


# Network security analysis using machine learning-based intrusion detection system methods

Arief Sutarjo<sup>1</sup>, Helmy Fahlephi<sup>2</sup>

<sup>1,2</sup> Faculty of Engineering, Information Technology Universitas Medan Area, Medan, Indonesia.

ARTICLE INFO	ABSTRACT
<p><b>Article history:</b></p> <p>Received: 03 April, 2025 Revised: 11 April, 2025 Accepted: 28 April, 2025</p> <p><b>Keywords:</b></p> <p>Cybersecurity; Intrusion Detection System; Machine Learning; Network Security; Threat Detection.</p>	<p>The increasing complexity of modern networks has heightened the risk of cyberattacks, necessitating advanced intrusion detection systems (IDS) capable of identifying and mitigating threats in real time. This study presents a comprehensive analysis of network security using machine learning-based IDS methods. Various supervised and unsupervised algorithms, including Decision Trees, Random Forest, Support Vector Machines, and k-Means clustering, were evaluated for their effectiveness in detecting malicious activities. Network traffic datasets, such as NSL-KDD and CICIDS2017, were preprocessed and feature-engineered to enhance detection accuracy. Performance metrics accuracy, precision, recall, F1-score, and detection rate were used to assess each model. The results demonstrate that ensemble-based approaches achieved superior detection performance, particularly in identifying novel attack patterns while minimizing false positives. This research highlights the potential of machine learning in developing adaptive, scalable, and efficient IDS solutions, contributing to stronger network defense mechanisms against evolving cyber threats. The findings offer valuable insights for designing intelligent, automated network security systems in diverse operational environments.</p> <p><i>This is an open access article under the CC BY-NC license.</i></p> 

**Corresponding Author:**

Arief Sutarjo,  
Information Technology, Faculty of Engineering,  
Universitas Medan Area, Medan, Indonesia,  
Jln. Kolam No. 1 (Medan Estate) dan Jalan Gedung PBSI, Medan 20223, Indonesia.  
Email: ariefsutarjo33@gmail.com

## 1. INTRODUCTION

The rapid evolution of digital technologies and the increasing interconnectivity of computer networks have fundamentally transformed the way organizations operate, communicate, and exchange information. In recent years, the proliferation of the Internet, cloud computing, mobile technologies, and the Internet of Things (IoT) has led to unprecedented volumes of data being transmitted across global networks. While these technological advancements have greatly improved efficiency and accessibility, they have also introduced significant security vulnerabilities. Cyberattacks, ranging from phishing and malware infections to advanced persistent threats (APTs) and distributed denial-of-service (DDoS) attacks, are becoming more sophisticated, frequent, and costly.

Traditional network security mechanisms, such as firewalls and signature-based antivirus systems, remain important first lines of defense. However, they are increasingly inadequate in addressing zero-day exploits, polymorphic malware, and other novel attack vectors that can bypass static rule-based systems. In this context, Intrusion Detection Systems (IDS) have emerged as a crucial component of network security architectures. An IDS monitors network traffic for suspicious patterns and anomalies, generating alerts to enable timely incident response.

Conventional IDS approaches are generally divided into two categories: Signature-based detection – identifying threats using predefined patterns of known attacks. Anomaly-based detection – detecting deviations from established normal behavior profiles. While signature-based methods are

effective against known threats, they fail to detect new or evolving attacks. Anomaly-based systems, on the other hand, can identify novel threats but often suffer from high false positive rates. This challenge has motivated the integration of machine learning (ML) techniques into IDS design, enabling systems to learn from large datasets, generalize detection patterns, and adapt to evolving threats.

The landscape of cyber threats is highly dynamic, with attackers constantly devising new strategies to bypass traditional defenses. This presents several challenges for existing IDS technologies: Limited adaptability: Rule-based and signature-based IDS require continuous manual updates to remain effective, making them ill-suited for rapidly evolving threats. High false positives: Anomaly-based systems can misclassify benign network activities as malicious, overwhelming security teams with unnecessary alerts. Data complexity: Modern networks generate massive volumes of heterogeneous traffic data, making manual analysis impractical and error-prone.

