ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1639

Machine Learning Techniques for Cybersecurity Threat Detection: A Systematic Review

Musa Tanimu Karatu[1]; Ibrahim Musa Mungadi[2]; Anas Shehu[3]

[1,2,3]Department of Computer Science, Federal University Birnin Kebbi, 860222, Nigeria

Publication Date: 2026/04/03

Abstract: The increasing complexity and prevalence of cyber threats have made the adoption of intelligent and adaptive security frameworks imperative. Traditional signature-based detection methods have proven insufficient, particularly in identifying zero-day exploits and rapidly evolving attack patterns. In this context, machine learning (ML) has emerged as a robust approach to cybersecurity threat detection, owing to its ability to learn underlying patterns and detect anomalies within large and complex datasets.

This study presents a comprehensive review of machine learning techniques applied in cybersecurity, encompassing supervised, unsupervised, and deep learning paradigms. It examines the application of these techniques in key areas such as intrusion detection, malware analysis, phishing detection, and network traffic monitoring. Furthermore, the paper evaluates commonly utilized datasets, performance metrics, prevailing challenges, and prospective research directions.

The findings reveal that hybrid and deep learning models generally outperform conventional methods in terms of detection accuracy and adaptability. However, challenges such as data imbalance and vulnerability to adversarial attacks continue to pose significant limitations, highlighting the need for further research and innovation in this domain.

Keyword: *Cyber Security, Detection, Learning, Machine, Techniques, Threat.*

How to Cite: Musa Tanimu Karatu; Ibrahim Musa Mungadi; Anas Shehu (2026) Machine Learning Techniques for Cybersecurity Threat Detection: A Systematic Review. *International Journal of Innovative Science and Research Technology,* 11(3), 2992-2998. https://doi.org/10.38124/ijisrt/26mar1639

I. INTRODUCTION

The rapid digital transformation of contemporary society has resulted in an unprecedented dependence on interconnected systems, including cloud computing infrastructures, mobile technologies, critical infrastructures, and the Internet of Things (IoT). Although these technological advancements have significantly enhanced efficiency and accessibility, they have concurrently introduced substantial vulnerabilities within cyberspace. Consequently, cybersecurity has emerged as a critical concern for governments, organizations, and individuals on a global scale.

Over the past decade, cyber threats have increased considerably in both scale and complexity. Modern attackers utilize sophisticated techniques such as polymorphic malware, zero-day vulnerabilities, ransomware-as-a-service (RaaS), and Advanced Persistent Threats (APTs) to circumvent conventional security mechanisms. These threats are typically dynamic, covert, and adaptive, making them difficult to detect using traditional security approaches [1].

Conventional cybersecurity systems largely depend on signature-based and rule-based detection techniques. Signature-based approaches identify malicious activities by matching observed patterns against pre-existing attack signatures stored in databases. While effective for detecting known threats, these methods are inherently limited in identifying novel or previously unseen attacks, commonly referred to as zero-day attacks. Additionally, the continuous maintenance and updating of signature databases require significant time and computational resources [2].

To address these challenges, the cybersecurity field has increasingly embraced machine learning (ML) techniques. As a branch of artificial intelligence, machine learning allows systems to autonomously learn from data, identify patterns, and make intelligent decisions with limited human involvement. Unlike traditional methods, ML-based systems possess the ability to generalize from historical data and identify anomalies that may indicate potential security threats.

A major advantage of machine learning in cybersecurity is its capacity to process and analyze large volumes of heterogeneous data generated by modern network environments. Such data include network traffic logs, system event records, user activity logs, and application-level information. By leveraging these diverse data sources, ML

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1639

models can uncover hidden relationships and patterns that are often undetectable through manual or rule-based analysis [18].

