# A Review of Network Vulnerability Scanner Tool with Integrated AI-Driven Threat Intelligence

Mujahid Hussain
Department of ICE
Faculty of Engineering
Bahawalpur, Pakistan
mujahid92472@gmail.com

Hamza Khazir
Department of ICE
Faculty of Engineering
Bahawalpur , Pakistan
hamzakh4767@gmail.com

Muhammad Mujahid
Department of ICE
Faculty of Engineering
Bahawalpur , Pakistan
malik148wb@gmail.com

Abdul Rehman Chishti
Department of ICE
Faculty of Engineering
Bahawalpur , Pakistan
rehmanchishti@gmail.com

***Abstract*—This paper examines current trends in vulnerability scanners based on threat intelligence powered by artificial intelligence. It explores how machine learning and deep learning, two types of artificial intelligence, enhance Qualys, OpenVAS, and Nessus, among other software packages. The report underlines the benefits of incorporating AI into real-time threat detection, contextual risk assessment, automated prioritization, and predictive analytics. Using research and case studies, it demonstrates how AI improves cybersecurity systems' accuracy, scalability, and response time. The study also examines architectural and operational advances in vulnerability management enabled by automation and sensible decisions. Furthermore, it addresses challenges such as algorithmic bias, data privacy, and ethical considerations, encouraging greater research into transparent and safe AI for cybersecurity.**

***Index Terms*—Network Vulnerability, Vulnerability scanning, Vulnerability scanner Tool, AI-Driven threat intelligence**

## I. Introduction

The author in [1] has discussed the Actor-Network Theory of cybersecurity, viewing humans and technology as active agents. It highlights security as a continuous, relational activity. A comprehensive, socio-technical viewpoint is preferred over just technological solutions. The author in [2] has discussed a machine learning-based intrusion detection system that employs Decision Trees and SVM methods. It trains on the KDD Cup 99 dataset. The results show greater accuracy and fewer false alarms. The author in [3] presents a safe cloud storage infrastructure that employs hybrid encryption with ChaCha20 and AES. ChaCha20 encrypts the AES key, improving security while minimizing performance loss. The results indicate increased security against threats while preserving efficiency. The author in [4] has discussed vulnerability scanning technologies such as Nmap and Nessus for network security, focusing on VAPT. It evaluates their efficiency in detecting risks, like as SQL injection, and recommends more complex methods, such as POMDP, for increased accuracy. VAPT is important for effective cyber protection. The author in [5] has discussed how artificial intelligence (AI), namely deep learning and reinforcement learning, improves network performance by optimizing routing, managing traffic, and enhancing security. AI models outperform traditional methods, with latency reduced by up to 30 percent and intrusion detection accuracy of 97 percent. Real-world applications highlight AI's ability to build better, more resilient network infrastructures. The author in [6] has discussed how AI improves cybersecurity (for example, malware detection), yet it is permitting to adversarial attacks. Examines ML/DL techniques for security and defense against AI threats.Calls for secure AI systems, particularly in distributed learning, and suggests further study. The author in [7] has discussed a tool that merges Nessus and OpenVAS information and generates simplified summaries using OpenAI's API. It automates difficult report combining, making results available to non-experts. Plans include additional tools, GPT-4 integration, and interactive dashboards. The author in [8] has discussed how artificial intelligence (AI) revolutionizes cybersecurity by enabling real-time threat detection, minimizing false positives, and identifying zero-day vulnerabilities. It also improves risk management by using predictive analytics to better allocate resources and make decisions. The author in [9] has discussed how AI can improve telecom security through real-time detection, predictive analytics, and automation. Case studies show improved sensivity and fewer breaches, but also highlight obstacles and the need for ethical AI, blockchain, and quantum solutions. The author in [10] has discussed. The paper looks at the rising role of artificial intelligence in automating threat detection and response. I imagine a future in which AI systems aggressively seek hazards without human intervention, utilizing big data analytics, machine learning, and threat intelligence. This model seeks to acutely cut response time, improve threat visibility, and strengthen overall cybersecurity view in complex contexts. The author in [11] has discussed a project proposal, which describes a tool that combines standard network scanning (e.g., port, service, OS, and vulnerability detection) with AI to improve threat analysis and prediction. Real-time scanning, threat intelligence integration, PDF report production, and a user-friendly interface are among the key features, with plans to deploy web and Android apps as well. The plan prioritizes innovation, real-world application, and academic and professional recognition through publications and challenges. The author in [12] has discussed how to improve Cyber Threat Intelligence (CTI) by combining counterintelligence approaches and offensive operations. It focuses on proactive defense methods, such as


