The Role of Machine Learning in Detecting Cyber Threats: A Comparative Review of Techniques, Datasets, And Evaluation Challenges

Mustapha Mukhtar Tijjani[1], Ridwan Salmanu[2], Usman Mohammed.[3]
[1, 3] Dept of information technology
[2]Dept of Computer Science
[1, 2, 3] Bayero University Kano.

Abstract- *Traditional systems that rely on signatures or rules have not been able to keep up with the increasing complexity, frequency, and effect of cyber threats. There has to be a dramatic change to threat detection systems that use machine learning (ML) to keep up with the ever-changing threat landscape. A thorough comparative analysis of ML's function in cyber threat detection is presented in this review. We aim to thoroughly analyze the main ML techniques, identify the domains where they are applied, and assess the benchmark datasets and assessment issues that are essential to this field of study. Deep learning (DL) models show better feature extraction and high accuracy (98-99%) in complex environments, according to a comparative study of supervised, unsupervised, DL, and hybrid/ensemble methods. However, the best architectures for maximizing generalizability and robustness are currently hybrid and ensemble models. Problems with out-of-date content, class imbalance, and real-world representation are prevalent in analyses of popular datasets (e.g., CICIDS2017, NSL-KDD). Inadequate dataset quality, the interpretability problem of "black box" models, and susceptibility to adversarial attacks are some of the ongoing, practical obstacles that limit ML's efficacy, according to the study's conclusions. Establishing adversarially resilient, explainable (XAI), and data-quality-conscious ML pipelines is an important need for future research in order to guarantee the deployment of reliable and scalable cyber security systems.*

I. INTRODUCTION

Cyber threats—malicious actions aimed at compromising the confidentiality, integrity, and availability of digital systems—have escalated in frequency, complexity, and consequence as society grows more dependent on networked technologies. These threats include various attacks such as malware, phishing, ransomware, and advanced persistent threats, presenting substantial risks to individuals, organizations, and nations [1] [2]. Conventional cybersecurity methods, like signature-based detection and rule-based systems, frequently fail to adapt to the swiftly changing strategies of cybercriminals, resulting in significant vulnerabilities in defense. [3] [1] [2]. In reaction to these issues, machine learning (ML) has arisen as a vital instrument in cybersecurity. Machine learning empowers systems to assimilate extensive data, identify nuanced patterns, and adjust to novel and previously unencountered attack vectors without direct programming. Through the automation of network traffic monitoring, user behavior assessment, and system log examination, machine learning algorithms may identify abnormalities and dangers in real time, providing a more dynamic and proactive strategy for cyber defense than traditional techniques. [3] [4] [1]. The use of machine learning into cybersecurity frameworks improves detection precision, decreases response times, and alleviates the workload on human analysts [3] [1] [2]. This paper seeks to deliver a thorough comparative examination of machine learning's function in cyber threat detection. The objectives are three in number: (1) to analyze and contrast the principal machine learning techniques utilized in cybersecurity, (2) to assess the datasets frequently employed for training and evaluating these models, and (3) to address the significant challenges in appraising machine learning-based threat detection systems, encompassing concerns regarding data quality, adversarial attacks, and model interpretability. The paper aims to underscore both the progress and the persistent obstacles in utilizing machine learning for effective and adaptive cyber threat detection [3] [1] [2].

II. BACKGROUND AND MOTIVATION

Conventional cyber threat detection techniques, including signature-based antivirus programs and rule-based intrusion detection systems, have historically been the cornerstone of cybersecurity. These methodologies depend on established patterns or signatures to detect recognized threats, rendering them effective for previously encountered attacks but mostly ineffectual against novel, unknown, or swiftly evolving threats. As cyberattacks have increased in frequency, sophistication, and variety—encompassing malware, phishing, advanced persistent threats, and ransomware—traditional systems have found it challenging to adapt. They frequently struggle to identify zero-day exploits and are constrained in their capacity to adjust to novel attack methodologies, leading to heightened risk for persons, businesses, and critical infrastructure. [1] [2] [3] [4] [5].

