International Journal of Cyber Threat Intelligence and Secure Networking (IJCTISN)
eISSN: 3087-4297
Volume03 Issue09 | Page No: - 14-22

Received: 23 July 2026, Revised: 30 July 2026, Accepted: 25 August 2026, Published: 03 September 2026

DOI: https://doi.org/10.55640/ijctisn-v03i09-03

A Review of Machine Learning Techniques for Network Intrusion Detection Systems

Mr. Madhav Sharma [1]

[1] Assistant Professor Department of Computer Science and Applications Mandsaur (M.P.)

ABSTRACT: Security researchers rely heavily on Network Intrusion Detection Systems (NIDS) to keep an eye on network traffic and notify administrators of any suspicious activities. The purpose of this paper is to offer a comprehensive overview of intrusion detection systems (IDS), including the following topics: fundamentals, kinds of IDS, methods for detecting intrusions in NIDS, the architecture of IDS, data pre-processing, and examples of ML techniques used in NIDS. This covers several detection methods, including signature-based, anomaly-based, specification-based, and behavior-based approaches, as well as their advantages and disadvantages in recognizing both existing and new cyber threats. The review also covers the architecture of NIDS which consists of network sensors, preprocessors, network traffic analysis, alert generation and security analysis. A variety of ML techniques, including supervised, unsupervised, semi-supervised, ensemble, and deep learning (DL) approaches, are being explored to improve the accuracy and adaptability of intrusion detection systems (IDS). Other applications such as DoS/DDoS attack detection, Malware detection, Botnets, Brute force attacks, Insider compromise, IoT compromise and Critical infrastructure threats are also shown. Despite all the challenges in terms of false positives, scalability, computational complexity, data quality, and novel attack styles, the features that ML can provide for intelligent, adaptive, and accurate intrusion detection systems are appealing.

KEYWORDS: Network Intrusion Detection Systems, Machine Learning, Deep Learning, Cybersecurity, Anomaly Detection, Network Security.

1. Introduction

Network security has become an essential field of research due to the internet's and other communication technologies' explosive expansion over the past ten years [1]. Online data and networks may be protected by using cybersecurity measures such as intrusion detection systems (IDS), antivirus software, and firewalls [2]. To ensure the necessary level of protection, a network-based intrusion detection system (NIDS) is utilized [3]. It does so by continuously tracking what is taking place on the network for malicious and suspicious activity. However, the false alarm rate in many IDSs remains high, producing numerous false alarms for relatively benign events, making security analysts' work more difficult and sometimes causing important events to be ignored [4]. With that in mind, a lot of effort has gone into creating IDSs that are more accurate and have lower false alert rates. The inability of current IDSs to identify unknown threats is another issue with them. Due to the dynamic nature of network infrastructures, new and different types of assaults are always appearing. Must thus create IDS capable of detecting previously unseen threats. Security components such as IDS and firewalls work together to protect networks from a wide range of threats. Machine learning (ML) is utilized by two primary types of intrusion detection systems (IDS): those that identify anomalies and those that detect misuse [5]. Systems based on signatures, which depend on multi-classification, are vital for abuse detection since they can identify malicious attacks and destructive acts. Their inability to detect new attacks without an existing IDS signature is a major drawback.

ML has recently emerged as the leading method in computer vision, both in academia and business. It is both popular and challenging. In the fields of medicine, economics, security, data management, trend forecasting, and analysis, it is now the most popular area for scientific innovation. ML is based on the idea of teaching computers to learn from their own data and make judgments on their own, without any human input. Among the many forms of AI, ML is most known for its ability to simulate human intellect via the incorporation of past data and instruction [6]. In order to evaluate data

and identify trends, it uses minimum human interaction. Many facets of society are impacted by ML. These include food production, transportation, education, healthcare, and healthcare systems[7]. A lot of things are changing because of ML, including the way live and work, the things buy, and even the food sector [8][9]. ML and computer vision work toward the same aim of giving computers the capacity to learn from their experiences and make judgments using that knowledge. The IoT, the Industrial Internet of Things, and cognitive interactions with humans all rely on computer vision [10]. Complex human activities in multimedia streams may be identified and tracked using computer vision and ML techniques [11].

A. Structure of the paper

The following is the paper's structure: The kinds, architecture, foundations, and methods of NIDS are covered in Section II. Section III delves into the methods and uses of ML in NIDS. Section IV presents related literature, comparative analysis, and research gaps. Section V concludes the analysis and emphasizes areas for further investigation.