DOI: https://doi.org/10.67535/tsp.000001.039
Published under the ICACNC 2025 Proceedings

deception and counterattacks, to disrupt rivals and improve cybersecurity posture.

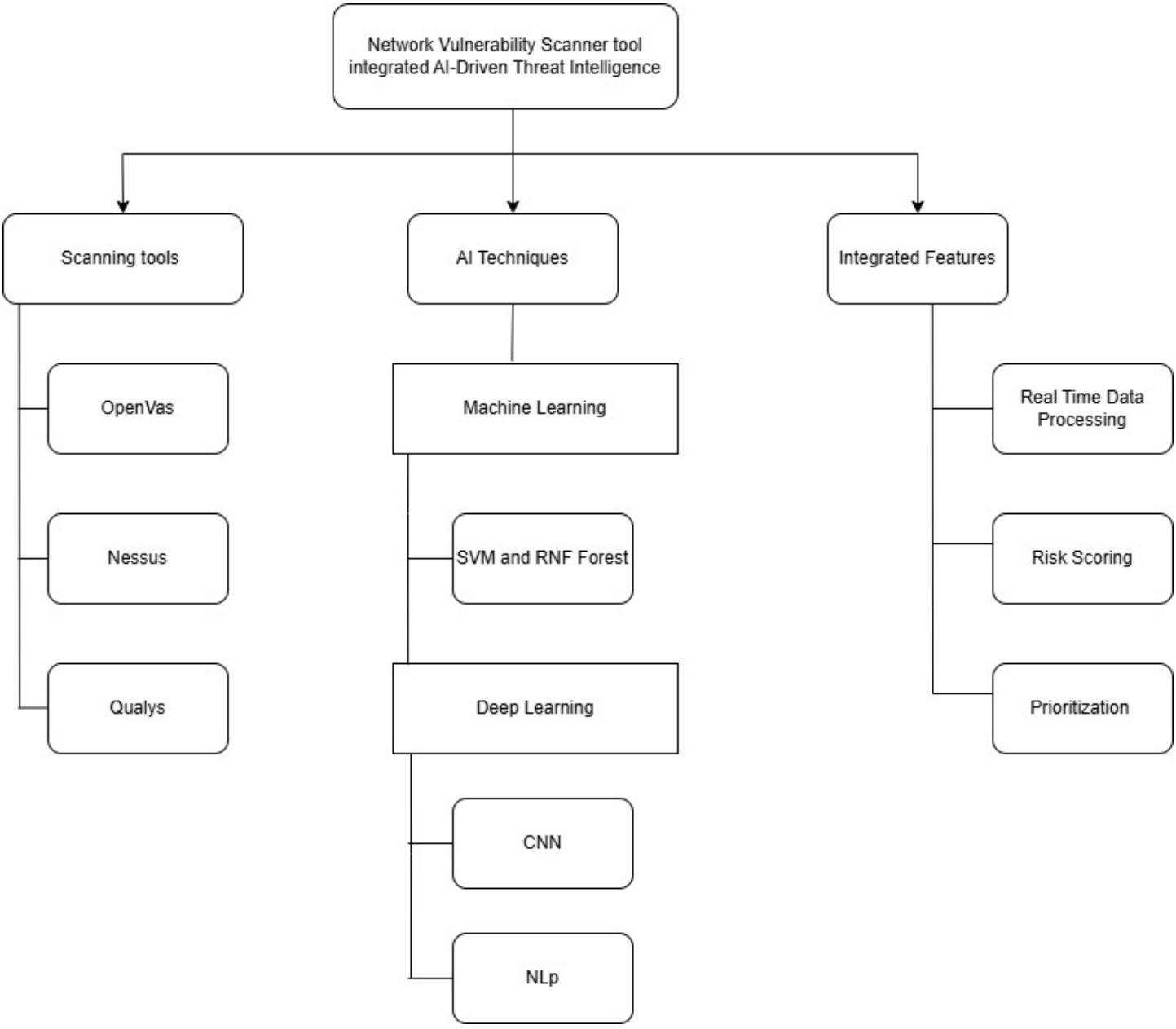


Fig. 1. vulnerability scanner Tool

The author in [13] has discussed a next-generation cyber-threat intelligence platform (TIP) to perform holistic real-time risk assessments in IT and OT systems. It finds gaps in current asset detection methods, particularly for OT networks, and investigates new sources of threat intelligence, such as gray literature and right applications.

The study highlights the importance of AI-driven automation in comparing vulnerabilities, threats, and system components and proposes a new ontology to improve predictive threat analysis and proactive security measures. The paper concludes with recommendations for improving passive asset discovery and including generative AI into future cyber threat forecasts.

## II. Vulnerability Scanner Tool

### A. *Common Scanning Tools*

*1) **Nessus**:* The author in [14] has discussed network vulnerabilities in FTMM and KUITTHO using the Nessus

scanning tool to identify security problems and provide mitigation strategies. It underlines the importance of doing proactive vulnerability assessments to improve network security and prevent a potential flood.

The author in [15] has discussed Nessus, Acunetix, and Nikto, finding that Acunetix is the best option for web security, Nessus for business scanning, and Nikto as a low-cost basic utility. The author in [16] has discussed internal vulnerability scanning at Sanoma Media by using Tenable's Nessus Scanner in a cost-effective single-scanner configuration. It assesses arrangement situations, applies the favoured solution, and examines scan findings. Recommendations for increasing scan efficiency and future work are also included. The author in [17] has discussed in the document how automation improves security testing's coverage, accuracy, and efficiency. It looks at methods and technologies for automating