In light of these constraints, machine learning (ML) has arisen as a revolutionary influence in cybersecurity. Machine learning systems can examine extensive and intricate datasets, autonomously identify patterns of both benign and dangerous activity, and adjust to emerging dangers without direct programming. This adaptability enables ML-based systems to identify minor anomalies, previously unrecognized malware, and complex intrusion attempts that conventional approaches may overlook. [1] [6] [2] [3] [4] [5]. Deep learning, a subset of machine learning, augments detection skills by extracting intricate features from unprocessed data, whereas reinforcement learning allows systems to refine protection methods in fluctuating settings. [6] [1] [7]. As cyber threats advance, the necessity for intelligent, adaptive, and scalable detection systems has become critical, rendering machine learning an indispensable element of contemporary cybersecurity measures. 1 2 [3] [4] [5].

2.1 Taxonomy of Machine Learning Techniques

Machine learning techniques for cyber threat detection can be categorized into several main types, each with distinct characteristics, algorithms, and application domains [6] [8] [9] [2]:

- **Supervised Learning:**This methodology employs labeled datasets to train models for the classification or prediction of threats. Prevalent algorithms encompass Support Vector Machines (SVM), decision trees, random forests, and neural networks. Supervised learning is extensively employed for intrusion detection, malware categorization, and spam detection, utilizing labeled instances of both benign and malicious activities.[10] [11] [2] [8].
- **Unsupervised Learning:**Unsupervised approaches do not necessitate labeled data and are employed to identify anomalies or cluster data based on similarities. Methods such as k-means clustering, Isolation Forest, and autoencoders are proficient at detecting undiscovered or developing threats, particularly in anomaly-based intrusion detection where novel attack patterns may remain unclassified. [6] [2] [10] [8].
- **Semi-Supervised Learning:**This methodology integrates a limited quantity of labeled data with an extensive array of unlabeled data, enhancing detection in contexts where labeled data is deficient. Semi-supervised learning is especially advantageous in cybersecurity, because acquiring labeled attack data poses significant challenges [6] [2] [8].
- **Deep Learning:**Deep learning utilizes multi-layered neural networks, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and autoencoders, to autonomously extract intricate features from unprocessed data. These models demonstrate superior performance in intrusion detection, malware analysis, and behavioral analytics, frequently surpassing conventional machine learning methods in both accuracy and adaptability. [6] [10] [9] [8].
- **Reinforcement Learning:**Reinforcement learning instructs models by trial and error, enabling them to enhance defense tactics in fluctuating settings. This methodology is efficacious for adaptive intrusion prevention and automated response systems, wherein the system acquires knowledge to react to threats based on feedback from its activities. [6] [9] [7] [8].

2.2 Application Domains: These ML techniques are applied across a range of cybersecurity domains, including:

- Intrusion Detection Systems (IDS): Detecting unwanted access or anomalous network behavior.
- Malware Detection: Classifying and identifying malevolent software [10] [9] [2].
- Fraud Detection: Identifying fraudulent transactions or conduct [10] [9] [2].
- Phishing and Spam Detection: Filtering harmful emails and hyperlinks [10] [9] [2].

By leveraging these diverse ML approaches, cybersecurity systems can achieve higher accuracy, adaptability, and resilience against the ever-evolving spectrum of cyber threats [6] [9] [2] [10] [8].

ML Approach	Typical Algorithms	Application Domains	Citations
Supervised	SVM, Decision Trees, RF, NN	IDS, malware, spam, fraud detection	[10] [11] [2] [8]
Unsupervised	K-means, Isolation Forest, AE	Anomaly, unknown threat detection	[6] [2] [10] [8]
Semi-supervised	Hybrid models	IDS, malware detection	[6] [2] [8]

Deep Learning	CNN, RNN, Autoencoders	IDS, malware, behavioral analytics	[6] [10] [9] [8]
Reinforcement	Q-learning, DQN	Adaptive defense, automated response	[6] [9] [7] [8]

Figure 1: Expanded taxonomy of ML techniques and their cybersecurity applications.

