Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 12, Issue 2, pp: (65-71), Month: May - August 2025, Available at: www.noveltyjournals.com

The Role of Machine Learning in Cybersecurity Practice: A Narrative Review

[1]Ifteker Hossen Rakib, [2]Md Sumon Prodhan

DOI: https://doi.org/10.5281/zenodo.16939724

Published Date: 25-August-2025

Abstract: **The rising complexity of cyber threats, consisting of AI-generated phishing and polymorphic malware, has outpaced the skills of traditional signature-based safety structures, exposing essential vulnerabilities in modern-day virtual infrastructure. This assessment significantly examines and synthesizes 24 peer-reviewed research posted between 2014 and 2024 to evaluate the transformative function of system getting to know (ML) in bridging this cybersecurity gap. The evaluation indicates that ML provides adaptive, actual-time defense mechanisms, improving accuracy in intrusion detection, malware classification, and phishing prevention. notwithstanding these advantages, demanding situations remain, such as restrained datasets, susceptibility to antagonistic attacks, and the opaque "black container" nature of complicated models, which constrain sensible deployment. The look at concludes that ML is an critical foundation for destiny cybersecurity, yet its complete capacity relies upon on studies targeted on Explainable AI (XAI), hostile resilience, and efficient set of rules layout. almost, these findings underscore the significance of interdisciplinary collaboration to translate ML-pushed intelligence from theoretical frameworks into powerful, resilient, and trustworthy cybersecurity structures.**

Keywords: **Machine Learning; Cybersecurity; Intrusion Detection; Adversarial Attacks; Explainable AI (XAI); Threat Detection.**

1. INTRODUCTION

Cybersecurity has grow to be one of the maximum essential concerns in nowadays's interconnected virtual society, in which facts represents a middle asset for people, companies, and governments alike. With the growing reliance on cloud computing, virtual transactions, and far flung working practices, the hazard of cyberattacks which includes malware, phishing, ransomware, and denial-of-service (DoS) has grown exponentially ([1]). conventional rule-primarily based protection structures, along with firewalls and signature-based intrusion detection, are no longer enough in addressing these evolving threats due to the fact they warfare to discover zero-day vulnerabilities and adapt to sophisticated opposed processes ([1]). This urgent dilemma has created a need for wise and adaptive processes, where device getting to know (ML) has emerged as a transformative generation in strengthening cybersecurity practices.

the educational and realistic importance of ML in cybersecurity lies in its ability to investigate large volumes of data, identify complicated chance styles, and offer real-time responses that es that supervised and unsupervised ML fashions can accurately locate intrusions, classify malware, and predict phishing tries, often with accuracy quotes exceeding ninety eight% in controlled experiments ([2]). moreover, ML-based frameworks have been applied to safeguard critical infrastructures which include smart grids ([3]) and IoT ecosystems, showcasing their broader applicability past traditional community defense. those contributions emphasize why ML has come to be a imperative recognition in contemporary cybersecurity discourse.

The developing reliance on digital infrastructures has led pupils and practitioners to increasingly more explore the capability of ML in cybersecurity practices. A big body of recent research constantly emphasizes that conventional rule-primarily based detection mechanisms are inadequate in tackling state-of-the-art and 0-day assaults, thereby motivating the shift toward adaptive ML-driven techniques ([4]). research have shown that ML affords enormous improvements in intrusion

detection, malware class, phishing identity, and anomaly detection, supplying a dynamic alternative to static protection systems. as an example, [5] conducted a comparative evaluation of diverse ML techniques, highlighting their effectiveness in intrusion, spam, and malware detection, whilst also pointing to barriers which includes outdated datasets and the want for greater complete assessment frameworks. Further, [6] burdened that most ML studies in cybersecurity is protective instead of offensive, largely due to the problems in quantifying offensive strategies. These opinions suggest that whilst ML has superior substantially, there's no single widely wide-spread algorithm that could address all categories of threats.

