INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES
ISSN: 2322-0821(O)
ISSN: 2394-9910(P)
VOLUME 14 ISSUE 2
Apr 2026 - June 2026
www.irjeas.org

Research Article

A Survey on Machine Learning – Based Cyber Threat Detection System

Yogita Mishra [1*]

[1*] Assistant Professor, Department of CSE, Bansal Institute of Research &Technology, Bhopal (M.P)
yogitamishra.999@gmail.com

*Corresponding Author: yogitamishra.999@gmail.com

DOI–10.55083/irjeas.2026.v14i02002

Abstract: Cyber Security has become a critical concern in the digital era due to rapid increase in sophisticated cyber-attacks. This paper is a complete survey of machine learning (ML)-based cyber threat detection systems, motivated by the increasing demand for smart and adaptable defence mechanisms in the evolving digital world. As the sophistication of cyber-attacks has increased, including malware and phishing, intrusion and distributed denial-of-service (DDoS) attacks, traditional signature detection mechanisms have not kept up. This study provides a systematic review of existing methods based on statistical, supervised learning, unsupervised learning, and deep learning approaches along with their strengths and limitations and domains of applications. Furthermore, the paper also introduces new context-aware multi-layer review methodology (CMLRM), which organizes existing research as per threat context, learning models, and operational environments for a structured evaluation of cyber threat detection systems. Also introduced is a dataset-centric analysis that enables us to study the influence of data quality, imbalance and feature representation on model performance. In addition, the existing approaches are measured with respect to performance metrics (accuracy, precision, recall and F1-score) as well as practical aspects like computational, cost, scalability, interpretability, and real-world deployment feasibility.

Keywords: Machine Learning; Cyber security; Cyber Threat Detection; Threat attribution; Artificial Intelligence; Real-Time Detection.

1. INTRODUCTION

Due to a wider and more intricate attack surface, the vulnerability to potential cyber-attacks has expanded as digital technologies continue to develop and integrate into contemporary systems. From distributed denial-of-service (DDoS) assaults and

polymorphic malware to advanced persistent threats (APTs) and zero-day exploits, modern cyberattacks have grown more complex, adaptable, and widespread. Due to their reliance on predetermined patterns and limited capacity to generalize across unforeseen attack scenarios, traditional security mechanisms like rule-based firewalls and signature-based intrusion detection systems are frequently insufficient in identifying these developing threats.

Because machine learning (ML) allows for data-driven and adaptive threat detection, it has become a potent paradigm for improving cyber security in response to these constraints. With little assistance from humans, ML-based systems are able to recognize unusual behaviors, learn intricate patterns from past data, and locate hitherto undiscovered assaults. Many machine learning (ML) approaches, such as supervised learning, unsupervised learning, and deep learning, have been used in the last ten years for a variety of cyber security tasks, including network anomaly analysis, intrusion detection, malware classification, and phishing detection. Both academics and industry are paying close attention to these approaches since they have shown better detection accuracy and automation than traditional methods.

In addition to growing interest in explainable artificial intelligence (XAI), federated learning, and privacy-preserving frameworks, recent research trends (2021–2026) show a paradigm shift away from standard machine learning models and toward deep learning and hybrid techniques. Furthermore, because of resource limitations, heterogeneity, and widely dispersed locations, emerging fields like cloud computing and the Internet of Things present new difficulties. As a result, there is an increasing demand for systematic review frameworks that assess existing work from many contextual viewpoints in addition to summarizing it.

In order to meet the aforementioned challenges, this paper provides an exhaustive review of cyber threat detection systems using machine learning techniques. Unlike previous survey papers, this work proposes a new Context-Aware Multi-Layer Review Methodology (CMLRM) that categorizes the literature on the basis of three interrelated aspects: threat context, learning model, and operational context. With this method, a more systematic and realistic way to evaluate the performance of the detection techniques can be provided. In addition, the importance of t-based cyber threat detection approaches by examining various methodologies, datasets, evaluation metrics, and applications currently being developed. he datasets used for the analysis is also considered using a dataset-oriented analysis based on parameters like the freshness of data, feature set, and imbalance between the classes. The goal of this survey paper is to give a detailed overview of the ML

2. MOTIVATION

Detection of Cyber Security Threats Using Statistical Methods and Machine Learning Techniques

The detection of cyber security threats has undergone considerable evolution due to the incorporation of various data-driven techniques, such as statistical methods and machine learning algorithms. These methodologies facilitate the detection of potential threats by examining vast amounts of data and identifying underlying patterns.