III. COMPARATIVE ANALYSIS OF MACHINE LEARNING TECHNIQUES FOR CYBER THREAT DETECTION

3.1. Major Machine Learning Techniques: Strengths, Weaknesses, and Performance

3.1.1 Supervised Learning

- Strengths: Exceptional precision when trained on high-quality, labeled datasets; proficient for recognized attack types and clearly delineated issues (e.g., spam, malware, intrusion detection); models such as Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), and Artificial Neural Networks (ANN) are extensively utilized and interpretable [12] [2] [10] [13] [14].
- Weaknesses: Performance deteriorates with imbalanced or insufficient labeled data; encounters difficulties with zero-day or unique attacks; necessitates periodic retraining as attack patterns vary [12] [2] [10] [13] [14].
- Performance: Random Forest (RF) and Support Vector Machine (SVM) frequently attain elevated accuracy levels, reaching up to 99% in certain studies, for intrusion and malware detection [12] [10] [14].

3.1.2 Unsupervised Learning

- Strengths: Identifies new or unexpected dangers through anomaly detection; advantageous in scenarios with limited labeled data; methodologies encompass k-means clustering, Isolation Forest, and autoencoders [8] [2] [15] [10].
- Weaknesses: Elevated false positive rates resulting from the absence of ground truth; interpretation of outcomes may be complex; potential inability to differentiate between benign anomalies and genuine attacks [8] [2] [15] [10].
- Performance: Efficient for anomaly-based intrusion detection; nevertheless, precision and recall may fluctuate significantly based on the dataset and context. [8] [15] [10].

3.1.3 Deep Learning

- **Strengths**: Proficient in deriving intricate features from unrefined data (e.g., network traffic, logs); exceptional efficacy in expansive, high-dimensional data contexts; notable models include Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), and Deep Neural Networks (DNN). [16] [17] [18] [10] [19] [20] [21] [22].
- **Weaknesses**: Demands extensive, varied datasets and substantial processing power; frequently functions as a "black box," diminishing interpretability; susceptible to adversarial assaults and data contamination [16] [17] [18] [10] [19] [20] [21] [22].
- **Performance:**Deep models, such as LSTM and CNN, have attained accuracy rates of 98–99% on benchmark datasets for intrusion and malware detection.[23] [17] [18] [10] [19] [20] [21] [22].

3.1.4 Reinforcement Learning

- **Strengths:** Acquires optimal defense tactics in dynamic situations; adjusts to emerging threats through continuous input; beneficial for automated responses and adaptive intrusion prevention [6] [24].
- **Weaknesses:** Demands substantial investigation and may exhibit sluggish convergence; less frequently utilized in practical applications due to its complexity [6] [24].
- **Performance:** Research indicates promising outcomes, particularly in adaptive and proactive protection; nonetheless, practical implementation remains in its nascent stages [6] [24].

3.2. Hybrid and Ensemble Models

Hybrid and ensemble models combine multiple algorithms to leverage their complementary strengths, often resulting in improved detection accuracy and robustness [8] [12] [25] [26] [27] [28] [20] [29] [14]. Common strategies include stacking, bagging, boosting, and integrating deep learning with traditional ML.

- **Strengths**: Increased accuracy, precision, and recall relative to individual models; superior generalization and less overfitting; enhanced resistance to adversarial attacks and data imbalance. [8] [12] [25] [26] [27] [28] [20] [29] [14].

- **Weaknesses**: Heightened computational complexity and resource demands; more difficult to explain and sustain; may necessitate meticulous tuning and integration [8] [12] [25] [26] [27] [28] [20] [29] [14].
- **Performance**: Stacked and boosted ensembles (e.g., Random Forest, XGBoost, AdaBoost) routinely attain accuracy over 99% on benchmark datasets [25]. [26] [27] [29] [14].

3.3. Comparative Table: ML Techniques in Cyber Threat Detection

Technique	Strengths	Weaknesses	Typical Use Cases	Performance Highlights	Key Citations
Supervised ML	High accuracy, interpretable, fast	Needs labeled data, less effective for zero-day	Spam, malware, intrusion detection	RF/SVM: 95–99% accuracy	[12] [2] [10] [13] [14]
Unsupervised ML	Detects unknown threats, no labels needed	High false positives, hard to interpret	Anomaly detection, novel attacks	Varies, often lower precision	[8] [2] [15] [10]
Deep Learning	Handles complex data, high accuracy	Data/computation intensive, black box	Large-scale IDS, malware, IoT	CNN/LSTM: 98–99% accuracy	[23] [16] [17] [18] [10] [19] [20] [21] [22]
Reinforcement L.	Adaptive, learns optimal strategies	Slow convergence, complex to deploy	Automated response, adaptive IDS	Promising, still emerging	[6] [24]
Hybrid/Ensemble	High accuracy, robust, generalizes well	Complex, resource intensive	Multi-class, real-time detection	$>99\%$ accuracy, low FPR	[8] [12] [25] [26] [27] [28] [20] [29] [14]

Figure 1: Comparative analysis of major ML techniques for cyber threat detection.

