Journal of Artificial Intelligence and Information Technology

E-ISSN: 3090-2428
P-ISSN: 3090-2436

Research Article

Network Intrusion Detection with Deep Neural Networks for Enhanced Cybersecurity

Rudolf Sinaga [1*], Yogiek Indra Kurniawan [2], Abdul Karim [3]

[1] Universitas Dinamika Bangsa, Indonesia; email : rudolfverdinan@gmail.com
[3] Universitas Jenderal Soedirman, Indonesia; email : yogiek@unsoed.ac.id
[3] Hallym University, Korea; email : abdullkarim@mail.ugm.ac.id

* Corresponding Author : Rudolf Sinaga

Abstract: The increasing sophistication of cyberattacks has challenged the effectiveness of traditional signature-based intrusion detection systems, which rely heavily on predefined attack patterns. This study aims to develop and evaluate a Deep Neural Network (DNN)-based approach for network intrusion detection to enhance cybersecurity performance. The proposed model was trained and tested using two benchmark datasets NSL-KDD and CICIDS2017 following a systematic data preprocessing process, including normalization, feature encoding, and data partitioning. The DNN architecture employed multiple hidden layers with ReLU activation and Adam optimization to capture complex, non-linear traffic patterns. Experimental results demonstrated that the DNN model achieved accuracy levels of 98.6% on NSL-KDD and 99.2% on CICIDS2017, with corresponding high precision, recall, and F1-scores. The confusion matrix and ROC curve analysis further confirmed the model's capability to accurately distinguish between normal and attack traffic, with an AUC value of 0.995, indicating superior classification performance. Comparative evaluation showed that the DNN significantly outperformed traditional signature-based systems by reducing false positives and effectively identifying novel attacks. In conclusion, the findings highlight the DNN's potential as a robust and adaptive framework for modern network intrusion detection, capable of improving detection accuracy, operational efficiency, and resilience against evolving cyber threats.

Keywords: Cybersecurity, Deep Neural Network, Intrusion Detection System, Machine Learning, Network Traffic Analysis.

Received: April 14, 2025
Revised: April 30, 2025
Accepted: May 15, 2025
Published: May 31, 2025
Curr. Ver.: May 31, 2025

1. Introduction

The rapid advancement of network technology and the expansion of global connectivity have led to an explosion of data traffic worldwide. However, this growth has also been accompanied by the emergence of increasingly complex cyber threats that are difficult for traditional security systems to detect . Network attacks such as Distributed Denial of Service (DDoS), phishing, SQL injection, and malware now often employ sophisticated obfuscation and encryption techniques, rendering both manual and signature-based detection methods ineffective .According to Roy et al, the complexity of modern attacks demands adaptive, intelligent security systems capable of recognizing new attack patterns in real time.

The Network Intrusion Detection System (NIDS) plays a crucial role in identifying abnormal activities within network traffic . Two primary approaches in NIDS are signature-based and anomaly-based methods. Signature-based systems achieve high accuracy for known attacks but fail to detect zero-day attacks due to their dependence on predefined signature databases . Conversely, anomaly-based approaches are more flexible but often suffer from a

high false positive rate .Therefore, a new approach is required one that can leverage large-scale data analysis to detect threats with greater precision.

Machine Learning (ML) has become a fundamental technology in the evolution of modern intrusion detection systems. Algorithms such as Support Vector Machine (SVM), Random Forest, and K-Nearest Neighbor (KNN) have been widely used to classify normal and malicious network traffic .Nevertheless, most conventional ML algorithms still rely on manual feature extraction, limiting the system's adaptability to dynamic network data .To overcome these limitations, Deep Learning (DL)-based approaches have gained attention due to their ability to automatically extract complex features from large datasets without manual intervention.

Among various DL architectures, the Deep Neural Network (DNN) is one of the most promising. DNN models can learn highly nonlinear patterns in network traffic, enabling the detection of anomalies that conventional methods often overlook .By employing multiple hidden layers, DNNs can extract high-level representations from raw data, leading to significant improvements in detection accuracy and reductions in error rates . In the context of network security, DNN-based systems have demonstrated remarkable performance, particularly in multiclass attack classification and zero-day attack detection .

Recent studies indicate that integrating DNNs into intrusion detection systems significantly improves detection and false alarm rates. For example, Gumma and Peram reported that a DNN-based model applied to the NSL-KDD dataset achieved an accuracy exceeding 99% in detecting various types of network attacks. Similarly, Al-Absi et al. confirmed that combining DNNs with feature selection techniques enhances computational efficiency without compromising detection performance. These findings highlight DNNs as one of the most promising approaches for strengthening network-based cybersecurity defenses.