II. FUNDAMENTALS OF NETWORK INTRUSION DETECTION SYSTEMS

A NIDS is a vital cybersecurity tool used to detect suspicious or malicious behavior in network traffic. They watch for suspicious activity in data packets and sound alarms if they find anything out of the ordinary[12]. NIDS employ signature-based, anomaly-based, or hybrid detection methods to ward against network attacks. IDS analyze network events to identify intrusions [13]. There are two primary types of IDS that are now in use: network-based (NIDS) and host-based (HIDS). NIDS targets various network activity in order to identify intrusions, whereas host-based (HIDS) targets individual hosts. Since NIDS can keep tabs on more network targets, it is able to catch additional attacks that HIDSs could miss since they can't view packet headers. This is because NIDSs monitor the output of packet sniffers. When it comes to IP-based DoS attacks, for example, NIDS can catch a lot of them since they watch the packet headers as they go across the network [14]. In addition, NIDS doesn't depend on the host OS to detect threats; it's specifically built to work with specific OSes. In order to detect intrusions, certain hybrid IDS use both HIDS and NIDS.

- Network-Based IDS (NIDS): The network-level operation involves constant packet analysis to detect malicious activities. Deploying these devices at key nodes in the network architecture, including gateways or intersubnets, allows for full insight into traffic flows [15]. Multiple threats, including malware propagation, port scanning, and DoS assaults, may be identified by NIDSs using methods like DPI and flow analysis.

- Host-Based IDS (HIDS): Monitors specific targets, like servers, PCs, or virtual machines, by keeping an eye on activities at the system level. This entails keeping an eye on things like system calls, file system updates, process activity, and log files. Unauthorized access attempts, malware execution, and privilege escalation are all host-specific risks that a HIDS excels at identifying [16]. The capacity to identify local threats that may avoid detection by network-level monitoring is a key benefit of HIDSs. A simplified diagram of the HIDS idea is shown in Figure 1.

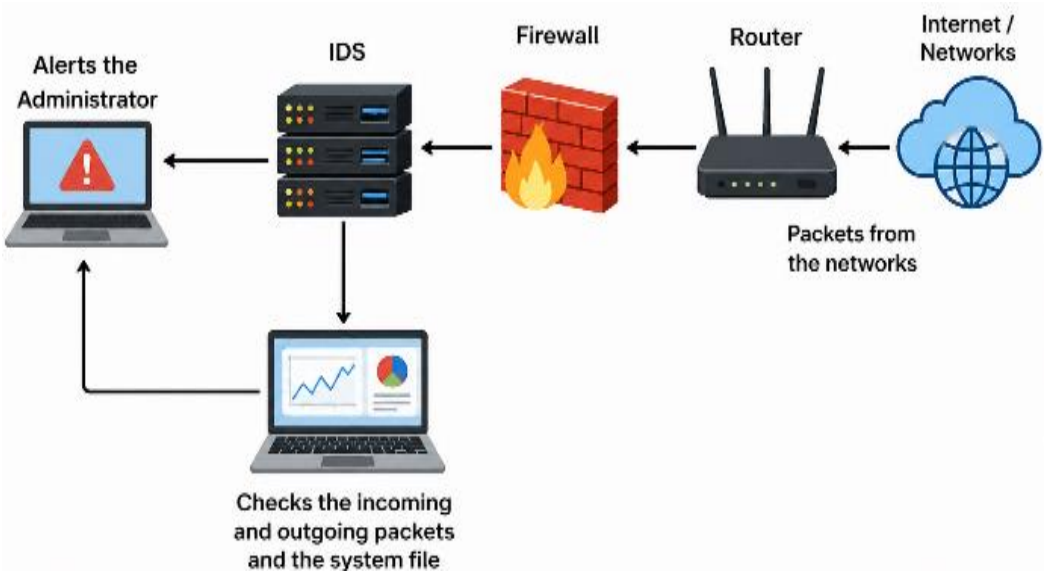

Fig. 1. Schematic representation of the HIDS concept

- Hybrid IDS: This security solution is designed to be integrated with NIDSs and HIDSs, making it more comprehensive. These systems take advantage of the best of both worlds, tracking both traffic and host activity. Hybrid IDSs can deliver higher ACC in detecting threats and lower FPR [17] by combining data from multiple sources. One of the benefits of hybrid IDSs is that they offer context awareness. Better detection of

multi-stage assaults, like APTs, is possible, for instance, since the NIDS may link suspicious host behavior with network anomalies.

1) Intrusion Detection Approaches

Network Intrusion Detection Approaches are the ways NIDS can detect intrusion or unauthorized activities in network traffic [18]. There are three main ways to detect cyber threats: signature-based, anomaly-based, and behavior-based. Each of these approaches has its own advantages and disadvantages in terms of recognizing new and old cyber threats, as summarized in Table I.

- Signature-Based Detection: These IDSs depend on the pattern-like characteristics or "signatures" of attacks that have already happened. The concept of these systems is to compare the observed to a collection of signatures, for instance a single sequence of bytes, a list of known hashes for malware (such as those seen in Figure 2) or unusual command sequences. The signature-based detection method is best for detecting known threats, and it has a low false-positive rate [19]. Intrusion detection systems that are signature-based have trouble identifying new or potentially malicious attacks.