3.4. Visual Summary: Performance of ML Techniques

Model Type	Typical Accuracy (%)	Notable Datasets	Key Citations
Random Forest	95–99	CICIDS2017, NSL-KDD	[12] [10] [14]
SVM	94–98	CICIDS2017, UNSW-NB15	[12] [10] [14]
CNN/LSTM (DL)	98–99	CICIDS2017, BoT-IoT	[23] [17] [18] [10] [19] [20] [21] [22]
Ensemble/Hybrid	99–100	CICIDS2017, TON_IoT	[25] [26] [27] [29] [14]

Figure 2: Performance comparison of major ML models on benchmark cyber threat datasets.

IV. DATASETS FOR CYBER THREAT DETECTION AND EVALUATION METRICS

4.1. Widely Used Datasets for Cyber Threat Detection

Robust and representative datasets are foundational for developing, benchmarking, and comparing machine learning (ML) and deep learning (DL) models in cyber threat detection. Over the years, several public datasets have become standard in the field, each with unique characteristics, coverage, and limitations.

4.1.1. Dataset Characteristics, Coverage, and Limitations

Dataset	Domain/Focus	Attack Types Covered	Key Limitations	Citations
NSL-KDD	General networks	DoS, Probe, U2R, R2L	Outdated, lacks modern threats	[10] [30] [9] [31]
CSE-CIC-IDS2018	General networks	Wide range, multi-class	Imbalanced, cleaning issues	[32] [10] [33]
CICIDS2017	General networks	DDoS, brute force, etc.	Class imbalance	[34] [10] [35] [17] [36]
UNSW-NB15	General networks	Modern attacks	Limited real-world diversity	[10] [35] [33] [37]
BoT-IoT	IoT	IoT-specific attacks	Domain-specific, imbalanced	[38] [39] [36] [40]
TON_IoT	IoT/IIoT	IoT, IIoT, OS logs	Limited sensor-network correlation	[36] [41] [42]
Edge-IIoTset	IoT/IIoT	14 attack types	New, still under evaluation	[36]
TestCloudIDS	Cloud	DDoS (15 variants)	Cloud-specific, new	[44]
SWaT, HAI	CPS	Network & sensor attacks	Limited to CPS, real testbeds	[41]
CTU-13	Botnet	Botnet traffic	Narrow focus	[43]

Figure 1: Summary of widely used cyber threat detection datasets and their limitations.

4.2. Evaluation Metrics and Challenges

4.2.1. Common Evaluation Metrics

To assess the performance of ML/DL models in cyber threat detection, several standard metrics are used [10] [30] [35] [49] [33] [36] [17] [9]:

- **Accuracy:** Proportion of correctly classified instances (both benign and malicious).
- **Precision:** Proportion of true positives among all predicted positives (attack detections).
- **Recall (Detection Rate):** Proportion of true positives among all actual positives (sensitivity).
- **F1-Score:** Harmonic mean of precision and recall, balancing false positives and false negatives.
- **False Alarm Rate (FAR):** Proportion of benign instances incorrectly classified as attacks.
- **ROC-AUC, Cohen's Kappa, MCC:** Additional metrics for nuanced performance evaluation, especially in imbalanced datasets [34] [35] [49] [33] [36] [17].

