IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14627

Intrusion Detection System

Diana Prince Chandran Jayasingh[1], U Vinayaka Prabhu[2], Adithya P[3], Prajvith P[4], Charan B[5]

Associate Professor, Department of CS&D, K S Institute of Technology, Bengaluru, India[1]

Department of CS&D, K S Institute of Technology, Bengaluru, India[2]

Department of CS&D, K S Institute of Technology, Bengaluru, India[3]

Department of CS&D, K S Institute of Technology, Bengaluru, India[4]

Department of CS&D, K S Institute of Technology, Bengaluru, India[5]

Abstract: This project presents the development of an Intrusion Detection System (IDS) using machine learning techniques to identify and classify potential threats in network traffic. Leveraging the NSL-KDD dataset, which provides a refined and widely accepted benchmark for network intrusion detection research, the system is trained to detect various types of attacks such as DoS, probe, R2L, and U2R. The project involves preprocessing the dataset, feature selection, and applying supervised learning algorithms like Decision Trees, Random Forest, and Support Vector Machines to build an accurate classification model. The goal is to enhance network security by enabling early detection of malicious activities and reducing false positive rates, ultimately providing a reliable and scalable solution for real-time threat detection in modern network environments.

Keywords: Intrusion Detection System (IDS), Machine Learning, NSL-KDD Dataset, Network Security, Supervised Learning, Random Forest, Feature Selection, Anomaly Detection, Cybersecurity, Attack Classification.

I. INTRODUCTION

In today's digital era, the rapid expansion of computer networks and internet connectivity has brought immense benefits but also increased the vulnerability of systems to various types of cyber threats. Organizations, governments, and individuals face the constant risk of cyberattacks such as Denial of Service (DoS), data breaches, and unauthorized access, which can lead to severe financial and reputational damage. As the complexity and frequency of these attacks grow, traditional security mechanisms like firewalls and antivirus software have proven insufficient in identifying and preventing sophisticated threats. Therefore, there is a pressing need for intelligent, automated systems that can detect intrusions effectively and adapt to evolving attack patterns.

An Intrusion Detection System (IDS) serves as a vital component of network security by monitoring network traffic for suspicious activity and flagging potential threats. IDS can be classified into signature-based and anomaly-based systems. While signature-based IDS is effective against known threats, it fails to detect new or evolving attacks. In contrast, anomaly- based IDS, especially those powered by machine learning, offer the ability to learn normal behavior patterns and identify previously unseen intrusions. This makes machine learning a promising approach to enhance the capability and accuracy of intrusion detection systems.

This project focuses on designing and implementing a machine learning-based IDS using the NSL-KDD dataset, a benchmark dataset derived from the original KDD Cup 99 dataset. The NSL-KDD dataset addresses several issues found in its predecessor, such as redundant records and imbalanced class distribution, making it more suitable for training and evaluating modern machine learning models. The dataset includes various types of network traffic instances categorized into normal and attack classes, allowing the model to learn and distinguish between benign and malicious behavior.

The methodology involves several stages, starting with data preprocessing to clean and normalize the input data, followed by feature selection to identify the most relevant attributes contributing to intrusion detection. Multiple supervised machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) are trained and evaluated on the dataset. Performance metrics like accuracy, precision, recall, and F1- score are used to compare model effectiveness and select the most suitable one for deployment.

Ultimately, this project aims to provide a robust, scalable, and accurate intrusion detection system that can be integrated into real-time network environments. By leveraging the power of machine learning, the system can significantly reduce false positives and detect a wide range of cyber threats, including novel attacks.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14627

This contributes to building a more secure and resilient cyberspace, protecting sensitive data and critical infrastructure from unauthorized access and malicious exploitation.

II. LITERATURE SURVEY

Intrusion Detection Systems (IDS) have been the subject of extensive research in recent years, particularly with the advent of machine learning and artificial intelligence methods. Various studies have utilized the NSL-KDD dataset to evaluate the performance of different algorithms for detecting network anomalies and attacks.