- Anomaly-Based Detection: These baselines can be statistical models, ML algorithms or heuristic methods. The ability of anomaly-based intrusion detection systems to identify new threats makes them well-suited to a threat landscape where threats are constantly changing, in contrast to signature-based systems [20]. There are, however, difficulties in relying on behavioral baselines, as demonstrated in Figure 2, especially in a highly variable environment. It can be hard to define normal behavior in such systems, making it more likely that have false positives.

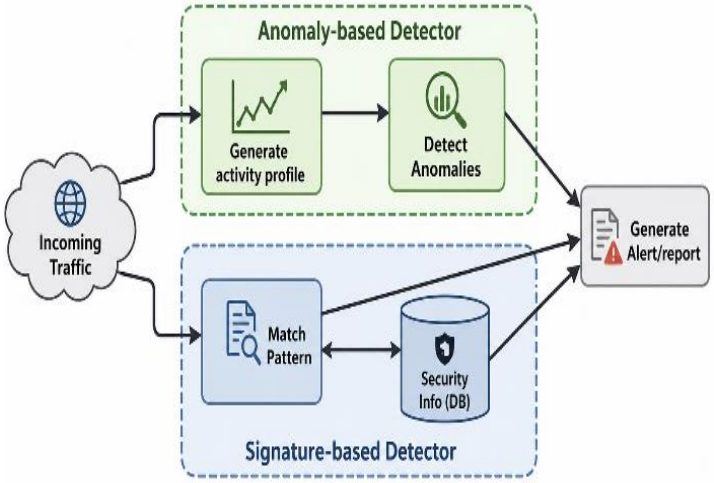

Fig. 2. Schematic representation of both the anomaly-based and signature-based IDS concepts

- Specification-based IDS: The hybrid method of specification-based intrusion detection systems is both predictable, like rule-based systems, and flexible, like anomaly detection systems [21]. These systems are based on a set of expected behaviors that are typically defined by hand by experts and used to detect deviations that are considered suspicious. In controlled contexts with well-defined operating parameters, such as in ICS or IoT networks, this method is very successful and delivers better accuracy than anomaly-based systems alone.

- Behavior-Based Detection: Behavior-based detection is deeper and more specific in analyzing the nature of the activities observed and the intent of users, applications, or devices, identifying if the series of activities they have performed is consistent with known malicious actions. The ability to identify sophisticated malware, insider threats, and multi-phase attacks is a major strength of this approach. In this procedure, known as behavior profiling, the system keeps track of user actions over time in order to create comprehensive models of typical and out-of-the-ordinary actions [22]. Anomaly detection, which is the other type, looks for significant variations from statistical norms, whereas behavior-based detection does so based on the sequence and context of activity.

TABLE I. COMPARISON OF DIFFERENT IDS TYPES AND THEIR TYPICAL APPLICATIONS, ADVANTAGES, AND DISADVANTAGES

Type of IDS	Main Techniques	Typical Applications	Advantages	Disadvantages
NIDS [23]	DPI, flow analysis	Distributed infrastructures, enterprise networks	Suitable for big networks, it monitors several devices at once.	Problems arise while dealing with encrypted data and performance drops when traffic is heavy.
HIDS	System log monitoring and process behavior	Virtual machines, endpoints, and servers	Identifies risks that are particular to hosts; works well with encrypted endpoints	Scalability issues in big environments; unable to detect assaults on the whole network

Hybrid IDS	Merging NIDS with HIDS	Comprehensive safety in intricate networks	Reduces the number of false positives while increasing the accuracy of diagnosis	Extremely difficult; demands a large amount of computer power
Signature-based	Comparison of databases that contain threat signatures	Common malware prevention measures, conventional networks	Very few false positives; very high accuracy for known dangers	Ineffective against constantly changing threats; regular upgrades are necessary
Anomaly-based	Monitoring for changes from typical patterns of conduct	Emerging landscapes such as cloud and IoT	Apt for zero-day attacks and able to identify unexpected threats	Excessive false positives; heavy-duty infrastructure needed
Specification-based	Detection based on predefined specifications of expected behavior	Industrial systems, IoT	Ideal for ICS or the IoTs; achieves better accuracy in regulated environments	Manually defining criteria; restricted adaptability
Behavior-based [24]	Behavior profiling, action correlation	Essential infrastructure, banking, medical care	Finds sophisticated assaults and insider dangers	Demands a lot of processing power; difficult to keep up with

2) The Architecture of an IDS

This section introduces the general architecture of an IDS and describes the relationship between the basic components. The architecture has been established to provide a systematic way of collecting network traffic, pre-processing data, detection of potential threats using various detection techniques, alerts, and security analysis. In order to improve cybersecurity as a whole, an IDS can keep an eye on a network around the clock, identify assaults as they happen, and help with decision-making. Figure 3 illustrates the overall IDS architecture, showing the workflow from network traffic monitoring to threat detection, alert generation, reporting, and security analysis. Multiple interdependent parts make up IDS, which together keep an eye out for, assess, and counteract any security risks.