Different students have focused on realistic implementations and demanding situations. [7] recognized a incredible gap between studies results and business deployment of ML systems in cybersecurity. They argue that many research studies prioritize overall performance metrics without addressing actual-world complexities which include antagonistic manipulation, concept go with the flow, and the combination of ML structures into legacy infrastructures. This claim resonates with the findings of who underscored the restrictions of current datasets, noting that inconsistencies in feature sets and outdated records undermine the robustness of ML models in practice. [8] examined ML-pushed intrusion detection for IoT environments, revealing ML's benefits over conventional methods in detecting massive-scale IoT assaults inclusive of botnets and packet flooding. in addition, confirmed that ML classifiers like Random Forests and Gradient Boosting finished accuracies above 97% in detecting fake records injection attacks in clever grids, underscoring the relevance of ML in crucial infrastructure safety. on the other hand, proposed a framework for community anomaly detection that integrates ensemble fashions and adaptive ML strategies, showing good sized upgrades in identifying complicated threats but also declaring privateness issues and integration difficulties in actual-world structures.

Notwithstanding those advances, multiple gaps continue to be throughout literature. First, hostile ML offers a first-rate challenge, as attackers can manage education records or craft antagonistic examples to mislead models [9]. Second, maximum contemporary studies are based totally on managed environments and benchmark datasets, restricting their applicability in real-international, dynamic cybersecurity contexts ([7]; [5]). 1/3, explainability stays a situation; as ML models develop in complexity, their "black box" nature reduces transparency, undermining believe amongst cybersecurity specialists and choice-makers. Moreover, there may be a loss of empirical studies testing ML frameworks in huge-scale industrial and IoT ecosystems, in which scalability and computational performance .

In phrases of methodologies, the reviewed studies hired diverse ML algorithms starting from supervised fashions inclusive of helping Vector Machines (SVM), Random Forests (RF), and k-Nearest buddies (KNN), to unsupervised processes for anomaly detection and clustering ([5]; [9]). extra latest works have also experimented with deep gaining knowledge of extensions together with Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Generative adversarial Networks (GANs) for malware type and sequential log evaluation [9]. whilst those models often record excessive accuracy in detecting cyber threats, they require tremendous computational assets and depend closely on large, balanced datasets, which can be often unavailable.

universal, the literature converges on the conclusion that ML is a transformative device in cybersecurity, providing adaptability, scalability, and progressed detection accuracy in comparison to conventional techniques. however, constant demanding situations in dataset satisfactory, adverse robustness, real-international deployment, and explainability highlight the need for future studies to bridge the space between concept and exercise. students more and more name for interdisciplinary collaboration among researchers, practitioners, and industry stakeholders to increase ML models which are both technically strong and almost feasible in addressing evolving cyber threats ([1]).

2. PROBLEM STATEMENT

In the swiftly evolving cyberspace of nowadays, businesses, governments, and individuals face a mounting array of threats. Key malicious vectors together with malware, phishing, ransomware, and disbursed Denial-of-service (DDoS) assaults have emerge as more and more pervasive and complex. for example, phishing incidents spiked with the aid of a awesome four,151% following the public launch of generative AI gear, while ransomware bothered 59% of corporations in 2024, compounding the urgency of the cybersecurity crisis [10]. these numbers replicate a chance panorama that isn't simplest expanding in volume however additionally in complexity and foxy.

conventional protection defenses—which includes rule-primarily based definitely structures, signature-based totally completely intrusion detection structures (IDS), and perimeter firewalls—were as soon as foundational system in

cybersecurity frameworks. however, their efficacy has diminished in opposition to rising threats. Signature-based totally IDS, for instance, fail to find out novel or polymorphic attacks because of their reliance on pre-defined styles. They require consistent updates and emerge as obsolete almost as quickly as new threats appear [11]. similarly, static rule-based systems and firewalls struggle with zero-day exploits and adaptive threats that could make the most device-degree weaknesses or pass signature styles altogether.This disparity has created a fundamental gap among an increasing number of sophisticated cyberattacks and old detection/prevention mechanisms, undermining organizational resilience. Malware-as-a-provider (MaaS) platforms, AI-generated assaults, and stealthy phishing schemes which include URL-based phishing or "quishing" have escalated the risk environment a ways beyond what conventional defenses can successfully counter [12].

To bridge this hole, there is a clear and pressing need for intelligent, adaptive, and scalable answers, which includes the ones enabled by device learning (ML). ML techniques provide the capability to dynamically research from big volumes of evolving statistics, pick out subtle and emerging attack styles, and reply in real time—talents that conventional structures fundamentally lack. therefore, leveraging ML in cybersecurity now not most effective addresses the fundamental obstacles of legacy methods however also equips defenders with proactive and resilient protection mechanisms appropriate for the current danger landscape.