4.2.2. Challenges in Evaluation

Metric	**Description**	**Key Challenges**	**Citations**
Accuracy	Overall correct predictions	Misleading in imbalanced datasets	[10] [30] [35] [49] [33] [36] [17] [9]
Precision	TP / (TP + FP)	Sensitive to false positives	[10] [30] [35] [49] [33] [36] [17] [9]
Recall	TP / (TP + FN)	Sensitive to false negatives	[10] [30] [35] [49] [33] [36] [17] [9]
F1-Score	Harmonic mean of precision/recall	Balances FP and FN	[10] [30] [35] [49] [33] [36] [17] [9]
FAR	FP / (FP + TN)	High FAR undermines trust	[10] [30] [35] [49] [33] [36] [17] [9]
ROC-AUC	Area under ROC curve	May not reflect real-world costs	[34] [35] [49] [33] [36] [17]

Figure 2: Evaluation metrics and their challenges in cyber threat detection.

V. OPEN ISSUES AND FUTURE DIRECTIONS

5.1. Current Research Gaps

Lack of Current and Accurate Datasets: The majority of published datasets are obsolete, synthetic, or insufficiently comprehensive about contemporary, advanced threats, hence constraining the creation and assessment of effective detection models. [10] [30] [9] [45] [46] [47] [48].

Adversarial Robustness: Machine learning and deep learning models continue to be susceptible to adversarial manipulation, necessitating investigation into robust and resilient architectures. [9] [44] [38].

Explainability and Interpretability: There is an urgent requirement for models that yield transparent, interpretable outputs to assist human analysts. [9] [44] [38] [51].

Generalization and Transferability: Ensuring that models trained on a certain dataset or environment can generalize to novel, unencountered threats and domains presents a significant problem [10]. [30] [9] [32] [38] [35] [49] [33] [36] [17].

5.2. Promising Future Research Directions

- **Development of Dynamic, Continuously Updated Datasets:** Establishing datasets that accurately represent contemporary attack trends and real-world diversity, encompassing multi-step and covert attacks. 45 [46] [52].
- **Adversarially Robust and Explainable Models:** Developing machine learning and deep learning models that are resilient to adversarial assaults while offering interpretable outcomes. 9 [44] [38] [51].
- **Federated and Transfer Learning:** Utilizing federated learning and domain adaptation to enhance generalization across varied environments [36] [42].
- **Synthetic Data Generation and Data Augmentation:** Employing generative models (e.g., GANs) to enhance datasets and replicate infrequent or novel attack situations [53].

VI. CONCLUSION

The imperative for intelligent, adaptive protection mechanisms in cybersecurity is unequivocal, signifying a clear transition from traditional, signature-based tools to data-driven systems enhanced by machine learning (ML) and deep learning (DL). This thorough research offers a comparative overview of machine learning's application in cyber threat detection, effectively achieving its goals by scrutinizing major methodologies, assessing prevalent datasets, and addressing significant problems impeding implementation.

Key Findings and Comparative Landscape

Our analysis confirmed that major ML techniques offer distinct, yet complementary, strengths and trade-offs:

- **Supervised Learning** remains foundational for classifying *known threats* efficiently but is inherently limited by its reliance on meticulously labeled data and its poor response to novel attack vectors.
- **Unsupervised Learning** is vital for detecting subtle anomalies and *zero-day exploits*, though its efficacy is often mitigated by the complexity of interpretation and a higher incidence of false positives.
- **Deep Learning** architectures, notably CNNs and LSTMs, exhibit superior performance in high-volume, complex environments, consistently achieving high accuracy (often 98–99%). However, this comes at the cost of high computational demands and reduced model transparency.

The convergence of these methods in **Hybrid and Ensemble Models** has yielded the most promising results, establishing them as the **current state-of-the-art**. By fusing multiple algorithmic strengths, these systems demonstrate enhanced accuracy, resilience, and generalization capabilities essential for combating dynamic, multi-class cyber threats.