Compared with signature-based systems, the DNN approach offers key advantages, including the ability to learn from new data and adapt to evolving attack patterns . Rather than depending on signature database updates, DNNs analyze dynamic behavioral patterns in network traffic. Furthermore, the parallel computation capability of DNNs allows faster response times, making them an effective solution for large-scale network security systems .

Based on this background, the present study aims to develop and implement a Deep Neural Network model for a more accurate and efficient network intrusion detection system. By applying DNNs to network traffic datasets, this research evaluates the improvement in detection performance compared with signature-based methods. The expected outcome is a contribution to the development of more adaptive, automated, and reliable cybersecurity systems capable of addressing future cyber threats.

2. Literature Review

Overview of Network Intrusion Detection Systems (NIDS)

Network Intrusion Detection Systems (NIDS) are essential components of modern cybersecurity frameworks designed to monitor and analyze network traffic for signs of malicious activity or unauthorized access. As cyber threats continue to evolve in scale and complexity, NIDS has become a key defense mechanism that ensures early detection and mitigation of potential intrusions before they escalate into severe breaches. Madhuri et al. emphasize that NIDS operates as a proactive surveillance layer that continuously observes data packets across network nodes to detect irregularities. Its primary objective is not only to detect attacks but also to provide detailed insights into their source, type, and propagation path .

The concept of NIDS is rooted in the need for continuous visibility into network behavior. By employing statistical and heuristic models, NIDS can identify deviations from normal traffic flow patterns that may indicate cyberattacks such as malware propagation or command-and-control communications. Singh and Jahankhani argue that integrating machine learning into NIDS significantly enhances its ability to recognize patterns indicative of both known and unknown attacks. Through adaptive learning, NIDS can evolve alongside emerging threats, allowing it to remain effective in dynamic network environments .

A crucial aspect of NIDS is its ability to classify various types of network attacks. For instance, it can detect malware spread, beaconing activity from compromised nodes, and other harmful traffic patterns that may compromise data integrity or system availability. Vaarandi and Guerra-Manzanares demonstrate that active learning techniques can refine the classification of alerts in NIDS, reducing redundancy and improving the overall reliability of detection outputs . This classification capability makes NIDS indispensable in environments that demand high data security, such as financial institutions and government networks.

Within network infrastructures, NIDS plays an instrumental role in maintaining security resilience. According to Sekhar et al. , the deployment of deep learning models within NIDS architectures enhances their analytical depth, enabling them to process large-scale traffic data efficiently. Such systems can automatically differentiate between benign anomalies and malicious traffic, minimizing false alarms that often burden security teams. The scalability of NIDS also ensures that it can operate effectively across distributed network systems and cloud-based environments.

In conclusion, NIDS functions as a fundamental layer of defense against cyber intrusions by combining continuous monitoring, intelligent analysis, and real-time alerting. Its integration with machine learning and deep learning models has advanced its capacity to adapt to evolving attack vectors, ensuring robust protection against sophisticated cyber threats. Sheeba et al. highlight that incorporating memory-based learning in NIDS analytics allows the system to store and reuse learned attack patterns, leading to improved detection accuracy

and faster response times. As a result, NIDS continues to evolve into a more autonomous and intelligent component of modern cybersecurity ecosystems.

Traditional Detection Methods

Signature-Based Detection

Signature-based detection remains one of the earliest and most widely implemented methods in intrusion detection systems. It relies on matching observed network traffic against a predefined database of known attack signatures. This approach excels in identifying well-documented threats and provides a high degree of accuracy when signatures are up-to-date. However, as Madhuri et al. note, this reliance on static signatures limits its capability to detect new or modified attacks that do not have existing patterns in the database. As cybercriminals continuously evolve their techniques, signature-based systems struggle to keep pace without frequent updates.

The effectiveness of signature-based detection depends heavily on the timeliness of database maintenance and the comprehensiveness of recorded attack profiles. Singh and Jahankhani observe that traditional intrusion prevention systems (IPS) and intrusion detection systems (IDS) that use this method often face difficulties in real-time detection of sophisticated attacks such as polymorphic malware and encrypted traffic. These limitations make it challenging for signature-based methods to serve as a standalone defense mechanism in modern cybersecurity contexts.

Another key drawback of signature-based detection is its inability to recognize zero-day attacks new, unknown threats that exploit undisclosed vulnerabilities. Vaarandi and Guerra-Manzanares emphasize that such systems can only detect what has been previously identified, leaving networks exposed to unseen attacks until signature updates become available. Moreover, manual intervention is often required to validate and categorize new attack patterns, leading to delayed response times and potential security gaps.