- **Statistical Model-Based Detection**

Statistical algorithms are one of the oldest building blocks of cyber intrusion detection techniques. Statistical methods employ probabilistic distributions and mathematical modeling to understand normal system behavior. Using statistics, an intruder could be detected by comparing deviations from the established baseline of the system's normal activities based on such parameters as traffic volume, packet size distribution, number of logins, or system calls. Various statistical techniques have been used for cyber security detection purposes, including hypothesis testing, Bayesian methods, Markov models,

and time series modeling. For example, a large deviation from the established baseline traffic profile can be considered a probable intrusion attempt. Although statistical approaches are efficient and easy to interpret, they suffer from limited applicability when applied to high dimensional data.

• **Supervised Learning-Based Detection**

The reason why supervised learning methods have become popular is that they have been successful at detecting known threats with high accuracy. This is because the algorithms used are trained using labeled data which include instances of both normal and malicious attacks. Some of the commonly used machine learning algorithms include Decision Trees, SVMs, k-NN, and Neural Networks. This method is especially useful when dealing with attacks with known signatures. With this information, the algorithms can be trained to detect attacks such as phishing attacks and malware attacks based on their signatures. However, supervised learning approaches rely too much on the availability and quality of training data. As a result, they cannot detect zero-day attacks.

• **Unsupervised Learning-Based Detection**

However, unsupervised learning algorithms tackle the problems associated with labeled data by discovering any hidden patterns and anomalies present in an unlabeled dataset. They are extensively used for anomaly detection where the purpose is to detect anomalies without any prior knowledge about the nature of the attack. Algorithms for clustering data such as k-Means and DBSCAN tend to cluster similar data points, making it possible to discover the outlier data that could signify a malicious activity. Methods like PCA are useful in reducing the dimensions of data to make it easier to detect anomalies in high-dimensional data. Further, auto encoders and other deep learning algorithms are useful in detecting anomalies. Unsupervised learning algorithms are especially useful when it comes to detecting new types of cyber-attacks. However, unsupervised algorithms may have more false positives.

• **Hybrid Approaches**

Hybrid architectures of cyber security have become common practice today, combining statistical, supervised learning, and unsupervised learning techniques in one system. These combinations improve detection performance due to the advantages of each approach. For example, statistics can be used for preprocessing data and filtering, classification can be done by supervised learners, and anomalies can be detected using unsupervised learning. The purpose of this survey is to give an insight into the field of machine learning-based cyber threat detection systems. We analyze the approaches, data sources, performance measures, and areas of application currently used in the literature on this topic.

Related survey and contribution:

Machine learning (ML) methods have played a major role in the design of intelligent cyber threats detection tools. Research works within this domain have transitioned from conventional ML algorithms to deep learning, hybrid learning models, and context-based architectures in the last few years. This chapter will critically review recent developments in cyber threat detection using ML in the period 2021–2026, with a focus on methodology, data sets, performance analysis, and future research directions. Research studies in the period of 2021–2022 mainly concentrated on improving traditional ML approaches used in IDS. Several supervised ML algorithms such as SVM, RF, DT, and k-NN were extensively used in the literature as they performed well for classification purposes. Most of these studies used benchmark data sets like NSL-KDD and UNSW-NB15 to train the ML algorithms, providing accurate classification of known cyber attacks.

In some research, feature selection and dimensional reduction were highlighted, helping in improving model efficiency and minimizing the computational cost incurred

by the models. Ensemble learning algorithms were applied by combining several models to produce better results in terms of increased accuracy and minimized false-positive detections. Unsupervised machine learning methods such as clustering and statistical anomaly detection were used to recognize new threats using an unsupervised learning framework. The weaknesses identified included heavy reliance on old data in training the models. The training datasets are static and thus do not reflect present-day cyber activity. Traditional machine learning approaches cannot capture complicated relationships and patterns, hence their inefficacy in detecting cyber threats.