Machine learning techniques can be broadly classified into supervised, unsupervised, and semi-supervised learning paradigms. Supervised learning utilizes labeled datasets to train models capable of classifying data into predefined categories, such as benign or malicious. In contrast, unsupervised learning identifies underlying structures within unlabeled data and is particularly effective for anomaly detection. Semi-supervised learning combines both approaches, enabling models to learn from limited labeled data alongside abundant unlabeled data.

In recent years, deep learning, a more advanced branch of machine learning has attracted significant interest in cybersecurity applications. Models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can automatically learn intricate, high-level features from raw data, leading to improved detection accuracy. These models have demonstrated superior effectiveness in applications such as intrusion detection, malware classification, and network traffic analysis [6].

Despite these advancements, several challenges continue to hinder the effective deployment of machine learning in cybersecurity. Issues such as class imbalance, high false positive rates, limited model interpretability, and susceptibility to adversarial attacks remain significant concerns. Furthermore, the availability of high-quality and up-to-date datasets poses a major limitation, as many existing datasets are either outdated or fail to accurately represent real-world cyber threat scenarios.

In light of these challenges, there is an increasing need for comprehensive studies that evaluate the current state of machine learning applications in cybersecurity, identify existing research gaps, and propose future research directions. This paper aims to address this need by providing an extensive review of machine learning techniques, their applications, and their effectiveness in cybersecurity threat detection.

- *The Main Contributions of this Paper are Summarized as Follows:*

- A thorough examination of machine learning techniques utilized in cybersecurity threat detection
- A detailed analysis of their use across multiple areas, such as intrusion detection, malware analysis, and phishing detection
- A discussion of commonly used datasets and evaluation metrics
- Identification of key challenges and limitations in existing approaches
- Recommendations for future research directions

II. RELATED WORK

The application of machine learning (ML) techniques in cybersecurity has been widely explored over the past decade, with notable advancements occurring between 2020 and 2025. Early foundational studies critically examined the limitations of anomaly-based intrusion detection systems (IDS), highlighting that many proposed models failed to perform effectively in real-world environments due to unrealistic assumptions and the use of low-quality datasets [17]. These studies identified persistent challenges such as high false positive rates and the inherent difficulty in accurately modeling normal network behavior.

In recent years, there has been a growing emphasis on leveraging advanced machine learning and deep learning approaches to improve detection accuracy and system adaptability. For instance, recent studies have introduced intrusion detection frameworks based on deep neural networks (DNNs) for analyzing network traffic. The results indicate that deep learning models outperform traditional machine learning methods in terms of accuracy, scalability, and their capacity to process high-dimensional data [18].

Similarly, other studies introduced non-symmetric deep autoencoder architectures for intrusion detection. By combining unsupervised feature extraction with supervised classification, these approaches enable the learning of meaningful representations from raw network data. Experimental results indicate improved detection performance and reduced computational complexity when compared to conventional methods [16].

Comprehensive surveys in the literature have further analyzed ML-based intrusion detection systems by categorizing them into supervised, unsupervised, and hybrid approaches. These studies conclude that hybrid and ensemble techniques generally achieve superior performance, as they effectively integrate the strengths of multiple algorithms. Additionally, the importance of feature selection has been emphasized as a critical factor in improving model efficiency and minimizing overfitting [8].

In the context of large-scale and heterogeneous environments, particularly within the Internet of Things (IoT), deep learning has been identified as a promising solution for enhancing security. Existing research highlights unique challenges in IoT environments, including limited computational resources, energy constraints, and device heterogeneity. Consequently, there is a growing need for lightweight and efficient ML models capable of operating under constrained conditions while maintaining high detection accuracy [6].

Recent research has also investigated hybrid approaches that combine machine learning with complementary methods such as optimization algorithms, statistical techniques, and rule-based systems. Hybrid intrusion detection systems, which integrate anomaly-based and misuse-based detection strategies, have shown enhanced effectiveness in detecting both known and unknown threats.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1639

These systems utilize signature-based methods to identify known attacks while employing anomaly detection to capture zero-day threats, thereby improving overall system robustness.