deference checks, penetration tests, and vulnerability scans, which can help businesses cut expenses, identify risks more quickly, and stay in compliance with regulations. The author in [18] has discussed a next-generation Cyber Threat Intelligence Platform (TIP) for conducting real-time. It finds gaps in current asset detection methods, particularly for OT networks, and investigates new sources of threat intelligence, such as grey literature and right applications. The study highlights the importance of AI-driven automation in correlating vulnerabilities, threats, and system components and proposes a new ontology to improve predictive threat analysis and proactive security measures. The paper concludes with recommendations for improving passive asset discovery and includes generative AI in future cyber threat forecasts.

*2) **OpenVas**:* The author in [19] has discussed GVM-CLI to integrate OpenVAS into Huntdown, allowing vulnerability scans to be automated. It enhances usability, scalability, and efficiency. Key issues were overcome to ensure up-to-date, safe, user-friendly tests. The Author in [20] has discussed a smart, user-friendly vulnerability detection solution based on React and FastAPI, which includes tools such as OWASP ZAP, Nessus, and Nikto. It allows users to scan web applications by typing in URLs, detects common vulnerabilities such as XSS, SQLi, and CSRF, and delivers real-time results and protective recommendations. The author in [21] has discussed how cybersecurity visualization may improve threat identification and decision-making, current frameworks, and support user-centered, practical solutions for real-world applications. The Author in [22] has discussed how AI-enhanced cybersecurity for national defense is improved by machine learning, deep learning, and natural language processing. In addition to addressing issues like ethical problems, unfriendly attacks, and human-AI trust, it highlights their application in threat detection, vulnerability management, incident response, and biometric authentication.