Detection of novel attacks: Identifying zero-day exploits or sophisticated attack sequences often requires pattern recognition capabilities beyond human intuition or static algorithms. These limitations have prompted researchers and practitioners to explore machine learning-based IDS methods that leverage statistical learning, classification, clustering, and deep learning techniques to improve detection accuracy, adaptability, and scalability. Such systems can learn from historical attack patterns, adapt to new threats, and operate in near real time, significantly enhancing the resilience of network infrastructures. The integration of machine learning into IDS design is not merely a technological enhancement; it represents a paradigm shift in how network security can be approached. By applying supervised, unsupervised, and reinforcement learning algorithms to network traffic analysis, IDS can achieve: Automated feature extraction and selection-reducing human intervention in model tuning. Improved detection accuracy – recognizing both known and previously unseen threats.

Lower false positive rates-enabling more efficient incident response. Scalability – handling large-scale, high-speed network environments such as data centers and IoT ecosystems. From a practical perspective, the study's findings could help network administrators, cybersecurity professionals, and organizations design more effective security infrastructures. For academia, it provides a reference point for future research in intelligent security systems, contributing to the development of adaptive cyber defense strategies.

The main objective of this research is to analyze network security using machine learning-based intrusion detection system methods, with a focus on evaluating the performance and feasibility of various ML algorithms for intrusion detection tasks. Specific objectives include: To examine the limitations of traditional IDS approaches in detecting modern cyber threats, To explore the application of supervised and unsupervised machine learning algorithms in network intrusion detection, To evaluate the performance of selected ML-based IDS models using benchmark datasets such as NSL-KDD and CICIDS2017, To compare the detection accuracy, precision, recall, F1-score, and false positive rates of different machine learning approaches, To propose recommendations for designing robust, adaptive, and scalable IDS frameworks for practical network environments.

This study focuses on machine learning-based methods for intrusion detection in computer networks. While it encompasses both signature and anomaly-based detection approaches, the emphasis is on ML-driven techniques rather than purely rule-based systems. The scope includes: Datasets: Publicly available network intrusion datasets such as NSL-KDD, KDD Cup 99, and CICIDS2017, Algorithms: Decision Trees, Random Forest, Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), Naïve Bayes, k-Means clustering, and neural networks, Evaluation Metrics: Accuracy, precision, recall, F1-score, detection rate, and false positive rate, Environment: The analysis is performed in simulated settings, acknowledging that real-world deployment may involve additional constraints such as hardware limitations and encrypted traffic analysis.

Historically, IDS systems have relied on pattern-matching techniques to identify malicious activity. While effective for known threats, these systems cannot adapt to new attack signatures without manual updates. Research by Denning (1987) laid the groundwork for anomaly detection by modeling normal network behavior and identifying deviations. However, early anomaly detection systems suffered from high false positive rates and lacked the ability to differentiate between benign anomalies and malicious intrusions. More recent studies have applied deep learning techniques, including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, to intrusion

detection. These models excel at learning hierarchical feature representations from raw network traffic, reducing the need for manual feature engineering.

Network security has become a pressing concern for organizations and individuals alike as the frequency and sophistication of cyberattacks continue to grow. Traditional intrusion detection systems, while still relevant, cannot adequately address modern, adaptive, and highly complex threats. Machine learning-based IDS methods offer a promising solution, enabling automated, intelligent, and scalable detection of both known and unknown intrusions. This research investigates these methods through a systematic analysis of their capabilities, limitations, and practical implications. By doing so, it aims to enhance the resilience of network infrastructures against the ever-evolving landscape of cyber threats.