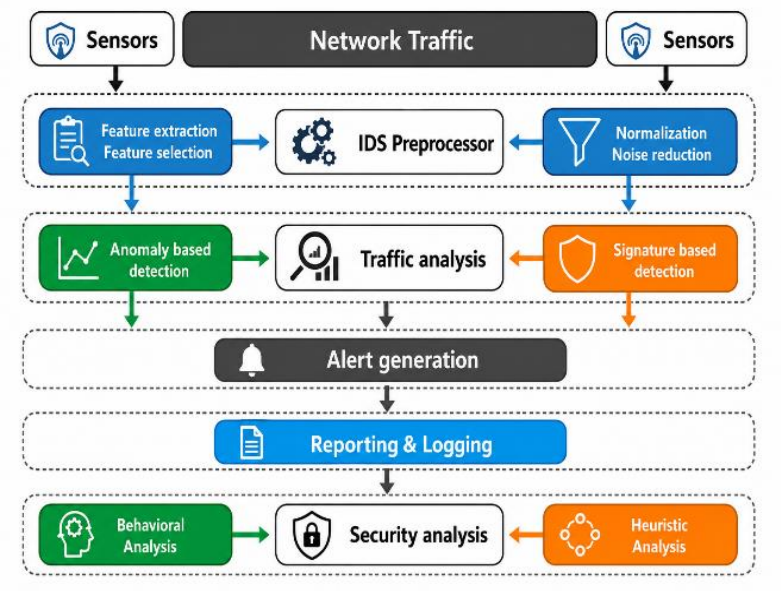

Fig. 3. The Architecture of an IDS

- Network sensors: All data and packets traveling via a network, both incoming and outgoing, are constantly being tracked by network sensors. As data packets travel over the network, they collect their raw data. The preprocessor receives the raw data that has been gathered [25]. Data normalization and preparation for detection engine analysis are both performed by the preprocessing.

- IDS Preprocessor: Errors, duplicates, or missing numbers, as well as background noise, are common in raw data. The initial network data is prepared for additional analysis by preprocessing. After processing, the data is normalized to make it appropriate for further processing and to ensure consistency. The first step is data extraction. Among the details that must be identified are the IP addresses of the sending and receiving devices, the ports they use, and anything else that might be relevant [26].

- Alert generator: The alert generator takes in warnings from engines that match anomalies and signatures, and then sorts them according to how serious they are. Alerts are designed to be easily understood by humans. Not only that, but the alert generator records all the pertinent details of the occurrences it detects. Time stamps, source and destination IP addresses, port numbers, and the identified type of attack are all part of these warnings [27].

- Security analysts: Analyzing the IDS alarms for false positives and negatives is the job of the security analysts. Valid judgments and actions, including halting network traffic, are based on their analyses [28].

- Traffic analysis: Traffic analysis examines network

packets and flow patterns to identify abnormal or malicious activities. It helps detect suspicious communication, unusual traffic behavior, and potential cyberattacks by analyzing network protocols, packet characteristics, and traffic patterns.

III. APPLICATIONS OF MACHINE LEARNING AND TECHNIQUES FOR NIDS

ML is widely applied in NIDS to detect and classify diverse cyber threats, including DoS/DDoS attacks, malware, botnets, network scanning, brute-force attacks, and insider threats[29]. In addition to enhancing intrusion detection in critical infrastructure, wireless networks, the IoT, and MANETs, ML allows for the automatic, adaptive, and accurate identification of unlawful network activity.

- DoS (Denial-of-Service) attacks: This occurs when a system is unable to handle a reasonable amount of requests because it is overwhelmed by a large volume of requests. This kind of attack can take advantage of security holes in software or protocols used by networks, or it can simply flood a target with requests until it crashes.

- IoT Network Intrusion Detection Systems: The data sent and received by various internet-connected devices in an IoT system. Protecting the network from outsiders and hostile assaults, it serves as a first line of protection. Today's computer network systems rely on NIDS as their main defense against network intrusion and other forms of assault. In order to detect both known and undiscovered harmful assaults on a network, NIDS monitors and studies the network and user activities of the hosted device.

- Insider Threat Models: Insider threats arise from authorized users who misuse their access privileges, either intentionally or unintentionally. ML-based NIDS uses classification and anomaly detection algorithms to examine network traffic and user behavior. This allows for the early identification of hostile insider actions while lowering false alarms [30].

- Brute-force attacks: One common sort of network attack is a brute-force attack, which can impact any device connected to a computer network. As a result of their propensity to be utilized for data exploitation or malicious software installation, brute-force assaults are notoriously dangerous to web applications [31]. A successful breach can allow the installation of numerous malicious programs, such as Web shells, which can raise the demand on the fundamental infrastructure as a result.