Advancements in 2023: Deep Learning and Critical Infrastructure

Deep Learning approaches for cyber threat detection gained much attention in 2023. Many researches employed Convolution Neural Network (CNN), Recurrent Neural Network (RNN), and LSTM models to analyze network traffic or computer system behavior. Deep learning models exhibited their superiority in terms of the ability to learn spatial and temporal characteristics. Moreover, hybrid DL models, such as CNN-LSTM combinations, were utilized to combine advantages of both types. They provided better results in terms of accuracy as opposed to traditional ML algorithms.

Adversarial machine learning was another interesting trend that appeared in this year. Adversarial learning is a practice of generating samples that trick machine learning algorithm into making mistakes in predictions or classifications. Researches proved that the use of machine learning models in cyber security can be exploited by attackers through creating adversarial samples. Unfortunately, the use of deep learning models resulted in several issues, such as high demands for computational power and time. The problem is connected with poor explainability of the obtained results.

Studies from 2024: Expansion into IoT and Real-Time Detection

As for the developments in 2024, research has turned its attention toward protecting new environments such as IoT and cloud networks. IoT networks are difficult to secure due to limitations in terms of computational capacity, heterogeneity of devices, and other aspects that require the development of lightweight ML algorithms for real-time detection.

Deep learning models have become the predominant method, which proved to be effective in identifying complex attacks in IoT networks. For instance, auto encoders and DNNs were often used in anomaly detection in order to detect the presence of unusual activities within the network. Moreover, real-time detection systems have been developed to ensure rapid response to possible attacks. Feature selection and dimensionality reduction methods have also received attention because they can help deal with the problems associated with high dimensional data. Unfortunately, the problems concerning scalability, heterogeneity of data, and lack of datasets for IoT have not yet been resolved.

Studies from 2025–2026: Towards Explainable, Adaptive, and Privacy-Preserving Systems

The latest research trends (2025-2026) have aimed at overcoming shortcomings and gaps associated with previous methodologies through the introduction of explainable, adaptive, and privacy-preserving models. XAI methods have been employed to increase the transparency of machine learning algorithms. Techniques such as SHAP (Shapley Additive Explanations) have been employed to gain an understanding of machine learning algorithms.

Federated learning is considered a potential methodology that can address the challenge of privacy preservation during cyber threat detection. Such an approach allows multiple devices or organizations to participate in the training process without disclosing raw data, which makes it effective in distributed environments such as IoT and cloud computing. Finally, hybrid, ensemble models utilizing both traditional ML approaches and deep learning techniques have become

popular among researchers as they allow detecting threats with increased precision and robustness. Reinforcement learning adaptive models have also been proposed.

Conducted systematic reviews reveal persistent problems associated with dataset imbalance, lack of real-world data, computational complexity, and vulnerability to adversarial attacks. It is important to note that many authors stress that currently used datasets, such as NSL-KDD or CICIDS2017, do not represent modern cyber threats accurately enough.

Critical Analysis and Research Gaps

However, after an extensive review of the literature published recently, it is possible to draw several important conclusions. Firstly, there is a visible shift from classical machine learning towards deep learning and their combinations due to the necessity of dealing with complicated and massive data. Secondly, even though the effectiveness of detecting malicious behavior has been greatly improved, the problem of scalability, interpretability, and deployment still persists.

It is also important to note the excessive use of benchmark data in previous research, which do not reflect the real-life specifics such as dynamically changing traffic and attacks. Moreover, the majority of the articles concentrate on measuring performance without taking into consideration other important aspects such as computation time or real-time processing capabilities.

3. SURVEY METHODOLOGY

This survey employs a methodical and contextual approach for an in-depth study of cyber threat detection systems based on machine learning algorithms. While other traditional review methodologies focus more on the algorithmic accuracy of the system, this methodology incorporates a contextual classification system, dataset-based analysis, and deployment-oriented assessments of the available methods. The entire approach aims at providing a realistic analysis of the present methods by bridging the gap between theoretical research and cyber security practices.

The method starts with an efficient literature search process that gathers all the relevant papers related to cyber threat detection through machine learning or deep learning. The criteria for inclusion include applicability to cyber threat detection, usage of machine learning/deep learning algorithms, and high-quality publications [14]–[17]. Recent publications (from 2021 to 2026) receive preference during the search process.