3. METHODS

This evaluate changed into designed to synthesize and severely have a look at the prevailing body of literature on the function of system getting to know (ML) in cybersecurity practices. The method employed a dependent assessment of secondary sources, specializing in peer-reviewed studies articles, systematic critiques, and case studies. To ensure the credibility and reliability of the statistics, 4 main scientific databases had been searched: Google scholar, PubMed, Scopus, and net of science[13].

the hunt method trusted unique keywords and their combos, along with: "device learning in Cybersecurity", "Intrusion Detection using ML", "Malware class with system getting to know", "Phishing Detection", "Anomaly Detection", "Deep mastering for Cybersecurity", and "opposed gadget gaining knowledge of". Boolean operators which include AND, OR, and no longer were carried out to refine the quest and take away beside the point consequences.

The records collection time-frame protected research published between 2014 and 2024, thereby taking pictures each foundational research and the most current improvements in ML applications for cybersecurity. An preliminary pool of about 50 files become retrieved across the databases. each article become carefully screened by means of reviewing the title, summary, and keywords to determine its relevance to the targets of the assessment[13]. research that have been now not directly associated with ML applications in cybersecurity, reproduction data, and convention abstracts with out complete papers have been excluded.

After this initial screening, a total of 24 peer-reviewed studies articles were decided on for exact evaluation. each decided on paper was examine very well, and the findings, methodologies, contributions, and research gaps were systematically extracted. the selected literature included each empirical and conceptual works, making sure a balanced illustration of technical improvements, theoretical discussions, and real-international case applications[7].

This methodological approach allowed for a complete synthesis of the strengths, boundaries, and destiny directions of system gaining knowledge of in cybersecurity, making sure that the evaluation displays both the intensity and breadth of existing scholarship.

4. PROPOSED SOLUTIONS

Constructing on the vital evaluation of current cybersecurity challenges, this section explores system mastering (ML)-driven solutions as a promising avenue to beautify risk detection and prevention. The assessment highlights that ML methods can significantly improve the identity of state-of-the-art attacks, starting from malware and phishing to anomalies in IoT and cloud environments. Through synthesizing recent findings, its miles glaring that ML offers adaptive, real-time, and scalable protection mechanisms, capable of decreasing fake positives and improving risk intelligence. Moreover, the proposed answers bear in mind both technical efficacy and practical deployment challenges, inclusive of data pleasant, adverse vulnerabilities, and computational requirements, imparting a balanced angle at the implementation of ML in modern cybersecurity infrastructures.

4.1 Applications of ML in Cybersecurity

Machine getting to know (ML) has emerged as a transformative device in cybersecurity, providing dynamic solutions that may adapt to evolving threats. one of the number one packages of ML is in Intrusion Detection systems (IDS). traditional IDS depend heavily on predefined signatures and rules, which limits their effectiveness against novel or polymorphic attacks. In evaluation, supervised ML techniques which include guide Vector Machines (SVM) and Random Forests (RF) can examine from labeled datasets to perceive recognized threats with excessive accuracy, even as unsupervised techniques which includes clustering algorithms and autoencoders are capable of detecting previously unseen anomalies by using identifying deviations from everyday system conduct [14].

every other extensive location is malware detection and type. ML algorithms, in particular Convolutional Neural Networks (CNNs) and RF fashions, can robotically extract patterns from executable documents or network site visitors, permitting speedy identification and classification of malicious software program. This method reduces reliance on guide function engineering and improves detection prices in opposition to sophisticated malware editions [15].