*3) **Qualys**:* The author in [23] has discussed and compared standard and AI-enhanced network vulnerability scanners, highlighting how AI increases detection accuracy, threat prediction, and reaction automation. It also looks at tools, integration methodologies, problems, and future possibilities for merging AI with vulnerability assessment systems. The author in [24] has discussed how AI improves vulnerability identification and management through automated infrastructure and code scanning. It shows deep learning-based code analysis tools such as VulCNN and underlines the AI role in enhancing scalability, accuracy, and proactive threat mitigation in modern security workflows. The author in [25] has discussed an AI-enabled platform (AI4HCTI) that judges cyber risks in healthcare businesses by examining external threat intelligence, vulnerabilities, and business processes. It combines machine learning, natural language processing, and risk scoring to help healthcare organizations make bold security decisions. The author in [26] has discussed a multi-layered, proactive approach to cybersecurity. It urges firms to implement dynamic strategies for risk mitigation and incident response by examining modern threat landscapes, vulnerability assessments, employee awareness, and the use of AI in threat identification.

### *B. AI Techniques*

*1) **Machine Learning**:* The author in [27] has discussed how machine learning algorithms can detect and mitigate cyber risks in IoT networks, with an emphasis on DDoS attacks utilizing the MQTT protocol. The study simulates attacks and finds that Random Forest is the most accurate classifier, with 99.94 percent accuracy. Snort-based intrusion detection systems validate the suggested approach's effectiveness. The author in [28] has discussed. The study simulates attacks and finds that Random Forest is the most accurate classifier, with 967.94 percent accuracy. Snort-based intrusion detection systems validate the suggested approach's effectiveness. The author in [29] has discussed the looks at how AI-powered technologies, particularly ML and DL, improve mobile network security. It examines various approaches for detecting threats such as malware, intrusions, and data breaches, highlighting the importance of modern, adaptive security frameworks to combat growing cyber threats. The author in [30] has discussed Deep Neural Networks for Adversarial Inversion Attack in Wireless Networks, suggesting using a DNN-SVM hybrid model to detect negative reverse attacks in wireless networks. Automatically building and updating attack signatures enhances detection accuracy and efficiency, providing up to 93.67 percent accuracy and high throughput performance.

*2) **Deep Learning**:* The author in [31] has discussed the role of AI, specifically deep learning and combined learning, in improving cybersecurity in industries such as IoT and 5 G. It highlights developments like transformer models and blockchain, while also addressing issues such as data management and privacy. The report underlines that more research is needed to fully hold AI's word in danger detection. The author in [32] has discussed how AI enables autonomous danger hunting, resulting in faster and smarter cyber threat identification. It focuses on AI's importance, essential methodologies, and future difficulties in modern cybersecurity. The author in [33] has discussed ThreatWise AI, a comprehensive AI-powered system for managing Cyber Threat Intelligence

(CTI), which includes data collection, analysis, enhancement, and spreading. It uses machine learning, natural language processing, and powerful crawlers to quickly gather and correlate threat data from diverse sources. The author in [34] has discussed how Natural Language Processing (NLP) improves Cyber Threat Intelligence (CTI) by automating data extraction, analysis, and sharing across several web sources. It discusses NLP approaches, tools, and models used for threat detection, relationship extraction, and CTI standardization, while also covering problems such as data quality and ethics. The author in [35] has discussed that conducted a thorough examination of ML and DL techniques used to safeguard mobile networks. It examines several AI models for threat detection, assesses their effectiveness against cyberattacks such as malware and attacks on, and identifies current issues and future research paths in mobile cybersecurity. The author in [36] discusses that investigates the use of deep learning methods in several cybersecurity fields, such as spam filtering, malware analysis, and intrusion detection. It shows how deep learning may be used to automatically uncover complex patterns from massive amounts of data, increase detection accuracy, and adjust to changing threats.