The Imperative for Ongoing Research and Adaptation

Despite these technological advancements, the full operationalization of ML in cybersecurity is critically dependent on addressing three fundamental challenges:

1. **Data Quality and Realism:** The persistent reliance on outdated or synthetic public datasets, plagued by class imbalance and a lack of real-world threat diversity (as seen in NSL-KDD or CICIDS2017), severely limits model generalization and real-world applicability.
2. **Adversarial Robustness:** The vulnerability of ML/DL models to subtle adversarial manipulations represents a critical security failure point. Future research must concentrate on designing models and defense strategies that are intrinsically robust against sophisticated evasion tactics.
3. **Explainability (XAI):** The opacity of complex models, particularly in deep learning and ensemble structures, erodes the confidence of security analysts. Developing models that provide transparent, interpretable, and justifiable decisions is paramount for their adoption in mission-critical, human-in-the-loop defense systems.In closing, machine learning has transitioned from a theoretical concept to an indispensable core element of

modern cybersecurity infrastructure. The path forward requires a unified research focus: developing dynamic, highly robust, and transparent detection systems that leverage the power of advanced hybrid ML models while simultaneously addressing the foundational issues of data quality and adversarial resilience. Only through this sustained, multi-faceted approach can we ensure that cyber defense capabilities can effectively keep pace with the ever-evolving global threat landscape.

REFERENCES

[1] Al., N. AI in Cybersecurity: Threat Detection and Response with Machine Learning. *Tuijin Jishu/Journal of Propulsion Technology*. 2023. https://doi.org/10.52783/tjjpt.v44.i3.237

[2] Ahsan, M., Nygard, K., Gomes, R., Chowdhury, M., Rifat, N., & Connolly, J. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning - A Review. *J. Cybersecure. Priv.* 2022; 2. https://doi.org/10.3390/jcp2030027

[3] Abrahams, T., Okoli, U., Obi, O., & Adewusi, A. Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*. 2024. https://doi.org/10.30574/wjarr.2024.21.1.0315

[4] Prakriti, P. Cyber Threat Detection Using Machine Learning. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. 2024. https://doi.org/10.55041/ijsrem36799

[5] Liu, H., & Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences*. 2019. https://doi.org/10.3390/app9204396

[6] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*. 2024; 12. https://doi.org/10.1109/access.2024.3355547

[7] Meng, X. Advanced AI and ML techniques in cybersecurity: Supervised and unsupervised learning, reinforcement learning, and neural networks in threat detection and response. *Applied and Computational Engineering*. 2024. https://doi.org/10.54254/2755-2721/82/2024glg0054

[8] Salem, A., Azzam, S., Emam, O., & Abohany, A. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*. 2024; 11. https://doi.org/10.1186/s40537-024-00957-y

[9] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access*. 2018; 6. https://doi.org/10.1109/access.2018.2836950

[10] Ferrag, M., Maglaras, L., Moschoyiannis, S., & Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* 2020; 50. https://doi.org/10.1016/j.jisa.2019.102419

[11] Rishad, S. LEVERAGING AI AND MACHINE LEARNING FOR PREDICTING, DETECTING, AND MITIGATING CYBERSECURITY THREATS: A COMPARATIVE STUDY OF ADVANCED MODELS. *International Journal of Computer Science & Information System*. 2025. https://doi.org/10.55640/ijcsis/volume10issue01-02

[12] Shaukat, K., Luo, S., Chen, S., & Liu, D. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. *2020 International Conference on Cyber Warfare and Security (ICCWS)*. 2020. https://doi.org/10.1109/iccws48432.2020.9292388

[13] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., Chen, S., Liu, D., & Li, J. Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity. *Energies*. 2020. https://doi.org/10.3390/en13102509

[14] Avci, I., & Koca, M. Cybersecurity Attack Detection Model, Using Machine Learning Techniques. *Acta Polytechnica Hungarica*. 2023. https://doi.org/10.12700/aph.20.7.2023.7.2

[15] An, P., Wang, Z., & Zhang, C. Ensemble unsupervised autoencoders and Gaussian mixture model for cyberattack detection. *Inf. Process. Manag.* 2022; 59. https://doi.org/10.1016/j.ipm.2021.102844

[16] Lee, J., Kim, J., Kim, I., & Han, K. Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles. *IEEE Access*. 2019; 7. https://doi.org/10.1109/access.2019.2953095

[17] Vinayakumar, R., Alazab, M., Member, I., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*. 2019; 7. https://doi.org/10.1109/access.2019.2895334

[18] Vinayakumar, R., Alazab, M., Member, I., Poornachandran, P., & Venkatraman, A. Robust Intelligent Malware Detection Using Deep Learning. *IEEE Access*. 2019; 7. https://doi.org/10.1109/access.2019.2906934