In [1], the authors implemented a comparative study of traditional classification algorithms such as Naïve Bayes, Decision Tree, and Random Forest using the NSL-KDD dataset.

The study concluded that ensemble learning methods like Random Forest significantly outperform individual classifiers in terms of detection accuracy and robustness against overfitting. However, the model's performance was still affected by the imbalance of certain attack classes in the dataset.

The work in [2] introduced a hybrid IDS that combines Support Vector Machine (SVM) with Genetic Algorithms (GA) for feature selection. By optimizing the feature subset, the system achieved improved accuracy and reduced computational complexity. The approach showed promising results in detecting rare attack types, but required high processing power and tuning for scalability in real-time environments.

In [3], a deep learning-based approach using a multi-layer perceptron (MLP) was proposed to learn complex patterns in the network traffic data. The deep neural network (DNN) achieved higher detection rates for both known and unknown attacks compared to shallow machine learning models. Despite its effectiveness, the model faced challenges in terms of training time and interpretability.

Another study [4] utilized the K-Nearest Neighbors (KNN) algorithm for anomaly detection. The simplicity of KNN allowed for easier implementation, but its performance was highly dependent on the selection of the value of k and the distance metric. Moreover, KNN struggled with large datasets due to its computational overhead during prediction.

In [5], the authors developed an IDS using a combination of feature engineering and ensemble methods. By employing Principal Component Analysis (PCA) for dimensionality reduction and combining Gradient Boosting and AdaBoost classifiers, the system achieved a balanced trade-off between precision and recall. However, the use of PCA led to the loss of some interpretability in the transformed features.

These studies demonstrate that while various machine learning models have proven effective in detecting intrusions, each comes with trade-offs in terms of accuracy, computational efficiency, scalability, and ease of deployment. The NSL-KDD dataset continues to serve as a standard benchmark for evaluating IDS performance, though ongoing research is exploring more recent and real-time datasets for enhanced relevance to modern cyber threats.

III. METHODOLOGY

The proposed Intrusion Detection System (IDS) employs supervised machine learning techniques to detect and classify malicious network traffic using the NSL-KDD dataset. The methodology encompasses several critical stages: data preprocessing, feature selection, model training, evaluation, and performance comparison. A comprehensive approach is adopted to ensure the detection of both known and unknown attacks with high accuracy and minimal false positives.

A. Data Preprocessing

The raw NSL-KDD dataset includes 41 features and one label indicating the type of connection (normal or specific attack type). To prepare the data for machine learning models, preprocessing steps are applied. These include handling categorical variables (e.g., protocol_type, service, and flag) through one-hot encoding, normalizing numerical values using Min-Max scaling, and mapping target class labels into binary or multi-class formats depending on the experiment. The dataset is then split into training and testing sets to evaluate model generalizability.

B. Feature Selection

Feature selection plays a vital role in enhancing model performance and reducing computational overhead. Correlation-based Feature Selection (CFS) and Recursive Feature Elimination (RFE) are employed to identify the most informative features.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14627

These techniques help eliminate redundant and irrelevant features that may introduce noise or bias into the learning process, ensuring efficient and faster model training.

C. Model Training

Multiple machine learning algorithms are utilized to train the IDS model, including Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN). Each classifier is trained on the preprocessed and feature-reduced dataset. Cross-validation is applied to prevent overfitting and ensure robust performance. The training phase aims to build a model capable of learning patterns that distinguish between normal and intrusive behavior in the network data.

D. Evaluation Metrics

To evaluate the performance of the trained models, various metrics are used, including accuracy, precision, recall, F1-score, and confusion matrix. These metrics provide a balanced assessment of the classifier's ability to detect intrusions correctly while minimizing false positives and negatives. Special attention is given to recall and F1-score due to their importance in intrusion detection, where missing an attack can have severe consequences.