- Malware Detection Methods: There are essentially many ways to classify malware detection systems from different perspectives. If there are three types of malware detection methodologies, then this survey article falls under one of them [32]. This encompasses methods that utilize DL and recurrent and convolutional neural networks.

A. Machine Learning Techniques for Network Intrusion Detection

ML is now an important part of making intelligent NIDS. Automatically detecting malicious activity, these systems discover patterns in network data. Methods for intrusion detection range from supervised to unsupervised to semi-supervised to ensemble learning to DL. These techniques improve attack classification, anomaly detection, adaptability, and overall detection performance while supporting the identification of evolving and previously unseen cyber threats.

1) Supervised Machine Learning

Training models that can differentiate between safe and malicious activities in network traffic using labeled data is the main objective of supervised ML. It greatly improves the accuracy of intrusion detection and is very good at identifying patterns of known attacks [33].

2) Unsupervised Machine Learning

Unsupervised ML seeks for patterns and outliers in unlabeled network data. It is good for detecting undetected and undiscovered cyberattacks, since it does not require labeled datasets.

3) Semi-Supervised Machine Learning

Semi-supervised ML improves detection performance by utilizing a smaller quantity of labeled data in conjunction with a greater quantity of unlabeled data. It is helpful if there are not many or expensive labeled intrusion datasets.

4) Ensemble Learning

Ensemble learning is a method that improves detection accuracy, robustness, and generalization by combining numerous ML models. Several methods, including RF, Boosting, and Bagging, have been developed to enhance a NIDS's capacity to detect intrusions while minimizing the number of false alarms.

5) Deep Learning(DL) Algorithms

DL is a specific form of AI that can identify complex features from network traffic data automatically using multiple layers of NNs. Successfully detects sophisticated and emerging threats in cyber and provides high intrusion detection performance.

IV. LITERATURE OF REVIEW

A brief overview of the latest studies and research on using ML techniques for network intrusion detection,

incorporating algorithms, adaptive learning strategies, explainable AI techniques, and performance comparisons to improve detection accuracy, resilience, and real-time cybersecurity.

S. A. Moon, et al. (2026) introduces adaptive and explainable ML framework for real-time network intrusion detection combining XGBoost, CIL and LIME. When it comes to identifying massive amounts of high-dimensional network traffic, the XGBoost engine has shown to be both accurate and efficient. Class incremental learning is another feature of the system that allows it to adapt to previously unforeseen attack types without retraining the model or losing any previously learned information [34].

R. Rehyadd and P. Agarwal (2025) The comparison of ML and DL methods for network intrusion detection using benchmark datasets such as NSL-KDD, UNSW-NB15, CIDDS-001, and CIDDS-002. The evaluation included a number of models, such as CNN, LSTM (with embedding), ML (CART, KNN, XGBoost), and DL options. In order to evaluate the ACC, PRE, REC, and F1, several crucial performance indicators were examined. In comparison to more complicated DL models, CART consistently obtained better ACC with a shorter training time on both datasets [35].

S. Hiremath, et al. (2025) using several ML models trained on the CICIDS2018 dataset, a thorough investigation of intrusion detection has been carried out. There is no DL architecture that hasn't been attempted, from the most basic to the most complex. RF is ideal for classifiers due to its top-notch performance metrics, which include an F1 of 99.79%, ACC of 99.79%, and REC of 99.81%. Furthermore, this research suggests a real-time IDS/IPS that utilizes the Cyclometer dataset in conjunction with an RF classifier that has been trained on data acquired from the Cyclometer data collection tool [36].

R. S. Valasev, et al. (2024) offer a thorough evaluation of the network intrusion detection capabilities of conventional ML algorithms and contemporary DL approaches using the latest CICIDS-2018 dataset. The ML classifiers employed are KNN, LR, RF, and SVM, and compared with a hybrid DL model, CNN and GRU. The results of the research show that the ML algorithms, while having low computational complexity and being easily interpretable, outperform the hybrid CNN-GRU model with the ability to recognize complex and hidden patterns related to intrusive activities, high detection accuracy and high resistance to overfitting [37].

B. Li et al. (2024) investigated ML methods for NIDS in a simulated power load management system at length. A set of data was used in this research that was formulated to mimic an actual power load management system that has been attacked in various manners. Three ML models were employed to analyze the dataset: KNN, LR, and RF. These models were trained to identify normal and anomalous connections in the dataset. Several anomaly detection models were compared using F1, REC, ACC, and precision in this setting. The study lays a solid foundation for strengthening the safety of networks that house power load management systems [38].

K. Hemavathi and R. Latha (2023) CGAN-OMLIDS is an ideal ML-based intrusion detection system coupled with a conditional generative adversarial network. The CGAN-OMLIDS approach has two primary goals: the class imbalance data problem and intrusion detection. This is done at the start of the given CGAN-OMLIDS method by using Z-score normalization. Also, for dealing with issues of class imbalance, the CGAN-OMLIDS strategy makes use of the CGAN method. Also, the classification and intrusion detection mechanisms are based on ELM method. Besides, the ELM approach's parameter tuning is achieved by the LOA [39].