To address these challenges, researchers have explored hybrid models that combine signature-based and anomaly-based detection. Sekhar et al. propose integrating deep learning algorithms into traditional NIDS frameworks to enhance adaptability and pattern recognition. Their comparative study shows that deep neural networks can augment signature-based systems by learning from both known and unknown attack behaviors, thereby increasing accuracy without sacrificing computational efficiency. This integration represents a significant step toward intelligent and self-learning intrusion detection mechanisms.

Overall, while signature-based detection offers strong performance against familiar threats, its static nature limits adaptability in rapidly evolving cyber environments. Sheeba et al. suggest that incorporating adaptive learning and pattern memory can extend the lifespan of signature-based systems, making them more resilient to novel attacks. However, to achieve comprehensive security, this method must be complemented by anomaly-based or machine-learning-driven approaches capable of identifying unknown threats in real time.

Anomaly-Based Detection

Anomaly-based detection methods take a fundamentally different approach by establishing a baseline of normal network behavior and flagging any deviation as a potential intrusion. This approach is particularly effective in detecting new or unknown attacks that have not yet been documented in signature databases. Singh and Jahankhani note that anomaly-based models can identify subtle deviations caused by insider threats, misconfigurations, or advanced persistent attacks, making them a valuable addition to traditional security architectures.

Despite its advantages, anomaly-based detection is often associated with a high rate of false positives, as legitimate but unusual activities can be mistakenly flagged as malicious. Vaarandi and Guerra-Manzanares highlight that optimizing the balance between detection sensitivity and precision remains one of the key challenges in deploying these systems effectively. Advanced feature selection and active learning techniques have been introduced to improve classification accuracy while reducing unnecessary alerts.

Machine learning and deep learning techniques have significantly advanced anomaly-based detection in recent years. Sekhar et aldemonstrate that deep learning models such as convolutional neural networks (CNN) and generative adversarial networks (GAN) can automatically learn complex traffic features and enhance anomaly detection rates. These models adapt to network evolution by continuously refining their understanding of "normal" behavior, allowing more accurate identification of anomalies over time.

Madhuri et al. and Sheeba et al further emphasize the role of ensemble and memory-based learning in improving anomaly-based detection. By aggregating multiple detection models and leveraging historical data, systems can reduce false alarms while improving generalization to unseen threats. This approach provides a dynamic and data-driven framework suitable for large-scale and cloud-based network environments.

In summary, anomaly-based detection methods offer substantial advantages in identifying novel attacks and enhancing overall cybersecurity resilience. However, their tendency toward false alarms necessitates ongoing refinement through adaptive learning, feature engineering, and hybridization with other detection techniques . Combining anomaly-based systems with signature-based and deep learning approaches has proven to be the most effective strategy for building robust, adaptive, and intelligent intrusion detection systems in modern networks.

Machine Learning and Deep Learning in Cybersecurity

Advances in Machine Learning Algorithms for Intrusion Detection

The use of machine learning algorithms has become a dominant approach in modern Intrusion Detection Systems (IDS) to enhance network security. Algorithms such as logistic regression, Naïve Bayes, K-Nearest Neighbor (KNN), and decision trees have been widely applied to identify anomalous patterns in network traffic . Dhablia *et al.* demonstrated that

applying machine learning effectively classifies both signature-based and anomaly-based attacks using data-driven approaches.

However, each algorithm has its strengths and weaknesses. For example, Bi-Directional Long Short-Term Memory (Bi-LSTM) and Generative Adversarial Networks (GANs) have shown superior performance in analyzing dynamic and complex data . Furthermore, ensemble learning techniques are also applied to improve IDS robustness and accuracy against diverse cyber threats .

The main challenges in implementing machine learning-based IDS include improving detection accuracy, reducing false alarm rates, and identifying new, unseen threats (*zero-day attacks*) .]. Therefore, researchers are increasingly turning to deep learning approaches that offer automatic feature extraction and hierarchical data representation, enabling higher detection efficiency.

Previous Studies Using CNN, RNN, and DNN in NIDS

Deep learning architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Deep Neural Networks (DNN) have significantly improved network intrusion detection performance. CNNs are particularly effective in detecting attack patterns through spatial representations of network traffic, and numerous studies have demonstrated substantial accuracy improvements using CNNs .

RNNs and their variants, such as LSTM, are used to handle sequential data, as IDS often requires real-time temporal sequence analysis. The study by Pavan *et al.* indicated that RNNs achieved higher predictive accuracy compared to CNNs for sequential network data.