Phishing and unsolicited mail detection have also benefitted from ML, mainly through the mixing of natural Language Processing (NLP) strategies. by means of analyzing textual content, e mail headers, URLs, and metadata, ML models can correctly classify phishing tries and unsolicited mail messages with greater precision than conventional keyword-based totally filters [16]. Such models are especially effective in detecting AI-generated phishing campaigns, which can be more and more state-of-the-art.

furthermore, anomaly detection in IoT and cloud environments is a important software. IoT gadgets often perform with restrained protection protocols, making them at risk of unusual behavior patterns. ML-based totally anomaly detection fashions can display tool behavior in real-time, flagging deviations indicative of security breaches or performance problems [17]. further, cloud infrastructures advantage from ML strategies to identify unauthorized get entry to or configuration anomalies, thereby strengthening overall system resilience.

lastly, ML techniques are increasingly more employed in fraud detection in monetary transactions. by using analyzing transactional information, ML fashions can discover abnormal styles and suspicious activities in real-time, mitigating monetary losses and improving regulatory compliance. techniques along with ensemble gaining knowledge of and deep neural networks have proven excessive efficacy in detecting fraudulent conduct throughout large-scale datasets [18].

4.2 Advantages of ML in Cybersecurity

System mastering (ML) has grow to be a cornerstone in modern-day cybersecurity, offering several advantages over conventional safety features. one of the number one advantages is its adaptability to evolving threats. in contrast to static rule-primarily based systems, ML algorithms can study from new statistics, allowing them to come across previously unseen attacks. This dynamic studying functionality permits for timely identification of emerging threats, enhancing the general safety posture([19]).

any other huge benefit is the high accuracy and decreased false positives. ML fashions, especially deep mastering strategies, can analyze massive quantities of statistics to identify patterns indicative of malicious activity. This functionality results in greater correct threat detection and a lower in fake alarms, permitting security groups to recognition on true threats ([19]; [20]).

actual-time risk intelligence is also a important advantage of ML in cybersecurity. ML algorithms can manner and examine information in actual-time, imparting instantaneous insights into ability security incidents. This rapid evaluation enables groups to reply swiftly to threats, minimizing capacity damage [21]

Moreover, ML demonstrates applicability across diverse infrastructures, consisting of net of factors (IoT) devices, cloud environments, and employer networks. Its versatility permits for the mixing of ML-primarily based protection solutions across various structures, presenting complete protection against a huge variety of cyber threats.

The benefits of ML in cybersecurity—adaptability, accuracy, real-time intelligence, and infrastructural applicability—underscore its pivotal position in improving security measures. by means of leveraging these strengths, businesses can higher protect towards the increasingly more sophisticated cyber threats of brand new digital panorama.

4.3 Challenges and Limitations

Despite the promising advantages of system studying (ML) in cybersecurity, several demanding situations and limitations persist, hindering its great adoption and effectiveness.

4.3.1 Data Availability and Quality

ML models require massive volumes of, categorised statistics to teach effectively. but, acquiring such datasets in cybersecurity is frequently hard because of privateness issues, information silos, and the dynamic nature of cyber threats. the dearth of complete and representative datasets can lead to overfitting, reduced generalization, and compromised version performance [11].

4.3.2 Adversarial ML Attacks

Antagonistic device gaining knowledge of involves manipulating enter data to misinform ML models into making wrong predictions. Attackers can take advantage of vulnerabilities in ML algorithms through introducing diffused perturbations to enter data, leading to misclassification or evasion of detection systems. This poses a considerable threat to the reliability and robustness of ML-based totally cybersecurity answers ([22]; [16]).

4.3.3 Lack of Explainability and Interpretability

Many ML models, especially deep learning techniques, operate as "black boxes," making it difficult for security professionals to understand the rationale behind their decisions. This lack of transparency hinders trust and accountability, particularly in critical applications where understanding the decision-making process is essential for compliance and risk management ([23]).

4.3.4 High Computational Requirements

training and deploying complex ML fashions call for sizeable computational sources, including excessive-overall performance hardware and power intake. This requirement may be prohibitive for corporations with limited infrastructure, specifically whilst working in useful resource-limited environments like aspect computing or net of factors (IoT) devices [22].

4.3.5 Gap Between Lab Results and Real-World Deployment

while ML models regularly exhibit excessive accuracy in controlled laboratory settings, their performance can degrade while deployed in actual-global environments. factors such as statistics distribution shifts, adversarial conditions, and integration complexities can have an effect on the version's effectiveness, main to challenges in attaining regular and reliable performance outdoor the lab.