[19] Jullian, O., Otero, B., Rodríguez, E., Gutiérrez, N., Antona, H., & Canal, R. Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework. *Journal of Network and Systems Management*. 2023; 31. https://doi.org/10.1007/s10922-023-09722-7

[20] Hnamte, V., Nhung-Nguyen, H., Hussain, J., & Hwa-Kim, Y. A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE. *IEEE Access*. 2023; 11. https://doi.org/10.1109/access.2023.3266979

[21] Gümüşbaş, D., Yıldırım, T., Genovese, A., & Scotti, F. A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems. *IEEE Systems Journal*. 2020; 15. https://doi.org/10.1109/jsyst.2020.2992966

[22] Ferrag, M., Ndhlovu, M., Tihanyi, N., Cordeiro, L., Debbah, M., Lestable, T., & Thandi, N. Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices. *IEEE Access*. 2023; 12. https://doi.org/10.1109/access.2024.3363469

[23] Ali, S., Razzaque, A., Yousaf, M., & Ali, S. A Novel AI-Based Integrated Cybersecurity Risk Assessment Framework and Resilience of National Critical Infrastructure. *IEEE Access*. 2025; 13. https://doi.org/10.1109/access.2024.3524884

[24] Sewak, M., Sahay, S., & Rathore, H. Deep Reinforcement Learning in the Advanced Cybersecurity Threat Detection and Protection. *Information Systems Frontiers*. 2022; 25. https://doi.org/10.1007/s10796-022-10333-x

[25] Verma, A., & Rathore, M. Intelligent Cyber Threat Detection in IoT and Network Environments Using Hybrid Ensemble Learning. *Journal of Information Systems Engineering and Management*. 2025. https://doi.org/10.52783/jisem.v10i37s.6729

[26] Hossain, M., & Islam, M. Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. *Array*. 2023; 19. https://doi.org/10.1016/j.array.2023.100306

[27] P, A., T, S., B, S., & Jose, J. Enhancing Cyber Threat Detection Accuracy: An AI-Powered Approach with Feature Selection and Machine Learning with Ensemble Learning for Cyber Threat Detection. *International Journal for Multidisciplinary Research*. 2025. https://doi.org/10.36948/ijfmr.2025.v07i02.39812

[28] Shan, A., & Myeong, S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. *Sensors (Basel, Switzerland)*. 2024; 24. https://doi.org/10.3390/s24154888

[29] Okey, O., Maidin, S., Adasme, P., Rosa, R., Saadi, M., Melgarejo, D., & Rodríguez, D. BoostedEnML: Efficient Technique for Detecting Cyberattacks in IoT Systems Using Boosted Ensemble Machine Learning. *Sensors (Basel, Switzerland)*. 2022; 22. https://doi.org/10.3390/s22197409

[30] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I., & Xu, M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*. 2020; 8. https://doi.org/10.1109/access.2020.3041951

[31] Gawand, S., & Meesala, S. Improved Framework for Detecting and Predicting Various Cyber Attacks Using the NSL-KDD Dataset. *International Research Journal on Advanced Engineering Hub (IRJAEH)*. 2025. https://doi.org/10.47392/irjaeh.2025.0118

[32] Leevy, J., & Khoshgoftaar, T. A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. *Journal of Big Data*. 2020; 7. https://doi.org/10.1186/s40537-020-00382-x

[33] Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. *Applied Sciences*. 2023. https://doi.org/10.3390/app13137507

[34] Saranya, T., & Priyadharshini, I. A Dual-Strategy Framework for Cyber Threat Detection in Imbalanced, High-Dimensional Data Across Heterogeneous Networks. *IEEE Access*. 2025; 13. https://doi.org/10.1109/access.2025.3582788

[35] Talukder, M., Islam, M., Uddin, M., Hasan, K., Sharmin, S., Alyami, S., & Moni, M. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *Journal of Big Data*. 2024; 11. https://doi.org/10.48550/arxiv.2401.12262

[36] Ferrag, M., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access*. 2022; PP. https://doi.org/10.1109/access.2022.3165809

[37] Bagui, S., & Li, K. Resampling imbalanced data for network intrusion detection datasets. *Journal of Big Data*. 2021; 8. https://doi.org/10.1186/s40537-020-00390-x