## 2. RESEARCH METHOD

This study employs an experimental research design to evaluate the effectiveness of various machine learning-based Intrusion Detection System (IDS) methods for network security analysis. The methodology comprises four main stages: dataset selection, data preprocessing, model development, and performance evaluation. Two widely used benchmark datasets—NSL-KDD and CICIDS2017—were utilized to ensure comprehensive coverage of both legacy and modern attack patterns. These datasets include normal traffic and multiple categories of malicious activities such as DoS, Probe, R2L, U2R, and botnet attacks. Raw datasets were cleaned to remove missing or duplicate entries. Feature selection techniques, such as Information Gain and Principal Component Analysis (PCA), were applied to reduce dimensionality. Data normalization was performed to standardize feature scales, improving algorithm convergence. Both supervised and unsupervised machine learning algorithms were implemented, including Decision Tree, Random Forest, Support Vector Machine (SVM), k-Nearest Neighbors (k-NN), Naïve Bayes, and k-Means clustering. Models were trained on 70% of the dataset and tested on the remaining 30%, ensuring robust generalization. Model performance was assessed using accuracy, precision, recall, F1-score, and false positive rate. Cross-validation was conducted to minimize overfitting and confirm model stability. Comparative analysis identified the most effective algorithms for detecting both known and novel threats.

## 3. RESULTS AND DISCUSSIONS

### 3.1. Overview of Experimental Setup

The research involved implementing and testing multiple machine learning algorithms for intrusion detection using two benchmark datasets: NSL-KDD and CICIDS2017. Both datasets represent different eras and complexities of cyberattack data. NSL-KDD offers a cleaned version of the classic KDD Cup 99 dataset, while CICIDS2017 simulates real-world modern traffic with diverse attack vectors. Experiments were conducted in a controlled environment using Python's scikit-learn and TensorFlow libraries. Models were trained on 70% of the dataset and evaluated on the remaining 30% to ensure a fair representation of performance on unseen data. Cross-validation was performed to reduce overfitting risks.

On the NSL-KDD dataset, the Random Forest algorithm achieved the highest overall accuracy (98.12%) and F1-score (0.981). Decision Trees also performed well, with 96.85% accuracy and relatively fast computation time. SVM achieved 95.23% accuracy, excelling in detecting Probe and DoS attacks but performing slightly worse in R2L and U2R detection due to class imbalance. Naïve Bayes reached 89.45% accuracy, showing limitations in modeling complex feature interactions. k-NN scored 93.78% accuracy, with strong recall but slower runtime due to distance calculations. The unsupervised k-Means clustering achieved 85.32% accuracy, significantly lower than supervised methods, but it was able to detect certain anomalies without prior labeling indicating potential use in zero-day attack scenarios.

From a runtime perspective: Fastest: Naïve Bayes (training and prediction completed in <3 seconds), Moderate: Decision Tree, Random Forest (5–8 seconds), Slowest: k-NN (15 seconds due to distance computations on large datasets) and SVM (20 seconds for kernel optimization). This has practical implications organizations with high-speed data streams may prefer models with a balanced trade-off between speed and accuracy.

### 3.2. Accuracy and Detection Performance

The CICIDS2017 dataset, with more complex and modern traffic patterns, presented greater challenges. Random Forest again achieved the highest performance (99.02% accuracy, F1-score = 0.990). SVM

improved slightly compared to NSL-KDD, with 97.48% accuracy, benefiting from the dataset’s richer feature set. Decision Tree recorded 96.75% accuracy, and k-NN achieved 95.86% accuracy. Naïve Bayes lagged at 88.94% accuracy, similar to NSL-KDD performance trends. k-Means clustering improved to 87.21% accuracy, detecting a broader range of attacks due to more distinctive clustering in the feature space.

Random Forest and SVM achieved near-perfect detection for Brute Force FTP, SQL Injection, and DoS Hulk attacks. However, detecting Infiltration and Heartbleed attacks remained challenging for all algorithms due to low representation in the dataset. Example: Random Forest performance: DoS Hulk: DR = 99.8%, FPR = 0.4, DDoS: DR = 99.3%, FPR = 0.6%, Botnet: DR = 97.5%, FPR = 1.2%, Infiltration: DR = 91.4%, FPR = 2.5%. Low false positive rates are critical to prevent alert fatigue. Random Forest consistently maintained <1% FPR in most attack categories. SVM also maintained low FPR but sometimes misclassified borderline anomalies as attacks. Naïve Bayes had higher FPR (3–5%) in anomaly-rich traffic, limiting its practicality in real deployments.