5. FUTURE DIRECTIONS

The evolving cybersecurity panorama wishes non-prevent improvement of tool reading (ML) and artificial intelligence (AI) techniques to address rising threats correctly. A crucial awareness is Explainable AI (XAI), which enhances the transparency and interpretability of complex ML models, thereby growing person receive as actual with and duty in protection systems. furthermore, the aggregate of ML with blockchain, cloud computing, and IoT protection offers robust, actual-time danger detection and mitigation, leveraging decentralized, scalable, and interconnected infrastructures. The improvement of adaptive and independent defense mechanisms using reinforcement gaining knowledge of lets in structures to dynamically have a have a look at from interactions, enhancing their responses to novel and evolving attacks. To ensure constant evaluation and reproducibility, standardized datasets and benchmarking frameworks are vital for comparing model usual universal performance underneath diverse conditions (NeurIPS, 2024; Ferrag et al., 2024). in the long run, sustained collaboration among academia, enterprise, and policymakers is critical for fostering innovation, sharing records, and formulating recommendations that manual the deployment of advanced cybersecurity answers (Texas Tech college, 2025; TechRadar, 2025). collectively, these commands provide a roadmap for strengthening resilient, clever, and sincere cybersecurity systems inside the modern-day-day virtual technology.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 12, Issue 2, pp: (65-71), Month: May - August 2025, Available at: www.noveltyjournals.com

6. CONCLUSION

This assessment highlights that tool analyzing (ML) has fundamentally reshaped cybersecurity, reworking it from a reactive to a proactive subject. conventional signature-based totally absolutely defenses struggle in competition to threats including AI-generated phishing and polymorphic malware, whilst ML gives dynamic, records-pushed answers able to detecting novel and zero-day assaults with immoderate accuracy while reducing fake positives. programs span vital domain names, which include intrusion detection structures that use supervised and unsupervised models, malware class thru deep analyzing, and actual-time phishing detection via herbal language processing.

however those advances, numerous worrying situations prevent massive implementation. classified datasets are state-of-the-art scarce, most essential to overfitting and decreased model robustness, even as adversaries make the maximum vulnerabilities via detrimental device cutting-edge. The "black-field" nature state-of-the-art complex models complicates agree with, interpretability, and forensic evaluation. furthermore, performance brand newten declines outside managed lab environments, specifically in useful useful resource-confined or actual-time settings.

Addressing these problems calls for a multi-faceted studies time desk. Key priorities include growing Explainable AI (XAI) to enhance transparency, developing robust defenses in competition to opposed attacks, and designing mild-weight, green algorithms for thing and IoT gadgets. Standardized benchmarking and collaboration among academia, organisation, and policymakers are important to bridge the space between idea and workout. collectively, the ones efforts feature ML as a cornerstone for resilient, practical, and honest cybersecurity structures, capable of adapting to evolving threats and securing crucial virtual infrastructure.

REFERENCES

[1] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, “A Survey of Deep Learning Methods for Cyber Security,” *Information*, vol. 10, no. 4, p. 122, Apr. 2019, doi: 10.3390/info10040122.

[2] I. D. Aiyanyo, H. Samuel, and H. Lim, “A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning,” *Applied Sciences*, vol. 10, no. 17, p. 5811, Jan. 2020, doi: 10.3390/app10175811.

[3] “A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning.” Accessed: Aug. 20, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/10/17/5811

[4] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, “Advancing cybersecurity: a comprehensive review of AI-driven detection techniques,” *J Big Data*, vol. 11, no. 1, p. 105, Aug. 2024, doi: 10.1186/s40537-024-00957-y.

[5] I. J. Vourganas and A. L. Michala, “Applications of Machine Learning in Cyber Security: A Review,” *Journal of Cybersecurity and Privacy*, vol. 4, no. 4, pp. 972–992, Dec. 2024, doi: 10.3390/jcp4040045.

[6] R. Kaur, D. Gabrijelčič, and T. Klobučar, “Artificial intelligence for cybersecurity: Literature review and future research directions,” *Information Fusion*, vol. 97, p. 101804, Sept. 2023, doi: 10.1016/j.inffus.2023.101804.

[7] S. Okdem and S. Okdem, “Artificial Intelligence in Cybersecurity: A Review and a Case Study,” *Appl. Sci.-Basel*, vol. 14, no. 22, p. 10487, Nov. 2024, doi: 10.3390/app142210487.