### C. *Integration Features*

*1)* ***Real-Time Data Processing****:* The author in [37] has discussed how AI-powered threat intelligence solutions improve telecom network security by allowing for real-time threat detection, predictive analysis, and automated incident response. It stresses the use of machine learning, natural language processing, and big data analytics to carefully manage cyber threats and make better decisions. The author in [38] has discussed how to improve cyber threat detection using real-time threat intelligence and adaptive defense mechanisms powered by AI and machine learning. It stresses bold security, rapid reaction, and collaborative threat sharing to effectively combat developing cyber threats. The author in [39] has discussed "Automated Vulnerability Assessment Leveraging AI for Enhanced Security," which investigates how AI improves vulnerability management by automating the discovery, prioritization, and remediation of security vulnerabilities. It highlights considerable improvements in speed, accuracy, and cost-effectiveness, illustrating how AI-powered solutions enable bold and scalable cybersecurity strategies. The author in [40] has discussed AI-Driven Threat Detection and Response, investigating how AI may transform cybersecurity by improving threat detection and incident response. It highlights AI's role in detecting complex patterns, fighting zero-day attacks, and enabling automated, adaptive defenses, as well as considering ethical issues and future possibilities for AI integration.

*2)* ***Contextual Risk Scoring****:* The author in [41] has discussed using threat intelligence in threat modeling to better vulnerability identification and mitigation. It introduces a framework that integrates architectural analysis, OWASP standards, and real-time threat data to improve risk assessments and create more accurate, up-to-date, and responsive security solutions. The author in [42] has discussed the technical implementation and operational enhancements of a vulnerability management tool in an organization. It focuses on best practices, integration methods, and continuous development to achieve long-term cybersecurity flexibility and effectiveness. The author in [43] has discussed "Proactive Cyber Defense: Utilizing AI and IoT for Early Threat Detection and Cyber Risk Assessment in Future Networks," which looks at how AI and IoT can be combined to create proactive, real-time cyber defense systems. It focuses on AI's role in threat prediction, exception detection, and adaptive response while also integrating IoT data to improve threat intelligence and security monitoring in complex network environments. The author in [44] has discussed "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," which describes the CVSS methodology for determining the severity of software vulnerabilities. It describes the Base, Temporal, and Environmental metrics that businesses use to organize responses based on open, impact, and contextual aspects.

*3)* ***Automated Prioritization****:* The author in [45] has discussed how AI automates vulnerability assessment and patch management, increasing speed, accuracy, and scalability. It highlights AI's role in risk prediction, organization, and remediation while also addressing issues such as data quality, algorithmic bias, and transparency. The author in [46] has discussed a comprehensive vulnerability management methodology that includes automated risk evaluation for a betting organization. It presents a single tool and methodology to improve scan execution, risk rating, and remedial planning, providing a practical model for enterprises developing or improving cybersecurity plans. The author in [47] has discussed how Artificial Intelligence improves cybersecurity through threat detection, vulnerability analysis, and incident response. It also tackles ethical issues, data privacy, and explainability, as well as future trends like zero-trust security and negative machine learning.

## III. Conclusion

This study evaluated several vulnerability scanners that were improved using AI-driven threat intelligence. AI integration greatly improves response time, adaptability, and hazard detection accuracy. When combined with machine learning algorithms, technologies such as Qualys, OpenVAS, and Nessus exhibit advanced capabilities. These solutions can detect zero-day vulnerabilities while reducing false positives caused by artificial intelligence. While progress has been made, worries regarding adversarial threats, model openness, and data privacy remain. Tool effectiveness can only be increased through ongoing research and feedback from real-time threat data. AI-assisted scanners are a significant step forward for proactive cybersecurity defense.