E. System Architecture

The overall system architecture consists of data input, preprocessing and feature selection module, machine learning-based detection engine, and result visualization dashboard. Once trained, the detection engine can be deployed in a simulated or real-time network environment to monitor traffic and flag potential intrusions. The modular design ensures scalability and adaptability to new datasets or attack vectors.

IV. RESULT

The performance of the proposed Intrusion Detection System was evaluated using the NSL-KDD dataset. Four supervised machine learning algorithms—Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN)—were implemented and tested. Each model was assessed based on classification accuracy, precision, recall, and F1-score to determine its effectiveness in identifying normal and intrusive network traffic.

After data preprocessing and feature selection, the dataset was split into 80% training and 20% testing. The Decision Tree classifier achieved an accuracy of 89.24%, with a precision of 88.76%, recall of 89.13%, and an F1-score of 88.94%. The Random Forest classifier outperformed the other models, reaching an accuracy of 92.81%, a precision of 91.47%, recall of 93.22%, and an F1-score of 92.33%. This highlights the robustness of ensemble learning methods for complex classification tasks in intrusion detection.

The Support Vector Machine demonstrated comparatively lower performance with an accuracy of 86.02%, mainly due to its sensitivity to class imbalance and limited scalability on larger datasets. The KNN model, while simple and interpretable, achieved an accuracy of 85.64% and showed a tendency to overfit due to its non-parametric nature. Nonetheless, it was effective in detecting specific classes of attacks with reasonable precision.
Table I summarizes the comparative results of all four algorithms on the NSL-KDD test set.

Table I: Performance Metrics of Classifiers on NSL-KDD Dataset

Algorith m	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Decision Tree (DT)	89.24	88.76	89.13	88.94
Random Forest (RF)	**92.81**	**91.47**	**93.22**	**92.33**
SVM	86.02	85.11	86.70	85.90
KNN	85.64	84.95	85.43	85.19

From the results, it is evident that the Random Forest classifier delivers the best trade-off between accuracy and generalization for intrusion detection on the NSL-KDD dataset. Its ability to handle high-dimensional data and mitigate overfitting makes it a suitable choice for real-time deployment in network security systems.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14627

V. CONCLUSION

In this project, a machine learning-based Intrusion Detection System was developed and evaluated using the NSL-KDD dataset. Through careful data preprocessing, feature selection, and implementation of various supervised learning algorithms, the system was able to effectively classify network traffic normal and attack categories. Among the models tested, the Random Forest classifier demonstrated superior performance in terms of accuracy, precision, recall, and F1-score, making it the most reliable choice for detecting diverse types of intrusions. The results highlight the capability of machine learning to enhance cybersecurity by automatically learning from data and identifying complex attack patterns.

Despite the promising results, several challenges remain, including the need to address class imbalance, detect zero-day attacks, and enable real-time intrusion detection in dynamic network environments. Future enhancements could include the integration of deep learning techniques, continuous learning mechanisms, and deployment in real-world environments to test robustness and adaptability. Overall, this work contributes toward building intelligent and scalable IDS solutions that can significantly strengthen network defense mechanisms against evolving cyber threats.

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 Symposium on Computational Intelligence for Security and Defense Applications*, 2009.
[2]. S. Revathi and Dr. A. Malathi, "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection," *International Journal of Engineering and Technology*, vol. 5, no. 6, pp. 231-235, 2013.
[3]. D. Kumar and K. Suresh, "Efficient Intrusion Detection System using Random Forest Classifier," in *Proc. International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*,2017.
[4]. M. Gandhi, N. Rathod, and P. Shetty, "Comparison of Various Machine Learning Algorithms Using NSL-KDD Dataset for Intrusion Detection," *International Journal of Computer Applications*, vol. 180, no. 45, 2018.
[5]. N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)," in *Proc. Military Communications and Information Systems Conference (MilCIS)*, 2015.