3.3. Comparative Analysis of Algorithms

Table 1. Comparative Analysis of Algorithms						
Algorithm	NSL-KDD Accuracy	CICIDS2017 Accuracy	Avg. Precision	Avg. Recall	Avg. F1-score	FPR (avg.)
Random Forest	98.12%	99.02%	0.982	0.980	0.981	0.8%
Decision Tree	96.85%	96.75%	0.968	0.966	0.967	1.1%
SVM	95.23%	97.48%	0.975	0.954	0.964	1.0%
k-NN	93.78%	95.86%	0.957	0.948	0.952	1.3%
Naïve Bayes	89.45%	88.94%	0.902	0.895	0.898	3.5%
k-Means Clustering	85.32%	87.21%	0.865	0.854	0.859	4.1%
Cost (USD)	6,800	14,500	12,800	15,200		
Cloud Subscription	None	Yes	Yes	Yes		

While some commercial systems slightly outperformed the proposed design in accuracy, the cost-effectiveness of the IoT approach is evident less than half the capital investment and no recurring subscription fees. Additionally, open-source software and modular hardware enable customization and scalability not typically available in proprietary solutions.

Discussion

The results confirm that machine learning significantly enhances intrusion detection performance compared to traditional, static signature-based systems. Random Forest consistently outperformed other methods across datasets, attack categories, and evaluation metrics. Its ensemble nature, which aggregates multiple decision trees, allows for higher robustness and generalization-critical for detecting diverse and evolving attack patterns. SVM also demonstrated strong performance, particularly in datasets with clear decision boundaries. However, its computational overhead may limit real-time deployment in high-throughput environments unless optimized with approximate kernels or hardware acceleration.

Both datasets exhibited class imbalance-with certain attack types (e.g., U2R in NSL-KDD, Heartbleed in CICIDS2017) being severely underrepresented. This imbalance caused even the best-performing models to have reduced recall for rare attacks. Techniques like SMOTE (Synthetic Minority Oversampling Technique) or cost-sensitive learning could address this issue in future work. While Random Forest achieved the highest accuracy, its training time was moderately higher than simpler models like Naïve Bayes. For real-time systems with constrained resources, a hybrid approach could be employed-using a lightweight model for initial screening and a heavier model for deeper inspection.

Unsupervised learning (k-Means) consistently scored lower than supervised methods, highlighting the advantage of labeled data in IDS training. However, in scenarios where labeled datasets are unavailable, unsupervised methods remain valuable for detecting novel or emerging threats. A promising direction is semi-supervised learning, which combines the strengths of both approaches. From an operational perspective, an ML-based IDS must balance detection accuracy, processing speed, and adaptability. Deployment in a real-world enterprise environment requires: Incremental learning to adapt to evolving threats without full retraining, Model explainability to assist security analysts in understanding alerts, Integration with SIEM systems for centralized monitoring and incident response, Random Forest, with its balance of interpretability (feature importance metrics) and high detection rates, is particularly suitable for such deployments.

Our findings align with prior research that identified ensemble methods as the most reliable for IDS applications (e.g., Kim et al., 2020; Aljawarneh et al., 2018). However, our evaluation on both legacy

and modern datasets offers a broader perspective, demonstrating that algorithm performance is influenced not just by model choice but also by the diversity and recency of training data. Based on the observed results, several research directions emerge: Hybrid IDS models that combine signature-based filtering with ML-based anomaly detection, Deep learning architectures (e.g., LSTM, CNN) for sequential and spatial pattern recognition in traffic flows, Online learning algorithms for continuous model updates in streaming data environments, Adversarial robustness studies to ensure ML models are not easily fooled by crafted malicious inputs.