Another significant trend in recent research is the use of deep learning architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks. CNNs have been extensively utilized in malware detection by converting binary data into image-like formats, whereas RNNs and LSTMs are well-suited for processing sequential data, including network traffic patterns and user activities. These approaches have demonstrated strong performance in modeling both spatial and temporal relationships within datasets [18].

Despite these advancements, several limitations persist within the current body of research. A significant concern is the reliance on outdated benchmark datasets such as KDD Cup 99 and NSL-KDD, which fail to accurately represent modern network environments and evolving attack patterns. This limitation raises questions regarding the generalizability of many proposed models in real-world scenarios. Furthermore, data imbalance—where malicious instances are significantly underrepresented—continues to negatively impact model performance and bias detection outcomes.

Additionally, the emergence of adversarial machine learning has introduced new security challenges, as attackers can manipulate input data to deceive ML-based systems. This has led to increased research efforts focused on developing robust and resilient models capable of withstanding adversarial attacks. Moreover, model explainability and interpretability have become critical considerations, particularly in high-risk environments where understanding the decision-making process is essential for trust and accountability.

In summary, the literature reveals a clear shift from conventional machine learning methods toward more advanced deep learning and hybrid approaches in cybersecurity threat detection. Despite notable improvements in accuracy and efficiency, several challenges persist, including limited datasets, susceptibility to adversarial attacks, and insufficient model interpretability. Tackling these issues is crucial for developing dependable, scalable, and practical machine learning–driven cybersecurity solutions.

III. MACHINE LEARNING TECHNIQUES FOR CYBERSECURITY

Machine learning (ML) techniques have become essential in modern cybersecurity because of their ability to handle large-scale data, identify underlying patterns, and adapt to constantly evolving threats. In contrast to traditional rule-based methods, ML-based systems offer flexible and scalable solutions that can detect both known and emerging cyber-attacks. These approaches are generally classified into supervised, unsupervised, semi-supervised, deep learning, ensemble learning, reinforcement learning, and hybrid methods, each offering distinct strengths and limitations [8,6].

The effectiveness of these techniques is influenced by several factors, including data quality, feature representation, computational resources, and the specific characteristics of the cyber threats being addressed.

- *Supervised Learning*

Supervised learning is one of the most well-established and widely utilized approaches in cybersecurity. It depends on labeled datasets, where each instance is identified as either normal or malicious, enabling the model to learn decision boundaries for accurately classifying new, unseen data.

Common supervised algorithms include Support Vector Machines (SVM), Decision Trees, Random Forests, k-Nearest Neighbors (k-NN), and Logistic Regression [1]. Among these, Random Forest is noted for its resistance to overfitting and its effectiveness in handling high-dimensional data, while SVM performs particularly well in cases with clearly defined class boundaries and smaller datasets.

These techniques have been widely applied in domains such as intrusion detection systems (IDS), malware classification, phishing detection, spam filtering, and fraud detection. Their primary advantage lies in achieving high accuracy when trained on high-quality labeled data. However, the dependence on labeled datasets presents a major limitation, as such data are often costly and time-consuming to obtain. Additionally, supervised models struggle to detect zero-day attacks since they rely on previously learned patterns [2].

Another significant challenge is class imbalance, where malicious instances are underrepresented compared to benign ones. This imbalance can bias the model toward the majority class, thereby reducing its effectiveness in detecting rare but critical threats [6].

- *Unsupervised Learning*

Unsupervised learning plays a critical role in cybersecurity, particularly in anomaly detection, where the goal is to identify deviations from normal system behavior. Unlike supervised methods, unsupervised techniques do not require labeled data, making them well-suited for dynamic and evolving environments.

Common techniques include K-Means clustering, DBSCAN, and Principal Component Analysis (PCA) [2]. K-Means is frequently used for clustering similar data points, while DBSCAN is effective in identifying outliers and handling noisy data. PCA is primarily utilized for dimensionality reduction, enabling efficient processing of large datasets.