To facilitate a systematic analysis, this paper proposes a Context-Aware Multi-Layer Review Methodology (CMLRM), which divides all the existing research into three interlinked layers – threat context, learning model, and operating environment. Such an approach allows for examining each particular technique not only in terms of their technical characteristics but also in accordance with their potential use in certain scenarios. For example, intrusion detection algorithms may need to process data in real time, while malware detection may include offline deep learning algorithms [18], [19].

The survey also includes a data-focused analysis strategy to acknowledge the dependency of machine learning techniques on their datasets. Such important features as data freshness, balance of classes, rich set of features, and practical relevance will be considered when evaluating the reliability of datasets. It should be mentioned that there were several works emphasizing the drawbacks of widely used datasets in terms of their generalization ability due to old attacks and insufficient diversity [20], [21].

In addition, the methodology makes use of a two-level assessment model which weighs performance parameters alongside other practical aspects. While performance metrics like accuracy, precision, recall, and F1 score are often considered when assessing how effective a threat detection mechanism is, they do not take into consideration other practical issues. For this reason, this study evaluates the practical aspect of a method using various factors such as computational costs, scalability,

and interpretability among others. It helps gain a clearer insight about the limitations and capabilities of various existing models [22], [23]. Through the combination of context-dependent classification, dataset assessment, and performance and practical evaluation, the methodology presented here provides a way of conducting an extensive analysis of existing cyber threats detection systems.

Component	Description	Key Factors	Purpose
Literature Collection	Selection of relevant studies (2021–2026)	Source quality, relevance	Ensure updated and high-quality review
Context-Aware Classification (CMLRM)	Multi-layer categorization	Threat type, ML model, deployment context	Structured and realistic analysis
Dataset-Centric Evaluation	Assessment of dataset quality	Imbalance, freshness, features	Improve model reliability understanding
Performance Evaluation	Traditional metrics	Accuracy, Precision, Recall, F1-score	Measure detection performance
Practical Evaluation	Real-world constraints	Cost, scalability, interpretability	Ensure deployment feasibility

Table1. Components of the Proposed Review Methodology

The proposed framework begins with Literature Collection, where relevant studies published between 2021 and 2026 are selected based on source quality and research relevance to ensure an updated and high-quality review. Next, the Context-Aware Classification (CMLRM) approach performs multi-layer categorization by considering threat types, machine learning models, and deployment environments for a more structured and realistic analysis. The Dataset-Centric Evaluation phase examines dataset characteristics such as imbalance, freshness, and feature quality to improve understanding of model reliability and robustness. In the Performance Evaluation stage, traditional metrics including Accuracy, Precision, Recall, and F1-score are used to measure the effectiveness of detection models. Finally, the Practical Evaluation phase focuses on real-world constraints such as cost, scalability, and interpretability to ensure the feasibility of practical deployment.

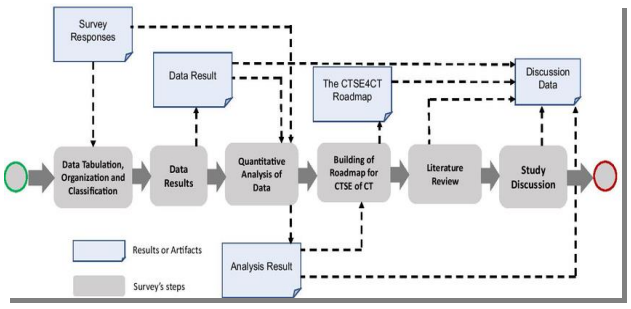

Figure 1. Proposed Workflow of the Survey Methodology

The figure presents a systematic research methodology for developing a roadmap for CTSE of CT. It starts with collecting and organizing survey responses, followed by quantitative data analysis to generate meaningful results. These findings are used to build the CTSE4CT roadmap, which is further supported through literature review and study discussion. The interconnected flow represents continuous feedback and refinement to ensure accurate and reliable research outcomes.

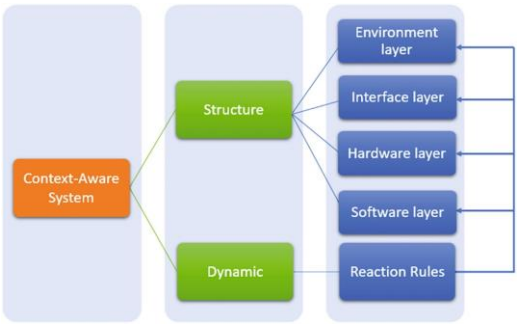

Figure 2 . Context-Aware Multi-Layer Review Methodology (CMLRM)

The figure represents the architecture of a Context-Aware System. The system is divided into two major components: Structure and Dynamic modules. The Structure module manages different operational layers, including the Environment, Interface, Hardware, and Software layers, while the Dynamic module handles Reaction Rules for adaptive responses. Together, these layers enable the system to sense context, process information, and respond intelligently to changing environments.