[8] S. Ankalaki, A. R. Atmakuri, M. Pallavi, G. S. Hukkeri, T. Jan, and G. R. Naik, “Cyber Attack Prediction: From Traditional Machine Learning to Generative Artificial Intelligence,” *IEEE Access*, vol. 13, pp. 44662–44706, 2025, doi: 10.1109/ACCESS.2025.3547433.

[9] A. Shees, M. Tariq, and A. I. Sarwat, “Cybersecurity in Smart Grids: Detecting False Data Injection Attacks Utilizing Supervised Machine Learning Techniques,” *Energies*, vol. 17, no. 23, p. 5870, Jan. 2024, doi: 10.3390/en17235870.

[10] M. Uddin *et al.*, “Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations,” *Artif. Intell. Rev.*, vol. 58, no. 8, p. 236, May 2025, doi: 10.1007/s10462-025-11219-5.

[11] G. Apruzzese, M. Andreolini, M. Colajanni, and M. Marchetti, “Leveraging explainable artificial intelligence for early detection and mitigation of cyber threat in large-scale network environments,” *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 4, no. 4, pp. 427–439, Aug. 2020, doi: 10.1109/TETCI.2019.2961157.

[12] G. Nalinipriya *et al.*, "Leveraging explainable artificial intelligence for early detection and mitigation of cyber threat in large-scale network environments," *Sci Rep*, vol. 15, no. 1, p. 24662, July 2025, doi: 10.1038/s41598-025-08597-9.

[13] J. Yu, A. V. Shvetsov, and S. H. Alsamhi, "Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions," *IEEE Access*, vol. 12, pp. 159579–159596, 2024, doi: 10.1109/ACCESS.2024.3482987.

[14] Y. Xin *et al.*, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[15] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *Journal of Defense Modeling & Simulation*, vol. 19, no. 1, pp. 57–106, Jan. 2022, doi: 10.1177/1548512920951275.

[16] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *WIREs Data Mining and Knowledge Discovery*, vol. 9, no. 4, p. e1306, 2019, doi: 10.1002/widm.1306.

[17] Ugochukwu Ikechukwu Okoli, Ogugua Chimezie Obi, Adebunmi Okechukwu Adewusi, and Temitayo Oluwaseun Abrahams, "Machine learning in cybersecurity: A review of threat detection and defense mechanisms," *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 2286–2295, Jan. 2024, doi: 10.30574/wjarr.2024.21.1.0315.

[18] K. Shaukat *et al.*, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," Jan. 2020, Accessed: Aug. 20, 2025. [Online]. Available: https://openresearch.newcastle.edu.au/articles/journal_contribution/Performance_comparison_and_current_challenges_of_using_machine_learning_techniques_in_cybersecurity/28973174/1

[19] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review," Sept. 01, 2022, *Social Science Research Network, Rochester, NY*: 4323317. Accessed: Aug. 20, 2025. [Online]. Available: https://papers.ssrn.com/abstract=4323317

[20] J. B. Fraley and J. Cannady, "The promise of machine learning in cybersecurity," in *SoutheastCon 2017*, Mar. 2017, pp. 1–6. doi: 10.1109/SECON.2017.7925283.

[21] M. M. Rathore, S. A. Shah, D. Shukla, E. Bentafat, and S. Bakiras, "The Role of AI, Machine Learning, and Big Data in Digital Twinning: A Systematic Literature Review, Challenges, and Opportunities," *IEEE Access*, vol. 9, pp. 32030–32052, 2021, doi: 10.1109/ACCESS.2021.3060863.

[22] A. Oun, K. Wince, and X. Cheng, "The Role of Artificial Intelligence in Boosting Cybersecurity and Trusted Embedded Systems Performance: A Systematic Review on Current and Future Trends," *IEEE Access*, vol. 13, pp. 55258–55276, 2025, doi: 10.1109/ACCESS.2025.3554739.

[23] G. Apruzzese *et al.*, "The Role of Machine Learning in Cybersecurity," *Digital Threats*, vol. 4, no. 1, p. 8:1-8:38, Mar. 2023, doi: 10.1145/3545574.

[24] M. Mijwil, I. Salem, and M. Ismaeel, "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, Jan. 2023, doi: 10.52866/ijcsm.2023.01.01.008.