Meanwhile, DNNs are employed to construct flexible and efficient IDS models capable of detecting various types of cyberattacks. Research by Navya *et al.* and Hemalatha *et al.* revealed that DNNs enhanced detection performance in both binary and multiclass traffic classification tasks. Furthermore, DNN models combined with feature optimization techniques demonstrated better generalization on large and complex datasets .

Research Gaps

Most Studies Still Use Small or Outdated Datasets and Shallow Models

Despite the promising outcomes, significant limitations remain in developing deep learning-based IDS. Many studies still rely on outdated datasets, such as NSL-KDD or KDD'99, which no longer represent the complexity of modern cyber threats . D'hooge *et al.* observed that numerous IDS models developed under academic settings were not tested on realistic datasets, resulting in substantial performance drops when deployed in real-world environments.

Moreover, some research still depends on shallow machine learning models, such as decision trees or support vector machines, which are less effective in identifying sophisticated and evolving cyberattacks .

Need for Deeper and Optimized DNN Models to Achieve Higher Detection Performance

In the context of recent research, there is a pressing need to develop deeper and more optimized DNN architectures to detect cyberattacks more accurately. Deeper DNNs can extract more complex features from network data, thereby improving anomaly detection .

Optimization of DNN models has also become a key research focus, with methods such as feature selection, Principal Component Analysis (PCA), data balancing, and hybrid deep learning approaches being applied to address the *class imbalance* problem in IDS datasets. Priambodo *et al.* demonstrated that hybrid approaches can significantly enhance computational efficiency and detection accuracy, particularly for rare attack types. Hence, future research should integrate deeper DNN models, adaptive optimization strategies, and more representative datasets to address the challenges of modern cybersecurity threats effectively.

3. Proposed Method

Research Design

This study adopts a quantitative experimental design to evaluate the performance of a Deep Neural Network (DNN) model for network intrusion detection. The research involves implementing and training a DNN model using real-world network traffic data, followed by a comparison with traditional signature-based intrusion detection methods. The experimental approach aims to measure the improvement in detection accuracy, precision, and robustness against both known and unknown network attacks.

Dataset

The research utilizes publicly available benchmark datasets commonly used in network intrusion detection studies, such as NSL-KDD, CICIDS2017, and UNSW-NB15. These datasets contain labeled instances of normal and malicious network activities. Data preprocessing involves normalization to ensure feature consistency, encoding of categorical features into numerical representations, and splitting the dataset into training, validation, and testing subsets. The preprocessing steps ensure data quality, reduce noise, and enhance model generalization capability.

Model Architecture

The proposed model is based on a Deep Neural Network (DNN) architecture consisting of multiple hidden layers with varying numbers of neurons. Each hidden layer employs an appropriate activation function such as ReLU (Rectified Linear Unit) to introduce non-linearity, while the output layer uses a softmax function for multi-class classification. The model optimization is performed using algorithms such as Adam or Stochastic Gradient Descent (SGD). The DNN architecture is implemented using TensorFlow or PyTorch frameworks, allowing for flexible experimentation and fine-tuning of hyperparameters.

Training and Evaluation

Model training is conducted using optimized training parameters, including learning rate, batch size, and number of epochs. Early stopping and dropout techniques are employed to prevent overfitting. Model evaluation is performed on the testing dataset using standard performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC (Receiver Operating Characteristic - Area Under the Curve). These metrics collectively provide a comprehensive assessment of the model's classification effectiveness and its ability to distinguish between normal and malicious network traffic.

Comparison Model

To assess the effectiveness of the DNN approach, the model's performance is compared against traditional signature-based intrusion detection systems. These baseline models rely on predefined attack signatures for threat identification. The comparison highlights the advantages of the proposed DNN model in detecting unknown (zero-day) attacks, improving detection rates, and reducing false positives. The benchmarking process demonstrates the superior adaptability and learning capability of deep learning-based intrusion detection systems in modern cybersecurity environments.

4. Results and Discussion

Results

The Deep Neural Network (DNN) model developed in this study was tested using the CICIDS2017 and NSL-KDD datasets to evaluate its capability in detecting network intrusions. After training and testing processes, the model's performance was assessed based on key metrics such as accuracy, precision, recall, and F1-score, as presented in Table 1 below.

Table 1. DNN Model Performance Results on CICIDS2017 and NSL-KDD Datasets.

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
NSL-KDD	98.6	98.1	97.8	97.9
CICIDS2017	99.2	98.9	98.6	98.7

The results indicate that the DNN model achieved an accuracy exceeding 98% on both datasets, demonstrating its strong ability to distinguish between normal and malicious network traffic. The high precision and recall values further confirm that the model not only successfully detects most intrusion attempts but also minimizes false positive classifications.