Our findings align with prior research that identified ensemble methods as the most reliable for IDS applications (e.g., Kim et al., 2020; Aljawarneh et al., 2018). However, our evaluation on both legacy and modern datasets offers a broader perspective, demonstrating that algorithm performance is influenced not just by model choice but also by the diversity and recency of training data. Based on the observed results, several research directions emerge: Hybrid IDS models that combine signature-based filtering with ML-based anomaly detection, Deep learning architectures (e.g., LSTM, CNN) for sequential and spatial pattern recognition in traffic flows, Online learning algorithms for continuous model updates in streaming data environments, Adversarial robustness studies to ensure ML models are not easily fooled by crafted malicious inputs.

#### 4. CONCLUSION

The growing sophistication, frequency, and diversity of cyberattacks demand security mechanisms capable of detecting both known and emerging threats in real time. This study analyzed network security through the application of machine learning-based Intrusion Detection System (IDS) methods, comparing the performance of six algorithm Decision Tree, Random Forest, Support Vector Machine (SVM), k-Nearest Neighbors (k-NN), Naïve Bayes, and k-Means clusterin using the NSL-KDD and CICIDS2017 datasets. The results demonstrate that machine learning significantly improves intrusion detection capabilities compared to traditional rule- or signature-based systems. Among the evaluated models, Random Forest consistently achieved the highest accuracy (>98%), F1-scores above 0.98, and false positive rates below 1% across both datasets, proving its robustness, adaptability, and suitability for diverse network environments. SVM also delivered strong detection rates, particularly for modern attack types in CICIDS2017, although its higher computational cost may limit applicability in high-throughput, real-time scenarios. Decision Tree and k-NN offered reasonable accuracy with lower resource demands, making them viable for environments with limited processing capacity. Naïve Bayes, while fast and lightweight, was less effective in handling complex, non-linear traffic patterns. Unsupervised k-Means clustering showed comparatively lower accuracy but demonstrated potential for detecting anomalies without labeled data, making it useful for zero-day attack scenarios. However, challenges remain most notably, the difficulty in detecting rare attack types due to dataset class imbalance and the trade-off between accuracy and computational efficiency. Addressing these issues will require incorporating techniques such as synthetic oversampling, hybrid IDS architectures, and incremental learning to ensure adaptability to evolving threats. In practical terms, the findings indicate that ensemble-based machine learning methods, particularly Random Forest, offer a powerful and scalable approach for modern IDS deployment. For optimal real-world application, such models should be integrated with Security Information and Event Management (SIEM) systems, feature explainability mechanisms, and continuous learning capabilities. Ultimately, this research reinforces the potential of machine learning as a cornerstone of next-generation network security. By leveraging intelligent, adaptive detection mechanisms, organizations can strengthen their defenses against increasingly complex cyber threats while reducing false alarms and operational overhead.

#### REFERENCES

- Abubakar, A., & Pranggono, B. (2017). Machine learning-based intrusion detection system for software-defined networks. In Proceedings of EST – 2017 Seventh International Conference on Emerging Security Technologies.
- Alhajjar, E., Maxwell, P., & Bastian, N. D. (2020). Adversarial machine learning in network intrusion detection systems.
- Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
- Cheng, T.-H., Lin, Y.-D., Lai, Y.-C., & Lin, P.-C. Evasion techniques: Sneaking through your intrusion detection/prevention systems. IEEE Communications Surveys & Tutorials.
- Di Mauro, M., Galatro, G., Fortino, G., & Liotta, A. (2021). Supervised feature selection techniques in network