Applications of unsupervised learning in cybersecurity include network anomaly detection, insider threat detection, behavioral analysis, and fraud detection. A key advantage of this approach is its ability to detect unknown or zero-day

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1639

attacks. However, it is often associated with high false positive rates, as not all anomalies correspond to malicious activities [5].

Furthermore, the performance of unsupervised models is highly dependent on feature selection and distance metrics. Inadequate feature representation may lead to inaccurate clustering and reduced detection performance, emphasizing the importance of effective feature engineering.

- *Semi-Supervised Learning*

Semi-supervised learning merges the advantages of supervised and unsupervised methods by making use of both labeled and unlabeled data. This approach is especially useful in cybersecurity, where labeled datasets are often scarce but unlabeled data is plentiful. Techniques like self-training, co-training, and graph-based learning allow models to improve iteratively by utilizing high-confidence predictions derived from the unlabeled data. [7,9]. For example, in intrusion detection, an initial model trained on a small labeled dataset can be progressively refined using unlabeled data.

The key advantages of semi-supervised learning include reduced reliance on labeled data, improved generalization, and enhanced scalability. However, challenges such as error propagation and sensitivity to the quality of initial labeled data can negatively impact performance [6,10].

- *Deep Learning Techniques*

Deep learning has brought significant advancements to cybersecurity by enabling the automatic extraction of features and the modeling of complex, high-dimensional data. Unlike traditional machine learning approaches, deep learning models learn layered feature representations directly from raw inputs.

Key architectures include Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, autoencoders, and Generative Adversarial Networks (GANs). CNNs are commonly applied in malware detection by transforming binary files into image-like formats, whereas RNNs and LSTMs are well-suited for analyzing sequential data such as network traffic and user behavior patterns [18,12].

Autoencoders are often used for anomaly detection by learning compact representations of normal activity, while GANs are utilized to generate synthetic attack data and improve model robustness. Despite their high performance, deep learning models typically demand significant computational resources and large datasets. Moreover, their limited interpretability presents challenges in critical cybersecurity applications [6,10,11].

- *Ensemble Learning*

Ensemble learning has gained prominence as an effective approach for boosting predictive accuracy and strengthening model robustness. It involves combining multiple base learners to reduce generalization error and mitigate issues such as overfitting and bias [8,14,15].

Ensemble methods are typically categorized into bagging, boosting, and stacking. Bagging techniques, such as Random Forest, reduce variance by training models on randomly sampled subsets of data. Boosting methods, including AdaBoost and XGBoost, improve performance by sequentially focusing on misclassified instances. Stacking combines multiple models using a meta-learner to leverage their complementary strengths.

In cybersecurity, ensemble learning has demonstrated strong performance in intrusion detection, malware classification, and fraud detection. However, these methods often introduce increased computational complexity and reduced interpretability, which may limit their applicability in real-time systems [6].

- *Reinforcement Learning*

Reinforcement learning (RL) represents a distinct paradigm in which agents learn optimal decision-making strategies through interaction with an environment. Unlike supervised and unsupervised learning, RL relies on a reward-based mechanism rather than labeled data [5].

In cybersecurity, RL agents observe network states and take actions such as blocking malicious traffic or isolating compromised systems, with the goal of maximizing cumulative rewards. Applications include adaptive intrusion response systems, automated threat mitigation, and dynamic resource allocation.

Recent developments in deep reinforcement learning (DRL), including Deep Q-Networks (DQN) and policy gradient methods, have enhanced the capability of RL in handling complex and high-dimensional environments. However, challenges such as environment modeling, delayed rewards, and the risks associated with exploratory actions remain significant barriers to practical deployment [6].

- *Hybrid Approaches*

Hybrid machine learning approaches combine multiple techniques to capitalize on their complementary strengths and mitigate individual limitations. These methods have attracted considerable attention in cybersecurity due to their potential to enhance detection accuracy and system robustness [8].