## REFERENCES


[1] B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, "Handbook of computer networks and cyber security," *Springer*, vol. 10, pp. 978–3, 2020.

[2] T. P. Parikh and A. R. Patel, "Cyber security: Study on attack, threat, vulnerability," *Int. J. Res. Mod. Eng. Emerg. Technol*, vol. 5, pp. 1–7, 2017.

[3] A. I. Mohaidat and A. Al-Helali, "Web vulnerability scanning tools: A comprehensive overview, selection guidance, and cyber security recommendations," *International Journal of Research*, vol. 10, no. 1, pp. 8–15, 2024.

[4] D. N. Railkar and S. Joshi, "A study on vulnerability scanning tools for network security," *International Journal of Research*, vol. 10, no. 1, pp. 8–15, 2024.

[5] H. K. Mistry, C. Mavani, A. Goswami, and R. Patel, "Artificial intelligence for networking," *Educational Administration: Theory and Practice*, vol. 30, no. 7, pp. 813–821, 2024.

[6] J.-h. Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, 2018.

[7] C. S. Dabholkar, "Integrating open-source vulnerability scanning tools reports with open ai api for automated report generation," Ph.D. dissertation, Dublin, National College of Ireland, 2023.

[8] W. Shah and T. Best, "Threat detection and risk management: Using ai to counter cyber threats," *Available at SSRN 5003638*, 2025.

[9] J. K. Manda, "Ai-powered threat intelligence platforms in telecom: Leveraging ai for real-time threat detection and intelligence gathering in telecom network security operations," *Available at SSRN 5003638*, 2024.

[10] S. R. Sindiramutty, "Autonomous threat hunting: A future paradigm for ai-driven threat intelligence," *arXiv preprint arXiv:2401.00286*, 2023.

[11] S. Shah and F. K. Parast, "Ai-driven cyber threat intelligence automation," *arXiv preprint arXiv:2410.20287*, 2024.

[12] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya, and S. Khan, "Offensive security: cyber threat intelligence enrichment with counterintelligence and counterattack," *IEEE Access*, vol. 10, pp. 108 760–108 774, 2022.

[13] A. K. Shaw, "Next-generation cyber threat intelligence platform," Ph.D. dissertation, Marymount University, 2024.

[14] F. A. Hamid Ali, "Vulnerability analysis on the network security by using nessus," Ph.D. dissertation, Universiti Teknologi MARA, 2004.

[15] S. Nrk *et al.*, "A comparative analysis of vulnerability management tools: Evaluating nessus, acunetix, and nikto for risk based security solutions," *arXiv preprint arXiv:2411.19123*, 2024.

[16] A. A. Zafar, "Improving internal vulnerability scanning and optimal positioning of the vulnerability scanner in," *arXiv preprint arXiv:2711.19124*, 2023.

[17] S. R. Vemula, "Automating security testing: Strategies for vulnerability scanning, penetration testing, and compliance checks," 2024.

[18] ——, "Automating security testing: Strategies for vulnerability scanning, penetration testing, and compliance checks," 2023.

[19] A. Frangos, "Openvas integration for huntdown," Master's thesis, Universitat Politècnica de Catalunya, 2024.

[20] D. Chawla and S. Jain, "Smart approach for vulnerability detection using react," 2024.

[21] S. Cavallo, "Visualizing cybersecurity-a comparative study toward a security visualization methodology," Ph.D. dissertation, Politecnico di Torino, 2023.

[22] T. R. Vance, "Examination of applications of artificial intelligence in cybersecurity: Strengthening national defense with ai."

[23] P. Heinl, A. Patapovas, and M. Pilgermann, "Towards ai-enabled cyber threat assessment in the health sector," *arXiv preprint arXiv:2409.12765*, 2024.

[24] T.-R. Gabriela, A.-M. DINCĂ, S.-D. AXINTE, I. C. BACIVAROV *et al.*, "Enhancing vulnerability management with artificial intelligence algorithms," in *International Conference on Cybersecurity and Cybercrime*, vol. 11, 2024, pp. 96–101.