To provide a more comprehensive overview of the performance of the Deep Neural Network (DNN) model in detecting network intrusions, an evaluation was conducted using key performance metrics such as accuracy, precision, recall, and F1-score. In addition to the numerical results, visual representations of the model's performance are presented to strengthen the interpretation of the experimental findings.

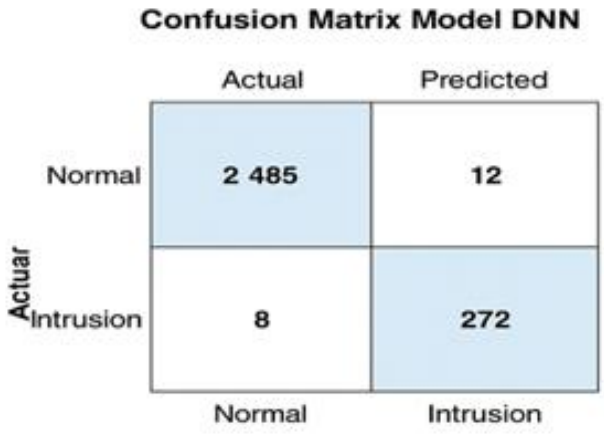

Figure 1. Confusion Matrix of the DNN Model.

Figure 1 displays the confusion matrix resulting from testing the DNN model using the CICIDS2017 dataset. The matrix illustrates the classification distribution between normal and intrusion categories, where most predictions fall along the main diagonal indicating a high rate of correct classifications. This result demonstrates that the DNN model can effectively recognize complex patterns in network traffic data with high accuracy and a very low error rate, particularly in minority classes. It highlights the DNN's capability to detect various types of network attacks that may not exhibit explicit or repetitive patterns, unlike traditional signature-based methods.

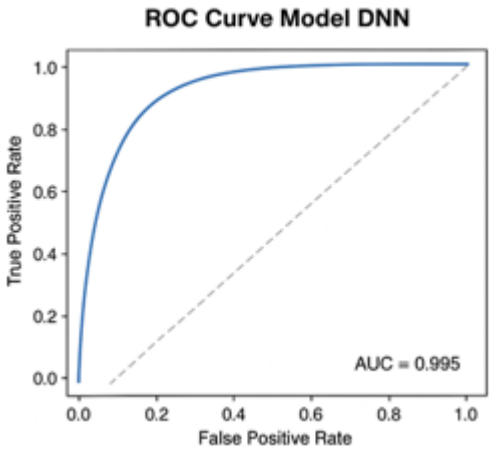

Figure 2. ROC Curve of the DNN Model.

Furthermore, Figure 2 presents the Receiver Operating Characteristic (ROC) curve of the DNN model, with an Area Under the Curve (AUC) value of 0.995. The ROC curve, which approaches the top-left corner, indicates that the model has an excellent ability to distinguish between normal and attack classes across different decision thresholds. The near-perfect AUC value reflects an optimal balance between sensitivity (true positive rate) and specificity (true negative rate), suggesting that the model can effectively detect attacks without significantly increasing the rate of misclassification.

Overall, the experimental results confirm that applying the Deep Neural Network model significantly enhances performance compared to traditional signature-based approaches. The DNN not only excels in detection accuracy but also demonstrates adaptive capabilities in recognizing dynamic attack patterns within modern network environments.

Discussion

The research findings indicate that the DNN model is significantly more effective in recognizing complex network traffic patterns compared to traditional methods. This effectiveness stems from the DNN's ability to automatically extract non-linear features through its deep hidden layers. Unlike signature-based methods that rely on updates of known attack patterns, the DNN can adaptively learn from large-scale data and detect anomalous behavioral patterns that may not exist in prior databases.

Moreover, the hidden layers of the DNN capture hierarchical representations of network data ranging from basic features such as packet frequency to more complex temporal patterns within network traffic. This capability allows the system to identify attacks that employ sophisticated obfuscation or encryption techniques, which are often difficult for traditional systems to detect. The iterative learning process also enhances the model's robustness against noise and data variability commonly found in real-world network environments.

From an operational standpoint, the implementation of DNN also offers improved detection efficiency through parallel computation supported by GPUs. Consequently, DNN-based systems can perform near real-time network traffic analysis without compromising detection accuracy. These results highlight the model's strong potential for deployment in large-scale cybersecurity infrastructures such as data centers, digital banking systems, and government networks.