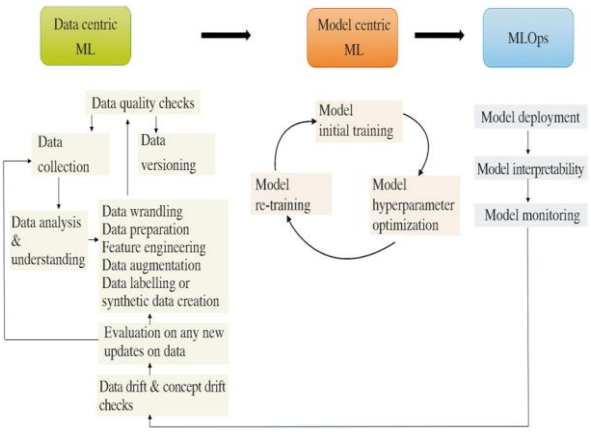

Figure 3. Dataset-Centric Evaluation Model

4. CHALLENGES IN MACHINE LEARNING-BASED CYBER THREAT DETECTION

The implementation of machine learning-based cyber threat detection techniques has yielded many improvements over conventional methods in terms of cybersecurity; however, a number of key challenges persist in their application and performance. These challenges stem from problems in data quality, model development, deployment, and the ever-changing nature of cyber-attacks. To solve them, it is necessary to design a more powerful cyber security mechanism. The first challenge to be faced is a lack of sufficient data patterns, artificially

generated traffic, and low data variety. This has a negative effect on the generalization of quality. Current models are mostly built using public benchmarks like NSL-KDD and CICIDS2017, which have outdated attack trained models in practice [24], [25]. Moreover, due to the dominance of benign data over malicious samples in real datasets, models tend to be heavily biased towards detecting common attack patterns while being incapable of recognizing other classes of attacks.

The other significant challenge is high dimensional space and complexity of features in network data. The cyber security dataset usually consists of many features, most of which may be redundant or unnecessary. This affects the computational complexity and leads to poor model performances. Despite the fact that some methods have already been proposed to tackle the problems of dimension reduction and feature selection, choosing an effective combination of features remains a difficult problem [26]. The use of deep learning approaches poses several problems concerning computational efficiency and scalability. Deep learning models are known to require a significant amount of data and computation resources. Hence, their real-time application becomes impossible in scenarios when resource efficiency plays an important role. Moreover, interpretability still poses a problem since many deep learning models act like black boxes and thus are inappropriate for critical applications [27], [28].

Adversaries may manipulate data input in order to fool models and reduce their effectiveness, posing serious threats to the safety of ML-based solutions. As shown in scientific research, even very accurate models may become subject to such attacks through specially designed inputs [29]. Furthermore, real-time detection imposes certain limitations in terms of the implementation of algorithms for anomaly detection. Most models were tested in an offline environment on static datasets, while in high-speed networks, ML-based methods must provide real-time response, low latency, and high throughput while being resource-efficient. This task is not easy to accomplish simultaneously [30].

Last but not least, privacy considerations lead to the unavailability of real-world datasets necessary for both training and testing ML-based systems. It is hard for organizations to agree to share their private data due to various reasons; hence, there is a need to overcome the lack of suitable datasets. Recent advances in federated learning seek to solve the problem [31].

