Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

AI-Based Network Intrusion Detection System Using Machine Learning

[Ms.B K.Sweta], [Nishadharshini .S , Sowmya .R, Vipin. R]
1[Associate Professor], Department of [Computer Science & Applications], [, Sri Krishna Arts and Science College], [Coimbatore]

2[Student III CSA A], Department of [Computer Science & Applications], [Sri Krishna Arts and Science College], [Coimbatore]

Abstract— The rapid expansion of digital networks and internet-connected devices has significantly increased the exposure of organizations to sophisticated cyber-attacks. Traditional signature-based Intrusion Detection Systems (IDS) struggle to identify novel and evolving threats due to their reliance on predefined attack patterns. This paper proposes an AI-based Network Intrusion Detection System (NIDS) that leverages machine learning algorithms to detect malicious network traffic with high accuracy and low false-positive rates. The proposed system employs data preprocessing, feature selection, and classification techniques including Decision Tree, Random Forest, Support Vector Machine, Naïve Bayes, and Artificial Neural Networks, trained and evaluated on benchmark intrusion detection datasets. Experimental results demonstrate that ensemble-based approaches, particularly Random Forest, achieve superior detection accuracy compared to conventional methods. The study concludes that integrating machine learning into intrusion detection significantly enhances the ability of networks to identify both known and previously unseen attacks in real time.

Keywords— Network Intrusion Detection System, Machine Learning, Cybersecurity, Random Forest, Support Vector Machine, Anomaly Detection, Network Security.

I. Introduction

With the exponential growth of internet-based services, cloud computing, and IoT devices, network infrastructures have become prime targets for cybercriminals. Network Intrusion Detection Systems (NIDS) serve as a critical line of defense by continuously monitoring network traffic to identify unauthorized access, malware propagation, and anomalous behavior. Conventional IDS solutions primarily rely on signature-based detection, which matches incoming traffic against a database of known attack patterns. While effective against previously documented threats, such systems are inherently incapable of detecting zero-day attacks or subtle variations of existing threats.

Machine learning (ML) offers a promising alternative by enabling systems to learn patterns directly from data, thereby generalizing detection capabilities to previously unseen attack types. By training classifiers on large volumes of labeled network traffic, ML-based NIDS can distinguish between normal and malicious behavior with considerably greater flexibility than static rule-based systems. This paper presents the design, methodology, and evaluation of an AI-based NIDS that integrates multiple machine learning algorithms to improve detection accuracy, reduce false alarms, and adapt to evolving threat landscapes.

II. Literature Review

Numerous studies have explored the application of machine learning to intrusion detection. Early research focused on applying single classifiers such as Decision Trees and Naïve Bayes to benchmark datasets like KDD Cup 99 and

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

NSL-KDD, achieving moderate success but suffering from high false-positive rates on imbalanced data. Subsequent work introduced ensemble methods such as Random Forest and Gradient Boosting, which combine multiple weak learners to improve overall classification robustness.

More recent studies have investigated deep learning architectures, including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, for capturing complex temporal and spatial patterns in network traffic. While these approaches often yield higher accuracy, they require substantial computational resources and large labeled datasets, which may not always be feasible in real-world deployment scenarios. This paper builds upon existing literature by comparing traditional and ensemble machine learning classifiers to identify an approach that balances detection accuracy with computational efficiency.

III. Existing System and Limitations

Traditional NIDS solutions are broadly classified into signature-based and anomaly-based systems. Signature-based systems compare network packets against a predefined database of attack signatures, offering high precision for known threats but failing entirely against novel attacks. Anomaly-based systems establish a baseline of normal network behavior and flag deviations as potential intrusions; however, they are prone to high false-positive rates due to the natural variability of legitimate traffic.

Key limitations of existing systems include the inability to adapt to evolving attack strategies, dependency on manual signature updates, poor scalability with increasing network traffic volume, and limited capacity to detect sophisticated, low-and-slow attacks that mimic normal behavior. These limitations motivate the need for intelligent, self-learning detection mechanisms capable of continuously improving their detection capability.

IV. Proposed System

The proposed AI-based NIDS integrates machine learning classifiers into a structured detection pipeline consisting of data acquisition, preprocessing, feature selection, model training, and real-time classification. The system is designed to analyze network traffic flows and classify them as either normal or one of several attack categories, including Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R) attacks.

Unlike static rule-based systems, the proposed model continuously refines its decision boundaries through supervised learning on labeled datasets, enabling it to generalize detection capability to previously unseen but structurally similar attack patterns. The system further incorporates feature selection techniques to reduce dimensionality, thereby improving computational efficiency without compromising detection accuracy

.

V. System Architecture

The system architecture comprises four principal modules: (1) Data Collection Module, which captures raw network traffic using packet-capturing tools; (2) Preprocessing Module, which cleans, normalizes, and encodes categorical features into numerical representations; (3) Feature Selection Module, which employs statistical and correlation-based techniques to identify the most discriminative attributes; and (4) Classification Module, which applies trained machine learning models to categorize traffic as benign or malicious.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

The output of the classification module is forwarded to an alerting mechanism that notifies network administrators of detected intrusions in real time, enabling prompt mitigation actions. This modular design ensures that individual components can be updated or replaced independently as new algorithms or data sources become available.