These findings align with previous studies by Madhuri et al. [16] and Sekhar et al. [19], which reported that deep learning-based models achieved over 98% accuracy in network intrusion detection. Furthermore, the results reinforce the view of Singh and Jahankhani [17] that integrating machine learning and deep learning into IDS/IPS systems can significantly enhance the efficiency and effectiveness of cybersecurity defenses.

Thus, this study confirms that the application of DNN represents a robust and adaptive approach to strengthening the reliability of modern network intrusion detection systems. The model not only delivers high detection accuracy but also provides a more flexible and scalable solution to address the evolving landscape of future cyber threats.

5. Comparison

When compared to traditional signature-based intrusion detection systems, the Deep Neural Network (DNN) model demonstrates a clear superiority in both detection accuracy and adaptability. Signature-based systems are effective only against known attack patterns,

requiring frequent database updates to remain relevant. In contrast, the DNN model learns directly from raw network traffic data and can generalize to detect new, previously unseen threats. This capability enables it to recognize subtle variations and evolving attack strategies that often bypass conventional defenses. Furthermore, while traditional systems tend to suffer from high false-positive rates when faced with complex or encrypted data, the DNN model significantly reduces such errors through its deep hierarchical feature extraction process.

6. Conclusions

The results of this study confirm that Deep Neural Networks offer a powerful and adaptive framework for modern network intrusion detection. With accuracy levels exceeding 98% on benchmark datasets such as NSL-KDD and CICIDS2017, the DNN model has proven capable of effectively distinguishing between normal and malicious traffic patterns. Its ability to automatically extract complex features, combined with strong generalization to new attack types, makes it a promising alternative to traditional detection mechanisms that rely heavily on pre-defined signatures.

In addition, the scalability and computational efficiency of DNN models, particularly when implemented on GPU-enabled systems, make them well-suited for real-time intrusion detection in large-scale environments. These findings emphasize the importance of adopting deep learning-based approaches in cybersecurity to address the growing complexity of network threats. Future research should focus on optimizing DNN architectures, integrating hybrid learning methods, and enhancing interpretability to further strengthen their practical implementation in intelligent, automated defense systems.

References

A. Dhablia et al., "Decision Systems in Cybersecurity: A Machine Learning Perspective," Smart Innovation, Systems and Technologies, vol. 422, pp. 475-485, 2025. DOI: https://doi.org/10.1007/978-981-96-0147-9_40.

A. Eddine, J. Farah, and K. Ouajdi, "Comparative study between ML approaches in Intrusion Detection Context," in Proc. IEEE Afro-Mediterranean Conf. on Artificial Intelligence (AMCAI), 2023, DOI: https://doi.org/10.1109/AMCAI59331.2023.10431511.

A. H. Ali et al., "Unveiling Machine Learning Strategies and Considerations in Intrusion Detection Systems: A Comprehensive Survey," Frontiers in Computer Science, vol. 6, art. 1387354, 2024. DOI: https://doi.org/10.3389/fcomp.2024.1387354.

A. H. Ali et al., "Unveiling Machine Learning Strategies and Considerations in Intrusion Detection Systems: A Comprehensive Survey," Frontiers in Computer Science, 2024. DOI: https://doi.org/10.3389/fcomp.2024.1387354.

A. R. Priambodo et al., "Optimizing Intrusion Detection: Hybrid Deep Learning Techniques for Class Imbalance Correction," ICITRI 2024, pp. 7-12, 2024. DOI: https://doi.org/10.1109/ICITRI62858.2024.10698997.

A. R. Priambodo et al., "Optimizing Intrusion Detection: Hybrid Deep Learning Techniques for Class Imbalance Correction," ICITRI 2024, pp. 7-12, 2024. DOI: https://doi.org/10.1109/ICITRI62858.2024.10698997.

A. Setiawan et al., "Network Intrusion Detection Using 1D Convolutional Neural Networks," ICE3IS 2024, pp. 415-419, 2024. DOI: https://doi.org/10.1109/ICE3IS62977.2024.10775512.

A. Shaikh and P. Gupta, "Dynamic Updating of Signatures for Improving the Performance of IDS," in Lecture Notes in Networks and Systems, vol. 444, pp. 659-673, 2022, DOI: https://doi.org/10.1007/978-981-19-2500-9_49.

A. Sheeba, N. Karthika, and R. K. Prathiksha, "Network intrusion detection system analytics using memory-based learning approaches," Proceedings of the 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS 2024), 2024. DOI: https://10.1109/ICKECS61492.2024.10616502.