Table 2: Challenges in ML-Based Cyber Threat Detection Systems

Challenge	Description	Impact on System	Possible Direction
Dataset Quality	incompleteness, noise, and bias	Incomplete model training, false conclusion, less accuracy and reliability	Use data imputation ,implement data cleaning
Model Interpretability	Difficulty in tracing how input features influence	Reduced ability to diagnosed errors or baise	Implement AI technique SHAP,LIME

	prediction		
Adversarial Attack	Evasion attack , poisoning attack, model inversion	Fail to detect malicious activities	Use input sanitization techniques , robot training techniques
Scalability	Computational resources, Real- time processing and model deployment	Increased cost, operational complexity	Optimized model algorithm and implement containerization technologies
Integration with existing system	Compatibility and customization	Conflict and integration issue	Design modular and interoperable systems and tailor model
Compatibilities	Security infrastructure	Conflict occur , integration issue	Compatibility testing
Real-Time Constraints	Delay in detection	Inefficient deployment	Edge computing, optimization
Privacy Issues	Limited data sharing	Insufficient training data	Federated learning

Future Research Directions

The fast pace of emergence of new types of cyber threats due to advanced types of attacks and increased use of digital infrastructure requires constant progress in cyber security approaches based on machine learning techniques. While considerable progress has been made in this area, many avenues are still worth exploring in the future, with a view to making intelligent systems more efficient, resistant to various types of attacks, and applicable in practice. Further development efforts must be focused on the design of adaptive and context-aware intelligent models.

One potential path that can be explored involves the use of explainable artificial intelligence (XAI) within cybersecurity architectures. Since most deep learning models function as black boxes, the inclusion of interpretability measures can help security experts comprehend the decision-making process [32], [33]. Moreover, the use of federated learning or privacy-preserving learning could allow for model training without compromising the confidentiality of sensitive information [34].

Yet another research direction that deserves mention is the development of lightweight and real-time detection algorithms that can

perform well even under conditions of limited computing power, for example, in IoT networks. Although existing deep learning methods deliver excellent results in terms of accuracy, they consume a significant amount of computing power, which makes them unfeasible for deployment in real-time applications. In addition, the use of hybrid learning algorithms that leverage supervised, unsupervised, and reinforcement learning will boost detection accuracy while allowing systems to adapt to known and new threats.

Developing models that are robust to such attacks should also be considered an essential task, given that numerous recent works have proven that current machine learning methods can be easily bypassed by adversarial attacks [35]. Furthermore, the problem of developing large and realistic cybersecurity datasets needs to be addressed. Indeed, existing benchmark datasets do not reflect the diversity and complexity of modern cyber threats, suggesting that there should be more efforts in creating dynamic and large-scale, Finally, incorporating automatic response and self-recovery features should be seen as another important direction for the development of advanced cybersecurity tools. While currently the main objective of machine learning methods is to detect various security threats, the systems of the future should also possess the ability to independently respond to detected threats and self-recover.

V. CONCLUSION

In conclusion, this study presented a comprehensive review of machine learning-based cyber security threat detection techniques developed between 2021 and 2026, with a focus on intelligent, adaptive, and scalable security solutions for modern digital environments. The review demonstrated that significant progress has been achieved through the adoption of advanced deep learning and hybrid models, which provide improved detection accuracy and better handling of complex cyber threats compared to traditional machine learning methods. However, the study also identified several critical challenges, including limited and outdated datasets, high computational complexity, lack of interpretability, and vulnerability to adversarial attacks, which continue to hinder practical deployment in real-world systems.

To address these issues, the proposed Context-Aware Multi-Layer Review Methodology (CMLRM) introduced a structured and systematic framework for analyzing cyber threat detection approaches based on threat context, learning techniques, and deployment conditions. Additionally, the dataset-centric and two-fold evaluation framework provided deeper insight into both detection performance and practical implementation factors such as scalability, efficiency, and interpretability. The findings revealed that although deep learning and hybrid approaches achieve superior accuracy, their real-world applicability remains limited due to resource requirements and explainability concerns. Overall, this study contributes a valuable framework for comparative analysis, identification of research gaps, and guidance for future research toward the development of reliable, efficient, and intelligent cyber security systems.

VI. REFERENCES

[1]. H. Sarker, "Cyber learning: Effectiveness analysis of machine learning security modeling to detect cyber anomalies and multi-attacks," arXiv preprint arXiv, 2021.

[2]. Y. Miao, C. Chen, L. Pan, Q. L. Han, and Y. Xiang, "Machine learning based cyber attacks targeting controlled information: A survey," arXiv preprint arXiv, 2021.

[3]. J. Zhang, L. Pan, Q. L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 3, pp. 377–391, 2022.

[4]. D. Uysal, P. Yoo, and K. Taha, "Data-driven malware detection for 6G networks: A survey," IEEE Open Journal of Vehicular Technology, 2022.