A common strategy involves integrating supervised and unsupervised learning, where supervised models target known threats while unsupervised models detect previously unseen anomalies. Another approach pairs deep learning for automatic feature extraction with traditional machine learning algorithms for classification.

Hybrid models can also incorporate optimization methods, such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO), for feature selection and parameter tuning. Furthermore, the inclusion of rule-based systems allows domain knowledge to supplement data-driven models, improving decision-making in complex scenarios.

While hybrid approaches offer greater performance and adaptability, they also present challenges related to system

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1639

complexity, computational demands, and maintenance. Despite these challenges, they provide a promising avenue for developing robust, scalable cybersecurity solutions capable of addressing evolving cyber threats [6].

➢ *Comparative Analysis of Techniques*

The Table 1 below provides a more detailed comparison of machine learning techniques used in cybersecurity:

Table 1. Comparison of Machine Learning Techniques Used in Cybersecurity

Technique	Accuracy Range	Strengths	Weaknesses	Best Use Case
Supervised Learning	85–99%	High accuracy, well-structured models, effective classification	Requires labeled data, poor zero-day detection	Malware detection, phishing
Unsupervised Learning	70–90%	Detects unknown threats, no labeling needed	High false positives, sensitive to features	Anomaly detection
Semi-Supervised Learning	80–95%	Reduces labeling effort, improves generalization	Error propagation risk	IDS with limited labels
Deep Learning	90–99%+	Handles complex data, automatic feature extraction	High computation, low interpretability	Advanced intrusion detection
Ensemble Learning	92–99%	High robustness, reduces overfitting	Complex, resource-intensive	High-accuracy systems
Reinforcement Learning	Variable	Adaptive, real-time decision making	Complex training, unstable learning	Automated response systems
Hybrid Models	95–99%+	Best performance, combines strengths	High complexity, expensive	Enterprise security systems

IV. APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY

Machine learning has become a core element of contemporary cybersecurity because of its ability to automatically identify patterns within large and complex datasets. The constantly evolving and dynamic nature of cyber threats requires intelligent systems that can detect both known and emerging attacks in real time. As a result, ML techniques have been extensively applied across various cybersecurity areas, including intrusion detection, malware analysis, phishing detection, and network traffic monitoring [1].

➢ *Intrusion Detection Systems (IDS)*

Intrusion Detection Systems (IDS) are among the most significant applications of machine learning in cybersecurity. Traditional signature-based IDS depend on predefined attack patterns, which restricts their ability to detect new or zero-day attacks. In contrast, ML-based IDS employ data-driven methods to identify anomalous patterns in network traffic.

Supervised learning algorithms, including Support Vector Machines (SVM), Random Forests, and Artificial Neural Networks (ANN), are frequently used for classification tasks, whereas unsupervised methods like clustering and anomaly detection help uncover previously unseen attack patterns. These systems can efficiently detect threats such as Distributed Denial of Service (DDoS) attacks, port scanning, and brute-force attacks by analyzing network traffic features like packet distribution and connection behavior [1].

Despite their strengths, ML-based IDS face challenges such as high false positive rates, concept drift, and reliance on large labeled datasets. Therefore, continuous retraining and feature optimization are critical to sustaining system performance in dynamic environments.

➢ *Malware Detection*

Malware detection is another key area where machine learning plays a vital role in cybersecurity. Traditional antivirus solutions rely on signature-based methods, which are often ineffective against polymorphic and metamorphic malware. Machine learning offers a more resilient approach by analyzing both static and dynamic features of executable files.

Static analysis examines characteristics such as byte sequences, opcode patterns, and metadata, while dynamic analysis evaluates runtime behavior, including system calls and network activity. Deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown superior performance by automatically extracting complex features from raw data [18].

Additionally, ensemble learning approaches improve detection accuracy by combining multiple classifiers. Nevertheless, challenges such as adversarial evasion and the need for real-time processing continue to pose significant obstacles.