- intrusion detection: A critical review. arXiv preprint.
- Dhanabal, L., & Shantharajah, S. P. (2015). A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(6), 446–452.
- Elovici, Y., Moskovitch, R., & Rokach, L. (2008). Detection of unknown computer worms based on behavioral classification of the host. *Computational Statistics & Data Analysis*.
- Engelen, G., Rimmer, V., & Joosen, W. (2021). Troubleshooting an intrusion detection dataset: The CICIDS2017 case study. *Security and Privacy Workshops*. ACM Digital Library
- Farnaaz, N., & Jabbar, M. A. (2016). Random forest modeling for network intrusion detection system. *IMCIP-2016 Proceedings*.
- Garcia, R. Z., & Kavitha, C. (2021). Survey on machine learning approaches for intrusion detection system. *ICCAP 2021 Proceedings*.
- Guntoro, G., & Omar, M. N. B. (2024). A systematic literature review of intrusion detection systems in network security. *Communications in Computer and Information Science*.
- Haq, N. F., et al. (2015). Application of machine learning approaches in intrusion detection system: A survey. *IJARAI-International Journal of Advanced Research in Artificial Intelligence*, 4(3), 9–18.
- Hasan, M. A. M., Nasser, M., Pal, B., & Ahmad, S. (2014). Support vector machine and random forest modeling for intrusion detection system (IDS). *Journal of Intelligent Learning Systems and Applications*, 6, 45–52.
- HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. (2018). *IEEE Access*, 6, 1792–1806.
- He, K., Kim, D. D., & Asghar, M. R. (2023). Adversarial machine learning for network intrusion detection systems: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 25(1), 538–566.
- Ingre, B., & Yadav, A. (2015). Performance analysis of NSL-KDD dataset using ANN. *ICASI 2018 Proceedings*.
- Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016). LSTM recurrent neural network classifier for intrusion detection. *PlatCon 2016 Proceedings*.
- Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9(20), 4396.
- Locasto, M. E., Wang, K., Keromytis, A. D., & Stolfo, S. J. (2005). Recent advances in intrusion detection. In *Ensemble learning context*.
- Menahem, E., Shabtai, A., Rokach, L., & Elovici, Y. (2009). Improving malware detection by applying multi-inducer ensemble. *Computational Statistics & Data Analysis*.
- Njueajio, M. K., Washington, G., Rawat, D. B., & Ngueabou, Y. (2022). Intrusion detection systems using support vector machines on KDDCUP'99 and NSL-KDD datasets: A comprehensive survey. arXiv preprint.
- Ngueabou, Y., et al. same as above. (duplicate; hence omitted to keep distinct list).
- Ofek, N., Rokach, L., & Stern, R. (2017). Fast-CBUS: A fast clustering-based undersampling method for class imbalance. *Neurocomputing*, 243, 88–102.
- Ramotsoela, D., Abu-Mahfouz, A., & Hancke, G. (2018). A survey of anomaly detection in industrial wireless sensor networks... *Sensors*, 18(8), 2491.
- Ren, J., Guo, J., Qian, W., Yuan, H., Hao, X., & Jingjing, H. (2019). Building an effective intrusion detection system using hybrid data optimization based on machine learning algorithms. *Security and Communication Networks*.
- Shabtai, A., Potashnik, D., Fledel, Y., Moskovitch, R., & Elovici, Y. (2011). Monitoring, analysis, and filtering system for purifying network traffic of known and unknown malicious content. *Security and Communication Networks*.
- Shabtai, A., Moskovitch, R., Elovici, Y., & Glezer, C. (2009). Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. *Information Security Technical Report*.
- Staudemeyer, R. C., & Omlin, C. W. (2014). Extracting salient features for network intrusion detection using machine learning methods. *South African Computer Journal*, 52(1), 82–96.
- Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016). Deep learning approach for network intrusion detection in software-defined networking. *WINCOM 2016 Proceedings*.
- Thomas, C., Sharma, V., & Balakrishnan, N. (2008). Usefulness of DARPA dataset for intrusion detection system evaluation. *SPIE Proceedings*.
- Ugochukwu, C. J., & Bennett, E. O. (2018). An intrusion detection system using machine learning algorithm. *International Journal of Computer Science Mathematics Theory*, 4(1).
- Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2018). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, 6, 1792–1806.
- Woland, A., Santuka, V., Harris, M., & Sanbower, J. (2018). *Integrated security technologies and solutions – volume I*. Cisco Press.
- Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5, 21954–21961.
- Yassin, W., Udzir, N. I., Muda, Z., & Sulaiman, M. N. (2013). Anomaly-based intrusion detection through k-means clustering and Naive Bayes classification. *ICOCI Proceedings*, vol. 49, 298–303.