[5]. K. He, D. S. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 538–566, 2023.
[6]. M. Eswaran et al., "Survey of cybersecurity approaches for attack detection and prevention," IEEE Access, 2023.
[7]. M. A. Khan et al., "Unveiling machine learning strategies in intrusion detection systems: A comprehensive survey," Frontiers in Computer Science, 2024.
[8]. "Deep learning for cyber threat detection in IoT networks: A review," Internet of Things and Cyber-Physical Systems, 2024.
[9]. "A survey of large language models for cyber threat detection," Computers & Security, 2024.
[10]. N. S. Musa et al., "Machine learning and deep learning techniques for DDoS detection," IEEE Access, 2024.
[11]. "Advancing cybersecurity: AI-driven detection techniques," Journal of Big Data, 2024–2025.
[12]. "Machine learning and large language models-based techniques for cyber threat detection: A comparative study," in Proc. IEEE Conf., 2024.
[13]. T. Yin et al., "Cyber-attack detection using machine learning and graph neural networks," arXiv preprint arXiv, 2024.
[14]. I. H. Sarker, "Cyber learning: Effectiveness analysis of machine learning security modeling," 2021.
[15]. Y. Miao et al., "Machine learning based cyber attacks: A survey," 2021.
[16]. J. Zhang et al., "Deep learning based attack detection," IEEE, 2022.
[17]. D. Uysal et al., "Data-driven malware detection," IEEE, 2022.
[18]. K. He et al., "Adversarial machine learning in IDS," IEEE, 2023.
[19]. M. Eswaran et al., "Cybersecurity approaches survey," IEEE Access, 2023.
[20]. M. Ring et al., "A survey of intrusion detection datasets," Computers & Security, 2019.
[21]. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. ICISSP, 2018.
[22]. M. A. Khan et al., "ML strategies in IDS," 2024.
[23]. N. S. Musa et al., "ML for DDoS detection," IEEE Access, 2024.
[24]. M. Ring et al., "A survey of intrusion detection datasets," Computers & Security, 2019.
[25]. I. Sharafaldin et al., "CICIDS2017 dataset," in Proc. ICISSP, 2018.
[26]. G. Creech and J. Hu, "Host-based intrusion detection systems," IEEE, 2014.
[27]. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
[28]. M. A. Khan et al., "ML strategies in IDS," 2024.
[29]. B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognition, vol. 84, pp. 317–331, 2018.
[30]. N. S. Musa et al., "DDoS detection using ML," IEEE Access, 2024.
[31]. T. Yin et al., "Federated learning in cybersecurity," 2024.
[32]. M. A. Khan et al., "Machine learning strategies in intrusion detection systems," 2024.
[33]. S. Tjoa and C. Guan, "A survey on explainable AI in cybersecurity," IEEE, 2020.
[34]. Q. Yang et al., "Federated learning: Challenges and applications," ACM Transactions on Intelligent Systems and Technology, 2019.
[35]. N. S. Musa et al., "Machine learning for DDoS detection," IEEE Access, 2024.
[36]. B. Biggio and F. Roli, "Adversarial machine learning," Pattern Recognition, 2018.
[37]. M. Ring et al., "Survey of intrusion detection datasets," 2019.
[38]. "Survey data analysis," ResearchGate.
[39]. Elsevier figure resource, "Cybersecurity architecture illustration," 2021.
[40]. ScienceDirect, "Cybersecurity and machine learning framework," 2023.
[41]. "Challenges in Applying ML to Cybersecurity," ResearchGate, 2024.

Conflict of Interest Statement: *The author declares that there is no conflict of interest regarding the publication of this paper.*

Generative AI Statement: *The author confirm that no Generative AI tools were used in the preparation or writing of this article.*

Publishers Note: *All statements made in this article are the sole responsibility of the authors and do not necessarily reflect the views of their affiliated institutions, the publisher, editors, or reviewers. Any products mentioned or claims made by manufacturers are not guaranteed or endorsed by the publisher.*

Cite this Article

Yogita Mishra. A Survey on Machine Learning – Based Cyber Threat Detection System. International Research Journal of Engineering & Applied Sciences (IRJEAS). 14(2), pp. 10-21, 2026. https://doi.org/10.55083/irjeas.2026.v14i02002