M. Bommy, et al. (2023) delve more into the potential of ML for MANET intrusion detection. Put a few of ML models to work detecting harmful network traffic. The models can be RF, MLP, NNs, SVM, etc. According to the results, the MLP Neural Network has many benefits, including increased ACC and adaptability. Using an RL-based adaptive learning method, the model should be able to quickly adjust to the changing network circumstances in order to enhance real-time intrusion detection [40].

The recent ML techniques used in network intrusion detection are summarized in Table II, where approaches, important results, problems, and future research directions are described.

TABLE II. MACHINE LEARNING TECHNIQUES FOR NETWORK INTRUSION DETECTION SYSTEMS

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
S. A. Moon et al. (2026)	Adaptive and explainable real-time NIDS	XGBoost, CIL, and LIME	High detection efficiency with continuous adaptation to new attack types and explainable predictions	Concept drift and continuous adaptation	Develop more robust adaptive models for evolving and zero-day attacks
R. Rehyadd and P.	ML and DL-based network	CART, KNN, XGBoost,	CART achieved high accuracy with lower	Dataset dependency and computational	Evaluate lightweight and scalable models

Agarwal (2025)	intrusion detection	CNN, and LSTM	training time than complex DL models	complexity of DL models	on diverse real-world datasets
S. Hiremath et al. (2025)	ML-based intrusion detection	15 ML/DL models and Random Forest with CICFlowMeter	Random Forest achieved 99.79% F1-score, 99.79% precision, and 99.81% recall	Limited evaluation across datasets and evolving attacks	Improve real-time detection and validate across heterogeneous network environments
R. S. Valasev et al. (2024)	Comparative ML and DL-based NIDS	KNN, LR, RF, SVM, and CNN-GRU	CNN-GRU achieved superior detection of complex intrusion patterns	Higher computational requirements and lower interpretability of DL	Develop explainable and computationally efficient hybrid models
B. Li et al. (2024)	Intrusion detection in power load management systems	Logistic Regression, Random Forest, and KNN	ML techniques effectively detected anomalous network connections	Simulated environment and limited model diversity	Test advanced ML methods in real-world critical infrastructure networks
K. Hemavathi and R. Latha (2023)	Class-imbalanced intrusion detection	CGAN, ELM, Z-score normalization, and LOA	CGAN addressed class imbalance, while LOA optimized ELM parameters	Imbalanced data and optimization complexity	Develop robust models for highly imbalanced and evolving attack data

V. CONCLUSION AND FUTURE WORK

AI has been an effective weapon in the battle against network threats, especially in the area of NIDS improvement. When it comes to automated traffic analysis and the identification of harmful behavior, AI has shown to be a formidable ally in the field of network intrusion detection. In this review the basic concept of the NIDS was reviewed, followed by the various intrusion detection techniques, data pre-processing techniques and ML techniques in network security. Signature-based methods still work for known attacks while anomaly- and behavior-based methods give more capabilities to detect unknown and evolving threats. DTs, KNN, and ANN are well suited to classification tasks, and RNN, DNN, and CNN are well suited for learning complex patterns from network data. The ML-based applications of the NIDS are used for identifying DoS/DDoS attacks, Malware detection, Botnets, Brute force attack, Intrusion in IoT and Critical Infrastructure. Data quality and class imbalance are still issues, as well as computational complexity, overfitting and adaptability. In conclusion, intelligent and adaptive ML-based NIDS solutions play a pivotal role in enhancing network security in the ever-evolving landscape of cyber threats.

Further research is required to develop adaptive lightweight ML-based NIDS with real-time capability of detecting zero-day and evolving attacks. Future research will also explore Hybrid ML-DL models, Explainable AI, Federated Learning, Secure feature selection, and real-world datasets, to enhance the scalability, privacy, explainability, and generalization of ML in various network contexts.

References

1. S. Kumar, P. Pathak, K. Agrawal, V. Goswami, and A. Mahindru, "Network Intrusion Detection System Using Machine Learning," Lect. Notes Networks Syst., vol. 730 LNNS, pp. 735–743, 2023, doi: 10.1007/978-981-99-3963-3_56.
2. S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in 2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.
3. Y. Muni, "Advanced Multi-Protocol Label Switching (MPLS)-Enabled Networks: A Survey of Emerging Approaches Via Traffic Engineering," Eng. Technol. J., vol. 11, no. 01, Jan. 2026, doi: 10.47191/etj/v11i01.22.
4. H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," Appl. Sci., vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.
5. D. Moon, S. B. Pan, and I. Kim, "Host-based intrusion detection system for secure human-centric computing," J. Supercomput., vol. 72, no. 7, pp. 2520–2536, 2016, doi: 10.1007/s11227-015-1506-9.
6. S. S. Dash, S. K. Nayak, and D. Mishra, "A review on machine learning algorithms," Smart Innov. Syst. Technol., vol. 153, pp. 495–507, 2021, doi: 10.1007/978-981-15-6202-0_51.
7. K. K. Mohammed, "A Survey on Digital Health Care Data Analysis Techniques for Developing Machine Learning Models," Int. J. Sci. Eng. Technol., vol. 13, no. 5, October, pp. 1–6, 2025, doi:

:10.5281/zenodo.17339813.

