. NIEEE Nsukka Chapter Conference. pp.338-348

[26] Ikwue, U., Ekwezia, A.V., Oguejiofor, B.B., Agho, M.O. and Daraojimba, C., 2023. Sustainable Investment Strategies In Pension Fund Management: A Comparative Review Of Esg Principles Adoption In The US AND NIGERIA. *International Journal of Management & Entrepreneurship Research*, *5*(9), pp.652-673.

[27] Khalil, R.A., Saeed, N., Masood, M., Fard, Y.M., Alouini, M.S. and Al-Naffouri, T.Y., 2021. Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications. *IEEE Internet of Things Journal*, *8*(14), pp.11016-11040.

[28] Koay, A.M., Ko, R.K.L., Hettema, H. and Radke, K., 2023. Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*, *60*(2), pp.377-405.

[29] Kumar, P., Wazid, M., Singh, D.P., Singh, J., Das, A.K., Park, Y. and Rodrigues, J.J., 2023. Explainable artificial intelligence envisioned security mechanism for cyber threat hunting. *Security and Privacy*, *6*(6), p.e312.

[30] Liu, X., Xie, L., Wang, Y., Zou, J., Xiong, J., Ying, Z. and Vasilakos, A.V., 2020. Privacy and security issues in deep learning: A survey. *IEEE Access*, *9*, pp.4566-4593.

[31] Malhotra, P., Singh, Y., Anand, P., Bangotra, D.K., Singh, P.K. and Hong, W.C., 2021. Internet of things: Evolution, concerns and security challenges. *Sensors*, *21*(5), p.1809.

[32] Muhammad, T., Munir, M.T., Munir, M.Z. and Zafar, M.W., 2022. Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future. *International Journal of Computer Science and Technology*, *6*(4), pp.99-135.

[33] Muhammad, T., Munir, M.T., Munir, M.Z. and Zafar, M.W., 2022. Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future. *International Journal of Computer Science and Technology*, *6*(4), pp.99-135.

[34] Nassar, A. and Kamal, M., 2021. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), pp.51-63.

[35] Ngo, F.T., Agarwal, A., Govindu, R. and MacDonald, C., 2020. Malicious software threats. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp.793-813.

[36] Oguejiofor, B.B., Omotosho, A., Abioye, K.M., Alabi, A.M., Oguntoyinbo, F.N., Daraojimba, A.I. and Daraojimba, C., 2023. A review on data-driven regulatory compliance in Nigeria. *International Journal of applied research in social sciences*, *5*(8), pp.231-243.

[37] Oguejiofor, B.B., Uzougbo, N.S., Kolade, A.O., Raji, A. and Daraojimba, C., 2023. Review of Successful Global Public-Private Partnerships: Extracting key Strategies for Effective US Financial Collaborations. *International Journal of Research and Scientific Innovation*, *10*(8), pp.312-331.

[38] Olowononi, F.O., Rawat, D.B. and Liu, C., 2020. Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS. *IEEE Communications Surveys & Tutorials*, *23*(1), pp.524-552.

[39] Oyetunde, O.A., Oluwafemi, O.K. and Bisola, A.M., 2016. Impact of vocational and entrepreneurship education on the economic growth of Ogun State, Nigeria. *Makerere Journal of Higher Education*, *8*(1), pp.25-33.

[40] Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Bagheri Baba Ahmadi, S. and Ayobi, S., 2021. A review on machine learning approaches for network malicious behavior detection in emerging technologies. *Entropy*, *23*(5), p.529.

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

[42] Rawindaran, N., Jayal, A. and Prakash, E., 2021. Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), p.150.

[43] Safitra, M.F., Lubis, M. and Fakhrurroja, H., 2023. Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), p.13369.

[44] Sarker, I.H., 2021. Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), p.160.

[45] Sarker, I.H., Khan, A.I., Abushark, Y.B. and Alsolami, F., 2023. Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, *28*(1), pp.296-312.

[46] Shah, V., 2021. Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), pp.19-42.

[47] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A. and Xu, M., 2020. A survey on machine learning techniques for cyber security in the last decade. *IEEE access*, *8*, pp.222310-222354.

[48] Silva, S.H. and Najafirad, P., 2020. Opportunities and challenges in deep learning adversarial robustness: A survey. *arXiv preprint arXiv:2007.00753*.

[49] Sivanathan, A., 2020. IoT behavioral monitoring via network traffic analysis. *arXiv preprint arXiv:2001.10632*.

[50] Soori, M., Arezoo, B. and Dastres, R., 2023. Artificial intelligence, machine learning and deep learning in advanced robotics, A review. *Cognitive Robotics*.

[51] Stasevych, M. and Zvarych, V., 2023. Innovative robotic technologies and artificial intelligence in pharmacy and medicine: paving the way for the future of health care—a review. *Big Data and Cognitive Computing*, *7*(3), p.147.

[52] Torfi, A., Shirvani, R.A., Keneshloo, Y., Tavaf, N. and Fox, E.A., 2020. Natural language processing advancements by deep learning: A survey. *arXiv preprint arXiv:2003.01200*.

[53] Tyagi, A.K. and Chahal, P., 2022. Artificial intelligence and machine learning algorithms. In *Research Anthology on Machine Learning Techniques, Methods, and Applications* (pp. 421-446). IGI Global.

[54] Uchechukwu, E.S., Amechi, A.F., Okoye, C.C. and Okeke, N.M., 2023. Youth Unemployment and Security Challenges in Anambra State, Nigeria. *Sch J Arts Humanit Soc Sci*, *4*, pp.81-91.

[55] Uddin, S.U., Chidolue, O., Azeez, A. and Iqbal, T., 2022, June. Design and Analysis of a Solar Powered Water Filtration System for a Community in Black Tickle-Domino. In *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-6). IEEE.

[56] Ukoba, K. and Jen, T.C., 2023. Thin films, atomic layer deposition, and 3D Printing: demystifying the concepts and their relevance in industry 4.0. CRC Press.

[57] Venkatesan, K. and Rahayu, S.B., 2024. Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. *Scientific Reports*, *14*(1), p.1149