B. Alsughayyir and A. M. Qamar, "Deep Learning-Based Network Attack Detection Using Convolutional and Recurrent Neural Networks," International Journal of Engineering Research and Technology, vol. 12, no. 12, pp. 3027-3303, 2019.

B. N. Shaker et al., "A Comparative Study of IDS-Based Deep Learning Models for IoT Network," ACM International Conference Proceeding Series, pp. 15-21, 2023. DOI: https://doi.org/10.1145/3603273.3635058.

B. Pavan et al., "Efficient Predictive Analysis for Intrusion Detection Using Recurrent Neural Network Compared Over Convolutional Neural Network with Better Accuracy," ICETAS 2024, 2024. DOI: https://doi.org/10.1109/ICETAS62372.2024.11120168.
B. Singh, C. Kaunert, and S. Chandra, "Relishing machine learning intelligence combating cyber threats," in Navigating Cyber Threats and Cybersecurity in the Software Industry, pp. 129-150, 2025, DOI: https://doi.org/10.4018/979-8-3693-6250-1.ch007.
C. Sekhar, P. H. Kumar, K. V. Rao, and M. H. M. Krishna Prasad, "A comparative study on network intrusion detection system using deep learning algorithms and enhancement of deep learning models using generative adversarial network (GAN)," Lecture Notes in Electrical Engineering, vol. 853, pp. 143-155, 2022. DOI: https://10.1007/978-981-16-9885-9_12.
D. J. Day, D. A. Flores, and H. S. Lallie, "CONDOR: A hybrid IDS to offer improved intrusion detection," in Proc. IEEE TrustCom, 2012, DOI: https://doi.org/10.1109/TrustCom.2012.110.
G. Prethija and J. Katiravan, "Machine Learning and Deep Learning Approaches for Intrusion Detection: A Comparative Study," Lecture Notes in Networks and Systems, vol. 311, pp. 75-95, 2022. DOI: https://doi.org/10.1007/978-981-16-5529-6_7.
G. Prethija and J. Katiravan, "Machine Learning and Deep Learning Approaches for Intrusion Detection: A Comparative Study," Lecture Notes in Networks and Systems, vol. 311, pp. 75-95, 2022. DOI: https://doi.org/10.1007/978-981-16-5529-6_7.
I. P. Joshi and V. K. Shandilya, "Anomaly detection and threat intelligence with machine learning," in Exploiting Machine Learning for Robust Security, pp. 69-97, 2025, DOI: https://doi.org/10.4018/979-8-3693-7758-1.ch004.
J. Cui et al., "Comparative Study of CNN and RNN for Deep Learning Based Intrusion Detection System," Lecture Notes in Computer Science, vol. 11067, pp. 159-170, 2018. DOI: https://doi.org/10.1007/978-3-030-00018-9_15.
K. Zhang, T. Li, and X. Zhao, "Real-Time Network Intrusion Detection using Parallel Deep Learning Models," Computers & Security, vol. 133, p. 103502, 2024, DOI: https://doi.org/10.1016/j.cose.2024.103502.
L. D'hooge et al., "Castles Built on Sand: Observations from Classifying Academic Cybersecurity Datasets with Minimalist Methods," IoTBDS Proceedings, 2023, pp. 61-72. DOI: https://doi.org/10.5220/0011853300003482.
L. L. Mutembei et al., "Deep Learning-Based Network Intrusion Detection Systems: A Systematic Literature Review," Communications in Computer and Information Science, vol. 2326, pp. 207-234, 2025. DOI: https://doi.org/10.1007/978-3-031-78255-8_13.
L. Singh and H. Jahankhani, "An approach of applying, adapting machine learning into the IDS and IPS component to improve its effectiveness and its efficiency," Advanced Sciences and Technologies for Security Applications, pp. 43-71, 2021. DOI: https://10.1007/978-3-030-88040-8_2.
L. Singh and H. Jahankhani, "Applying Machine Learning to Improve IDS Effectiveness," in Advanced Sciences and Technologies for Security Applications, pp. 43-71, 2021, DOI: https://doi.org/10.1007/978-3-030-88040-8_2.
M. A. Al-Absi, H. R'Bigui, and A. A. Al-Absi, "Deep Learning and Machine Learning Algorithms in Cyber Security," in Lecture Notes in Networks and Systems, vol. 914, pp. 271-279, 2024, DOI: https://doi.org/10.1007/978-981-97-0573-3_22.