[38] Kumar, P., Gupta, G., & Tripathi, R. Toward Design of an Intelligent Cyber Attack Detection System using Hybrid Feature Reduced Approach for IoT Networks. *Arabian Journal for Science and Engineering*. 2021; 46. https://doi.org/10.1007/s13369-020-05181-3

[39] Dey, A., Gupta, G., & Sahu, S. A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks. *Decision Analytics Journal*. 2023. https://doi.org/10.1016/j.dajour.2023.100206

[40] Ismail, S., Dawoud, D., & Reza, H. A Comparative Study of Datasets for Cyber-attacks Detection in Wireless Sensor Networks. *2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI)*. 2024. https://doi.org/10.1109/icmi60790.2024.10586154

[41] Tushkanova, O., Levshun, D., Branitskiy, A., Fedorchenko, E., Novikova, E., & Kotenko, I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. *Algorithms*. 2023; 16. https://doi.org/10.3390/a16020085

[42] Ismail, S., Dandan, S., & Qushou, A. Intrusion Detection in IoT and IIoT: Comparing Lightweight Machine Learning Techniques Using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset Datasets. *IEEE Access*. 2025; 13. https://doi.org/10.1109/access.2025.3554083

[43] Sharma, A., & Babbar, H. Detecting Cyber Threats in Real-Time: A Supervised Learning Perspective on the CTU-13 Dataset. *2024 5th International Conference for Emerging Technology (INCET)*. 2024. https://doi.org/10.1109/incet61516.2024.10593100

[44] Vashishtha, L., & Chatterjee, K. Strengthening cybersecurity: TestCloudIDS dataset and SparkShield algorithm for robust threat detection. *Comput. Secur.* 2025; 151. https://doi.org/10.1016/j.cose.2024.104308

[45] Kenyon, A., Deka, L., & Elizondo, D. Are public intrusion datasets fit for purpose characterising the state of the art in intrusion event datasets. *Comput. Secur.* 2020; 99. https://doi.org/10.1016/j.cose.2020.102022

[46] Anjum, M., Iqbal, S., & Hamelin, B. Analyzing the Usefulness of the DARPA Optic Dataset in Cyber Threat Detection Research. *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*. 2021. https://doi.org/10.1145/3450569.3463573

[47] Goldschmidt, P., & Chud'a, D. Network Intrusion Datasets: A Survey, Limitations, and Recommendations. *Comput. Secur.* 2025; 156. https://doi.org/10.1016/j.cose.2025.104510

[48] Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. *IEEE Access*. 2020; 8. https://doi.org/10.1109/access.2020.3000179

[49] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*. 2019; 2. https://doi.org/10.1186/s42400-019-0038-7

[50] Tran, N., Chen, H., Bhuyan, J., & Ding, J. Data Curation and Quality Evaluation for Machine Learning-Based Cyber Intrusion Detection. *IEEE Access*. 2022; 10. https://doi.org/10.1109/access.2022.3211313

[51] Le, T., Kim, H., Kang, H., & Kim, H. Classification and Explanation for Intrusion Detection System Based on Ensemble Trees and SHAP Method. *Sensors (Basel, Switzerland)*. 2022; 22. https://doi.org/10.3390/s22031154

[52] Almseidin, M., Al-Sawwa, J., & Alkasassbeh, M. Generating a benchmark cyber multi-step attacks dataset for intrusion detection. *J. Intell. Fuzzy Syst.* 2022; 43.

[53] Villegas-Ch., W., Gutierrez, R., & Govea, J. Generative Adversarial Networks for Dynamic Cybersecurity Threat Detection and Mitigation. *Emerging Science Journal*. 2025. https://doi.org/10.28991/esj-2025-09-02-029

[54] Gümüşbaş, D., Yıldırım, T., Genovese, A., & Scotti, F. A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems. *IEEE Systems Journal*. 2020; 15. https://doi.org/10.1109/jsyst.2020.2992966

[55] Tulsyan, R., Shukla, P., Singh, T., & Bhardwaj, A. Cyber Security Threat Detection Using Machine Learning. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. 2024. https://doi.org/10.55041/ijsrem37949