➢ *Phishing Detection*

Phishing detection is a critical application of machine learning focused on identifying fraudulent attempts to steal sensitive information. These attacks often occur via emails, websites, or social engineering tactics, posing ongoing risks to both individuals and organizations.

ML-based phishing detection systems combine natural language processing (NLP) with classification algorithms to analyze the content and structure of emails and web pages. Commonly used features include URL characteristics, domain age, lexical patterns, and HTML structures. Algorithms such as Logistic Regression, Decision Trees,

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1639

Random Forests, and Deep Neural Networks are frequently employed for these classification tasks.

Machine learning enables systems to adapt to evolving phishing techniques; however, attackers often use obfuscation methods like URL shortening and encoding to bypass detection. This highlights the need for continuous model updates and feature optimization [8].

- *Network Traffic Analysis*

Network traffic analysis entails monitoring and examining data packets across networks to detect potential threats. Machine learning greatly improves this process by enabling real-time identification of anomalies.

ML models evaluate features such as packet size, flow duration, IP addresses, and protocol usage to uncover abnormal patterns. Unsupervised techniques are especially effective for detecting unknown threats, while supervised models excel at identifying known attacks. Deep learning methods, including Long Short-Term Memory (LSTM) networks, can capture temporal dependencies within traffic data.

These systems support the detection of threats like DDoS attacks, data exfiltration, and botnet activity, often triggering automated responses to mitigate risks. Nonetheless, challenges such as high data dimensionality, encrypted traffic, and real-time processing requirements remain significant [6].

V. DATASETS AND EVALUATION METRICS

The development and evaluation of ML models in cybersecurity depend heavily on the quality of datasets and the selection of appropriate evaluation metrics. Datasets provide the foundation for training and validation, while metrics enable objective performance assessment and comparison across models [1].

- *Common Datasets*

Several benchmark datasets have been widely used in cybersecurity research. The KDD Cup 99 dataset, one of the earliest datasets, contains labeled network traffic records categorized into various attack types. However, it suffers from redundancy, class imbalance, and outdated attack patterns.

The NSL-KDD dataset was introduced to address these limitations by removing redundant records and improving data balance, although it still lacks representation of modern threats.

More recent datasets, such as CICIDS2017 and UNSW-NB15, provide realistic and comprehensive representations of contemporary network traffic and attack scenarios. These datasets include diverse attack types and more representative features, making them suitable for evaluating advanced ML models.

Despite these advancements, challenges such as data imbalance, limited diversity, and insufficient representation of emerging threats persist, highlighting the need for continuously updated datasets [6].

- *Evaluation Metrics*

The performance of machine learning models in cybersecurity is assessed using various metrics to provide a thorough evaluation. Accuracy indicates the proportion of correctly classified instances but can be misleading in datasets with class imbalance.

Precision measures the proportion of correctly predicted positive cases, while recall evaluates the model's ability to identify actual positive instances. The F1-score offers a balanced assessment by combining both precision and recall.

Another key metric is the Receiver Operating Characteristic – Area Under Curve (ROC-AUC), which evaluates the model's capability to differentiate between classes across multiple thresholds. Considering the limitations of individual metrics, it is recommended to use a combination of evaluation measures to achieve a more reliable assessment of model performance [6].

- *Challenges and Limitations*

Despite notable advancements in applying machine learning to cybersecurity, several challenges continue to hinder its effectiveness in practical settings. A primary concern is data imbalance, where malicious instances are underrepresented, resulting in biased model predictions and reduced detection sensitivity [8].

High false positive rates also remain a significant issue, as an excessive number of alerts can overwhelm security analysts and undermine confidence in automated systems. Moreover, adversarial attacks present serious threats, allowing attackers to manipulate input data to mislead ML models and evade detection [6].

Scalability is another challenge, especially in large-scale environments that require real-time processing of vast, high-dimensional datasets. In addition, the scarcity of realistic and up-to-date datasets limits the generalizability of many ML models, highlighting the need for improved data collection and benchmarking practices.