[25] H. Ghazizadeh, G. Tamm, and R. Creutzburg, "Automated tools for cloud security testing," *Electronic Imaging*, vol. 36, pp. 1–7, 2024.

[26] A. Elson, "Cyber threat analysis in the modern age: Developing security strategies for effective risk mitigation," 2024.

[27] A. Frangos, "Openvas integration for huntdown," Master's thesis, Universitat Politècnica de Catalunya, 2022.

[28] P. Heinl, A. Patapovas, and M. Pilgermann, "Towards ai-enabled cyber threat assessment in the health sector," *arXiv preprint arXiv:2409.12765*, 2023.

[29] C. Gupta, I. Johri, K. Srinivasan, Y.-C. Hu, S. M. Qaisar, and K.-Y. Huang, "A systematic review on machine learning and deep learning models for electronic information security in mobile networks," *Sensors*, vol. 22, no. 5, p. 2017, 2022.

[30] M. A. Al Ghamdi, "Analyze textual data: deep neural network for adversarial inversion attack in wireless networks," *SN Applied Sciences*, vol. 5, no. 12, p. 386, 2023.

[31] D. Kavitha and S. Thejas, "Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation," *IEEE Access*, 2024.

[32] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[33] A. Spyros, I. Koritsas, A. Papoutsis, P. Panagiotou, D. Chatzakou, D. Kavallieros, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Ai-based holistic framework for cyber threat intelligence management," *IEEE Access*, 2025.

[34] M. Arazzi, D. R. Arikkat, S. Nicolazzo, A. Nocera, M. Conti *et al.*, "Nlp-based techniques for cyber threat intelligence," *arXiv preprint arXiv:2311.08807*, 2023.

[35] R. Ofori-Boateng, M. Aceves-Martins, N. Wiratunga, and C. F. Moreno-Garcia, "Towards the automation of systematic reviews using natural language processing, machine learning, and deep learning: a comprehensive review," *Artificial intelligence review*, vol. 57, no. 8, p. 200, 2024.

[36] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," *Neurocomputing*, vol. 347, pp. 149–176, 2019.

[37] B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, "Handbook of computer networks and cyber security," *Springer*, vol. 09, pp. 928–3, 2025.

[38] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," *International Journal of Computer Applications Technology and Research*, vol. 13, no. 8, pp. 11–27, 2024.

[39] S. Pochu, S. R. Kathram, and S. Engineer, "Automated vulnerability assessment leveraging ai for enhanced security," *Journal of Multidisciplinary Research*, vol. 8, no. 01, pp. 14–25, 2022.

[40] A. Yaseen, "Ai-driven threat detection and response: A paradigm shift in cybersecurity," *International Journal of Information and Cybersecurity*, vol. 7, no. 12, pp. 25–43, 2023.

[41] I. H. Sarker, *AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability*. Springer Nature, 2024.

[42] V. Rantalaiho, "Technical implementation and operational enhancements of a vulnerability management tool in an organization," 2024.

[43] H. Rehman and H. Liu, "Proactive cyber defense: Utilizing ai and iot for early threat detection and cyber risk assessment in future networks," 2021.

[44] P. Mell, K. Scarfone, S. Romanosky *et al.*, "A complete guide to the common vulnerability scoring system version 2.0," in *Published by FIRST-forum of incident response and security teams*, vol. 1, 2007, p. 23.

[45] J. P. Seara and C. Serrão, "Automation of system security vulnerabilities detection using open-source software," *Electronics*, vol. 13, no. 5, p. 873, 2024.

[46] F. G. LO GIUDICE, "Methodologies and tools for a vulnerability management process with an integrated risk evaluation framework," 2022.

[47] ——, "Methodologies and tools for a vulnerability management process with an integrated risk evaluation framework," *arXiv preprint arXiv:2481.00747*, 2023.