8. S. Sah, “Machine Learning: A Review of Learning Types,” Neural Networks 152, vol. 7, no. 1, pp. 267–275, 2020, doi: 10.20944/preprints202007.0230.v1.

9. A. V. S. R. Dantuluri, “A Scalable Deep Learning Analytics Pipeline for Converting Longitudinal Real-World Data Into Predictive Disease Trajectories,” IEEE Access, vol. 14, pp. 24871–24878, 2026, doi: 10.1109/ACCESS.2026.3663571.

10. A. Joon, “Smart Predictive Maintenance: AI-Driven Adaptation for Industrial Equipment,” in 2025 IEEE North-East India International Energy Conversion Conference and Exhibition (NE-IECCE), IEEE, Jul. 2025, pp. 1–6. doi: 10.1109/NE-IECCE64154.2025.11183108.

11. L. Cheng and T. Yu, “A new generation of AI: A review and perspective on machine learning technologies applied to smart energy and electric power systems,” Int. J. Energy Res., vol. 43, no. 6, pp. 1928–1973, May 2019, doi: 10.1002/er.4333.

12. L. A. Yeruva, D. Singh, S. Suddala, N. Bhatt, and R. Uddin, “Augmented Data Management for Cache Performance, Cybersecurity, and Mobile Integration,” J. Comput. Mech. Manag., vol. 5, no. 3, pp. 280–293, June, Jun. 2026, doi: 10.57159/jcmm.5.3.26691.

13. A. Joon, B. K. R. Janumpally, A. Gogineni, and P. Chatterjee, “Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence,” in 2025 5th International Conference on Intelligent Technologies (CONIT), IEEE, Jun. 2025, pp. 1–8. doi: 10.1109/CONIT65521.2025.11167760.

14. M. Aljanabi, M. A. Ismail, R. Hasan, and J. Sulaiman, “Intrusion Detection: A Review,” Mesopotamian J. Cyber Secur., vol. 2021, pp. 1–4, 2021, doi: 10.58496/MJCS/2021/001.

15. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “A survey of network-based intrusion detection data sets,” Comput. Secur., vol. 86, pp. 147–167, Sep. 2019, doi: 10.1016/j.cose.2019.06.005.

16. H. Satilmiş, S. Akleylek, and Z. Y. Tok, “A Systematic Literature Review on Host-Based Intrusion Detection Systems,” IEEE Access, vol. 12, pp. 27237–27266, 2024, doi: 10.1109/ACCESS.2024.3367004.

17. S. Remya, M. J. Pillai, C. Arjun, S. Ramasubbareddy, and Y. Cho, “Enhancing Security in LLNs Using a Hybrid Trust-Based Intrusion Detection System for RPL,” IEEE Access, vol. 12, pp. 58836–58850, 2024, doi: 10.1109/ACCESS.2024.3391918.

18. V. Rohilla, K. Rohilla, P. Kumar, and N. Jain, “Intrusion Detection in Network Traffic Using Feature Selection and Optuna-Based Machine Learning Optimization,” in 2026 3rd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), IEEE, Apr. 2026, pp. 1–6. doi: 10.1109/RMKMATE69073.2026.11518834.

19. H. Y. Kwon, T. Kim, and M. K. Lee, “Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods,” Electron., vol. 11, no. 6, pp. 1–19, 2022, doi: 10.3390/electronics11060867.

20. B. Al-Fuhaidi, Z. Farae, F. Al-Fahaidy, G. Nagi, A. Ghallab, and A. Alameri, “Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms,” Appl. Comput. Intell. Soft Comput., vol. 2024, no. 1, p. 2625922, Jan. 2024, doi: 10.1155/2024/2625922.

21. E. Hotellier, F. Sicard, J. Francq, and S. Mocanu, “Standard specification-based intrusion detection for hierarchical industrial control systems,” Inf. Sci. (Ny)., vol. 659, p. 120102, Feb. 2024, doi: 10.1016/j.ins.2024.120102.

22. C. Wang and H. Zhu, “Wrongdoing Monitor: A Graph-Based Behavioral Anomaly Detection in Cyber Security,” IEEE Trans. Inf. Forensics Secur., vol. 17, pp. 2703–2718, 2022, doi: 10.1109/TIFS.2022.3191493.