VI. FUTURE RESEARCH DIRECTIONS

To address existing challenges, several promising research directions have been identified. Explainable Artificial Intelligence (XAI) aims to improve model transparency and interpretability, which is essential for trust and accountability in cybersecurity applications.

Federated learning offers a privacy-preserving approach by enabling collaborative model training across decentralized systems without sharing raw data. Hybrid machine learning models that combine multiple techniques

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1639

also show potential for improving detection accuracy and robustness [8].

Additionally, the development of real-time adaptive security systems capable of continuous learning is crucial for addressing evolving threats. The integration of machine learning with blockchain technology further presents opportunities for enhancing data integrity, transparency, and system resilience.

VII. CONCLUSION

Machine learning has profoundly impacted cybersecurity by enabling intelligent, data-driven methods for threat detection and prevention. By leveraging supervised, unsupervised, and deep learning techniques, modern systems can effectively recognize complex attack patterns and respond to threats in real time.

Among these methods, deep learning and hybrid models have shown superior performance due to their capacity to extract high-level features and combine multiple learning strategies. Nevertheless, challenges such as adversarial attacks, data imbalance, computational demands, and limited datasets continue to pose significant barriers.

Future developments in areas like explainable AI, federated learning, and hybrid modeling are expected to mitigate these challenges and improve the effectiveness of ML-based cybersecurity systems. Ongoing research and innovation are therefore crucial to fully harness the potential of machine learning in addressing increasingly sophisticated cyber threats.

REFERENCES

[1]. Ahmad, I., Basheri, M., Iqbal, A., & Rahim, N. (2021). Performance comparison of support vector machine and random forest for intrusion detection systems. *International Journal of Advanced Computer Science and Applications*, 12(2), 1–10.

[2]. Buczak, A. L., & Guven, E. (2020). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.

[3]. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761–768.

[4]. Dua, S., & Du, X. (2016). *Data mining and machine learning in cybersecurity*. CRC Press.

[5]. Ferrag, M. A., & Maglaras, L. (2021). Cyber security and machine learning: A systematic review. *Computer Science Review*, 42, 100–110.

[6]. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2022). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Network and Computer Applications*, 172, 102–140. https://doi.org/10.1016/j.jnca.2020.102823

[7]. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

[8]. Khan, W. Z., et al. (2021). Machine learning and deep learning approaches for intrusion detection systems: A review. *IEEE Access*, 9, 1–20.

[9]. Kotsiantis, S. B. (2007). Supervised machine learning: A review of classification techniques. *Informatica*, 31, 249–268.

[10]. Liu, H., Lang, B., & Li, M. (2021). Machine learning-based malware detection: A survey. *ACM Computing Surveys*, 54(6), 1–36. https://doi.org/10.1145/3460458

[11]. Mitchell, T. M. (1997). *Machine learning*. McGraw-Hill.

[12]. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *Military Communications and Information Systems Conference (MilCIS)*.

[13]. Nguyen, T. T., & Armitage, G. (2021). A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, 10(4), 56–76.

[14]. Sahu, A., & Shrivastava, V. (2020). Network traffic analysis using machine learning: A review. *Procedia Computer Science*, 167, 194–203. https://doi.org/10.1016/j.procs.2020.03.200

[15]. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)*.

[16]. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

[17]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *Proceedings of the IEEE Symposium on Security and Privacy*, 305–316.

[18]. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2020). Deep learning approach for intelligent intrusion detection system. *IEEE Transactions on Network and Service Management*, 17(2), 1–12.

[19]. Zhang, J., Chen, Z., & Zhao, X. (2022). Adversarial machine learning in cybersecurity: A survey. *IEEE Transactions on Dependable and Secure Computing*, 19(4), 1–18.

[20]. Zhou, Z. H. (2021). *Ensemble methods: Foundations and algorithms*. CRC Press.