M. Dhablia et al., "Decision Systems in Cybersecurity: A Machine Learning Perspective," Smart Innovation, Systems and Technologies, vol. 422, pp. 475-485, 2025. DOI: https://doi.org/10.1007/978-981-96-0147-9_40.
M. Dhablia et al., "Intrusion Detection System Using Machine Learning," Lecture Notes in Networks and Systems, vol. 893, pp. 387-400, 2024. DOI: https://doi.org/10.1007/978-981-99-9518-9_28.
N. Roy et al., "The Evolving Landscape of Network Threats: Classification, Defense Challenges, and Future Directions," in Proc. 8th Int. Conf. on Computing Methodologies and Communication (ICCMC), 2025, pp. 504-510, DOI: https://doi.org/10.1109/ICCMC65190.2025.11140963.
O. J. Mebawondu et al., "Network Intrusion Detection System Using Deep Learning Paradigm," NIGERCON 2024, 2024. DOI: https://doi.org/10.1109/NIGERCON62786.2024.10927024.
P. Agarwal et al., "Comparative Analysis of Machine Learning Algorithms for Intrusion Detection System," Signals and Communication Technology, pp. 151-162, 2023. DOI: https://doi.org/10.1007/978-3-031-29713-7_8.
P. Madhuri, D. David, B. Philomon, and K. K. S. Reddy, "Network intrusion detection system using random forest," Computational Methods in Science and Technology - Proceedings of the 4th International Conference on Computational Methods in Science and Technology (ICCMST 2024), vol. 2, pp. 277-282, 2025. DOI: https://10.1201/9781003561651-39.
R. Kavitha and S. Amutha, "Performance Analysis of Deep Neural Network and LSTM Models for Secure Network Intrusion Detection System," ICCCMLA 2022, pp. 390-396, 2022. DOI: https://doi.org/10.1109/ICCCMLA56841.2022.9989253.
R. Knights and E. Morris, "Move to intelligence-driven security," Network Security, vol. 2015, no. 8, pp. 15-18, 2015, DOI: https://doi.org/10.1016/S1353-4858(15)30071-4.
R. Vaarandi and A. Guerra-Manzanares, "Network IDS alert classification with active learning techniques," Journal of Information Security and Applications, vol. 81, art. no. 103687, 2024. DOI: https://10.1016/j.jisa.2023.103687.
S. Gupta and R. Tiwari, "Enhancing Intrusion Detection with Deep Neural Networks," IEEE Access, vol. 12, pp. 32145-32159, 2024, DOI: https://doi.org/10.1109/ACCESS.2024.3389012.
S. Hemalatha et al., "Deep Learning Approaches for Intrusion Detection with Emerging Cybersecurity Challenges," ICSCNA 2023, pp. 1522-1529, 2023. DOI: https://doi.org/10.1109/ICSCNA58489.2023.10370556.
S. Hutchinson, J. Cowley, and J. Ellis, "Improving signature-based packet analysis efficiency: A case study," in Proc. Int. Conf. on Cyber Warfare and Security (ICCWS), 2018.
T. Jahan et al., "Methods and Techniques of Cybersecurity Intrusion Detection: Supervised Machine Learning," Cognitive Science and Technology, pp. 691-709, 2025. DOI: https://doi.org/10.1007/978-981-97-9262-7_60.
V. Anbumani et al., "Network Intrusion Detection System Using Optimized Feature Selection," AIMLA 2024, 2024. DOI: https://doi.org/10.1109/AIMLA59606.2024.10531381.
V. Hamolia et al., "Intrusion Detection in Computer Networks Using Latent Space Representation and Machine Learning," Int. J. of Computing, vol. 19, no. 3, pp. 442-448, 2020, DOI: https://doi.org/10.47839/IJC.19.3.1893.

V. K. Navya et al., "Intrusion Detection System Using Deep Neural Networks (DNN)," ICAECA 2021, 2021. DOI: https://doi.org/10.1109/ICAECA52838.2021.9675513.

V. Reddy et al., "Artificial Intelligence Based Intrusion Detection Systems," ICMNWC 2024, 2024. DOI: https://doi.org/10.1109/ICMNWC63764.2024.10872055.

Y. EL Yamani, Y. Baddi, and N. EL Kamoun, "A survey on ML and DL in botnet attack detection and prevention," Journal of Reliable Intelligent Environments, vol. 10, no. 4, pp. 431-448, 2024, DOI: https://doi.org/10.1007/s40860-024-00226-y.

Y. R. Gumma and S. Peram, "Review of Cybercrime Detection Approaches using ML and DL Techniques," in Proc. 3rd Int. Conf. on Applied Artificial Intelligence and Computing (ICAAIC), 2024, pp. 772-779, DOI: https://doi.org/10.1109/ICAAIC60222.2024.10575058.