23. L. Diana, P. Dini, and D. Paolini, “Overview on Intrusion Detection Systems for Computers Networking Security,” 2025. doi: 10.3390/computers14030087.

24. A. Shamekhi, P. Shamsinejad Babaki, and R. Javidan, “An intelligent behavioral-based DDOS attack detection method using adaptive time intervals,” Peer-to-Peer Netw. Appl., vol. 17, no. 4, pp. 2185–2204, 2024, doi: 10.1007/s12083-024-01690-2.

25. Y. Hamid, S. Muthukumarasamy, and L. Journaux, “Machine Learning Techniques for Intrusion Detection: A Comparative Analysis,” 2016, pp. 1–6. doi: 10.1145/2980258.2980378.

26. M. Ozkan-Okay, R. Samet, Ö. Aslan, and D. Gupta, “A Comprehensive Systematic Literature Review on Intrusion Detection Systems,” IEEE Access, vol. 9, pp. 157727–157760, 2021, doi:

10.1109/ACCESS.2021.3129336.

27. B. E. Ricks, “Intrusion detection systems,” Phys. Secur. Saf. A F. Guid. Pract., no. 9, pp. 101–108, 2014, doi: 10.48175/ijarsct-17606.

28. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” Cybersecurity, vol. 2, 2019, doi: 10.1186/s42400-019-0038-7.

29. P. Kumar, “A Zero Trust-Based Approach to Modern Cybersecurity Challenges in Software Development,” Int. J. Emerg. Res. Eng. Technol., vol. 6, no. 9, pp. 113–122, September, 2025.

30. B. Bin Sarhan and N. Altwaijry, “Insider Threat Detection Using Machine Learning Approach,” Appl. Sci., vol. 13, no. 1, p. 259, Dec. 2022, doi: 10.3390/app13010259.

31. M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, “Machine Learning for Detecting Brute Force Attacks at the Network Level,” in 2014 IEEE International Conference on Bioinformatics and Bioengineering, IEEE, Nov. 2014, pp. 379–385. doi: 10.1109/BIBE.2014.73.

32. J. M. Waghmare and M. M. Chitmogrekar, “A Review on Malware Detection Methods,” SAMRIDDHI A J. Phys. Sci. Eng. Technol., vol. 14, no. 01, pp. 38–43, 2022, doi: 10.18090/samriddhi.v14i01.6.

33. T. D. Adugna, A. Ramu, and A. Haldorai, A Review of Pattern Recognition and Machine Learning, vol. 4, no. 1. 2024. doi: 10.53759/7669/jmc202404020.

34. S. A. Moon, B. Maram, B. V Srinivasulu, and P. V. K. Reddy, “A Live Network Attack Detection System Employing Self-Adjusting and Interpretable Machine Learning Techniques,” in 2026 4th International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), IEEE, May 2026, pp. 1177–1182. doi: 10.1109/ICSSAS68835.2026.11559485.

35. R. Rehyadd and P. Agarwal, “Performance Comparison of Machine Learning and Deep Learning Techniques for Detecting Network Intrusions,” in 2025 International Conference on Next Generation of Green Information and Emerging Technologies (GIET), IEEE, Aug. 2025, pp. 1–7. doi: 10.1109/GIET65294.2025.11234882.

36. S. Hiremath, R. D B, S. Singh, S. S V, and R. K R, “Machine Learning Models for Intrusion Detection System,” in 2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT), IEEE, Mar. 2025, pp. 235–238. doi: 10.1109/CSNT64827.2025.10967597.

37. R. S. Valasev, A. R. Priambodo, and R. N. Esti Anggraini, “Evaluating Contemporary Machine Learning and Deep Learning Strategies for Intrusion Detection,” in 2024 IEEE International Conference on Control & Automation, Electronics, Robotics, Internet of Things, and Artificial Intelligence (CERIA), IEEE, Oct. 2024, pp. 1–5. doi: 10.1109/CERIA64726.2024.10915015.

38. B. Li et al., “Enhancing Network Security: Machine Learning Evaluation for Intrusion Detection in Power Load Management System,” in 2024 5th International Conference on Information Science, Parallel and Distributed Systems (ISPDS), IEEE, May 2024, pp. 708–712. doi: 10.1109/ISPDS62779.2024.10667483.

39. K. Hemavathi and R. Latha, “Conditional Generative Adversarial Network with Optimal Machine Learning Based Intrusion Detection System,” in 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), IEEE, Nov. 2023, pp. 1176–1182. doi: 10.1109/ICSCNA58489.2023.10370325.

40. M. Bommy, T. Vivekanandan, Y. Sreeraman, D. Jagadeesan, C. Sunil Kumar, and G. Asha, “Mobile Ad Hoc Networks Supporting Adaptive Threat Detection through Intrusion Detection Effective Use of Machine Learning for Cyber Defense,” in 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), IEEE, Dec. 2023, pp. 1–5. doi: 10.1109/ICSES60034.2023.10465320.