VI. Methodology

A. Dataset Description

The proposed system is evaluated using the NSL-KDD dataset, a refined version of the original KDD Cup 99 dataset that eliminates redundant records and provides a more balanced distribution of attack and normal instances. The dataset contains 41 features describing network connections, along with a label indicating whether the connection is normal or belongs to one of four attack categories.

B. Data Preprocessing

Preprocessing steps include handling missing values, encoding categorical attributes such as protocol type and service using one-hot encoding, and normalizing numerical features using min-max scaling to ensure uniform contribution across all input dimensions during model training.

C. Feature Selection

To reduce dimensionality and eliminate redundant attributes, correlation-based feature selection and information gain ranking are applied. This step reduces the feature space while retaining the attributes most relevant to distinguishing between normal and malicious traffic, thereby improving both training speed and model generalization.

D. Machine Learning Algorithms

Five classification algorithms are implemented and compared in this study:

- Decision Tree (DT): A tree-structured classifier that splits data based on feature thresholds to form interpretable decision rules.
- Random Forest (RF): An ensemble of decision trees that aggregates predictions through majority voting to improve accuracy and reduce overfitting.
- Support Vector Machine (SVM): A classifier that identifies an optimal hyperplane to separate classes in high-dimensional feature space.
- Naïve Bayes (NB): A probabilistic classifier based on Bayes' theorem, assuming feature independence.
- Artificial Neural Network (ANN): A multi-layered network capable of learning complex non-linear relationships between input features and output classes.

VII. Implementation

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

The proposed models are implemented using Python with the scikit-learn and TensorFlow libraries. The dataset is split into 70% training and 30% testing subsets. Each classifier is trained using the same pre-processed feature set to ensure a fair comparison. Hyperparameter tuning is performed using grid search with 5-fold cross-validation to optimize each model's performance prior to final evaluation on the test set.

VIII. Results and Discussion

Table I summarizes the performance of each classifier in terms of accuracy, precision, recall, and F1-score. The Random Forest classifier achieved the highest overall accuracy of 98.7%, outperforming other algorithms due to its ensemble nature, which reduces variance and mitigates overfitting. The Artificial Neural Network also demonstrated strong performance, closely trailing Random Forest, while Naïve Bayes exhibited the lowest accuracy due to its independence assumption, which does not hold well for correlated network traffic features.

TABLE I. Performance Comparison of Machine Learning Classifiers

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	96.2	95.8	95.4	95.6
Random Forest	98.7	98.5	98.3	98.4
Support Vector Machine	95.1	94.6	94.0	94.3
Naïve Bayes	91.4	90.2	89.7	89.9
Artificial Neural Network	97.9	97.5	97.2	97.3

These results confirm that ensemble-based methods provide a favourable balance between detection accuracy and robustness against noisy or imbalanced data, making them well-suited for real-world intrusion detection deployment.

IX. Advantages of the Proposed System

- Improved detection accuracy for both known and previously unseen attack patterns.
- Reduced false-positive rates compared to traditional anomaly-based systems.
- Scalable architecture capable of handling high-volume network traffic.
- Modular design allowing easy integration of new algorithms and data sources.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

X. Future Enhancements

Future work will focus on incorporating deep learning architectures such as CNN and LSTM to capture temporal dependencies in network traffic, integrating real-time streaming data pipelines for online learning, and deploying the system within a distributed cloud environment to enhance scalability. Additionally, exploring explainable AI (XAI) techniques will help improve the transparency and interpretability of model decisions for network security analysts.

XI. Conclusion

This paper presented an AI-based Network Intrusion Detection System that leverages multiple machine learning algorithms to accurately classify network traffic as normal or malicious. Experimental evaluation on the NSL-KDD dataset demonstrated that ensemble-based classifiers, particularly Random Forest, achieve superior detection performance compared to traditional single-classifier approaches. The proposed system addresses key limitations of conventional signature-based and anomaly-based IDS by offering adaptive, data-driven detection capable of identifying evolving cyber threats. Future enhancements involving deep learning and real-time streaming analytics are expected to further strengthen the system's applicability in modern network security environments.

Acknowledgment

The authors would like to express their sincere gratitude to the Department of Computer Applications, Sri Krishna Arts and Science College, Coimbatore, for providing the resources and support necessary to carry out this research.

References

[1] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Computational Intelligence for Security and Defense Applications, 2009, pp. 1–6.

[2] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. Military Communications and Information Systems Conf., 2015, pp. 1–6.

[3] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[4] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525–41550, 2019.

[5] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[6] C. Cortes and V. Vapnik, "Support-vector networks," Machine Learning, vol. 20, no. 3, pp. 273–297, 1995.

[7] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018.

Indo Asian Journal of Management and Entrepreneurship (IAJOME)
‖ ISSN: 2319-2992, Impact Factor 5.007 ‖
‖ Peer-Reviewed | Open Access | International Journal ‖
‖ Volume: 17 | Issue: 07 | July 2026 | www.iajome.com ‖

[8] S. Revathi and A. Malathi, "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection," International Journal of Engineering Research & Technology, vol. 2, no. 12, pp. 1848–1853, 2013.

[9] T. Janarthanan and S. Zargari, "Feature selection in UNSW-NB15 and KDDCUP'99 datasets," in Proc. IEEE Int. Symp. Industrial Electronics, 2017, pp. 1881–1886.

[10] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 686–728, 2019.