International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A Deep Learning – Based Intrusion Detection System for Network Traffic Classification Using NSL – KDD Dataset

Priti Pradeep Khedekar *, Sagar Vyavahare**
*(Computer Science, CKT ACS College, New Panvel
Email: khedekarp958@gmail.com)
** (Computer Science, CKT ACS College, New Panvel
Email : gns.sagar@gmail.com)

----------**********----------

Abstract:
This research presents a comprehensive deep learning–based Intrusion Detection System (IDS) using an Artificial Neural Network (ANN) trained on the NSL-KDD dataset. The proposed model achieved an accuracy of 78.38% and an ROC-AUC score of 0.864, indicating strong classification capability. A comparative analysis with Random Forest and Gradient Boosting models highlights the robustness and effectiveness of deep learning for detecting network anomalies.The study also focuses on essential preprocessing techniques, class imbalance handling, feature engineering, and comprehensive performance evaluation metrics to improve detection reliability.

Keywords — **Intrusion Detection System, Artificial Neural Network, NSL-KDD, Deep Learning, Cyber Security, Network Anomaly Detection.**

----------**********----------

I. INTRODUCTION
The growth of network technologies and the internet has increased the risk of cyber-attacks. Today, organizations use computer networks for communication, data storage, online transactions, and many important operations. Because of this heavy dependence on digital systems, networks have become major targets for attackers [1]. Common cyber-attacks such as Denial-of-Service (DoS), probing attacks, Remote-to-Local (R2L), and User-to-Root (U2R) can cause serious problems like data loss, service interruption, and financial damage [2].

Intrusion Detection Systems (IDS) are used to monitor network traffic and detect suspicious activities [3]. Traditional IDS methods are mostly rule-based or signature-based. They work by comparing network activity with known attack patterns. These systems are effective for detecting known attacks, but they fail to detect new or unknown attacks and require regular updates to keep up with emerging threats [4].

To overcome these limitations, machine learning and deep learning techniques are being used for intrusion detection [5]. These techniques learn patterns from data and can identify unusual behaviour without depending only on predefined rules. Artificial Neural Networks (ANN), a type of deep learning model, can understand complex patterns in network traffic data. Therefore, deep learning-based IDS can improve detection accuracy and provide better protection against modern cyber threats [6].

II. LITERATURE REVIEW
Earlier research in intrusion detection mainly focused on traditional machine learning algorithms such as Support Vector Machines (SVM), Decision Trees (DT), k-Nearest Neighbours (KNN), and Naïve Bayes classifiers. These techniques were widely adopted because they are relatively simple to implement and provide good classification performance for detecting known attacks. Studies based on benchmark datasets such as KDD Cup 99 demonstrated that algorithms like SVM and Decision Trees can effectively classify network traffic

into normal and malicious categories [2]. However, traditional machine learning models often require manual feature selection and domain knowledge to identify relevant input attributes. Moreover, these models may struggle when dealing with large-scale network traffic data containing complex and non-linear attack patterns [4]. As network environments continue to evolve, the limitations of signature-based and conventional machine learning approaches become more evident [3]. In recent years, deep learning techniques have gained significant attention in the field of intrusion detection. Artificial Neural Networks (ANN), which are inspired by the structure of the human brain, are capable of learning complex and nonlinear relationships directly from data [6]. Unlike traditional approaches, deep learning models can automatically extract important features from raw network traffic, reducing the dependence on manual feature engineering. This capability improves their effectiveness in identifying both known and previously unseen attacks. Research indicates that advanced learning-based approaches enhance detection accuracy and adaptability compared to conventional systems [5]. Therefore, deep learning-based IDS models provide a more scalable and robust solution for protecting modern network infrastructures against sophisticated cyber threats [1].

III. MATERIALS AND METHODS

A. DATASET DESCRIPTION

The study utilized the **NSL-KDD dataset**, an improved version of the KDD Cup 99 dataset that removes redundant records and provides better evaluation for intrusion detection systems [2]. The dataset consists of network traffic records labelled Your paper must use a page size corresponding to as normal or attack categories, enabling supervised learning. The use of standardized datasets ensures consistency and comparability with previous IDS research studies [3], [4].

B. DATA PREPROCESSING

Before training the model, data preprocessing was carried out to enhance model efficiency and reliability. Feature scaling was applied to normalize the input attributes into a similar numerical range, as neural networks perform better when feature magnitudes are consistent [6]. Proper preprocessing improves convergence speed and model stability. The dataset was then divided into training and testing subsets to evaluate the generalization capability of the proposed model..

C. MODEL ARCHITECTURE

An Artificial Neural Network (ANN) was implemented as the classification model due to its capability to learn complex and nonlinear connected (dense) hidden layers to capture intricate traffic patterns. The Rectified Linear Unit (ReLU) activation function was applied in hidden layers to introduce nonlinearity and enhance computational efficiency. Dropout regularization was incorporated to minimize overfitting and improve the robustness of the model.

D. MODEL TRAINING

The ANN model was trained using the Adam optimization algorithm, which provides adaptive learning rates and ensures efficient convergence during training. Binary cross-entropy was selected as the loss function because the problem involves binary classification between normal and malicious traffic. The training methodology aligns with established machine learning-based intrusion detection approaches discussed in prior studies [1], [5].

E. PERFORMANCE EVALUATION

To assess the effectiveness of the proposed intrusion detection system, standard evaluation metrics were employed. These included accuracy, precision, recall, F1-score, and Receiver Operating Characteristic – Area Under Curve (ROC-AUC). These performance measures are commonly used in intrusion detection research to evaluate detection capability, classification balance, and false alarm rates [3], [4].

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed Artificial Neural Network (ANN) model achieved an accuracy of 78.38% on the test dataset, demonstrating effective classification of network traffic. The ROC-AUC score of 0.864 indicates strong capability in distinguishing between

normal and attack traffic, highlighting the strength of deep learning models in capturing complex patterns [6]. The confusion matrix shows that most instances were correctly classified, although some false negatives were observed in attack detection. The use of evaluation metrics such as accuracy, confusion matrix, and ROC-AUC follows standard intrusion detection assessment practices [3], [4]. Overall, the results confirm that the ANN-based approach is effective for intrusion detection, consistent with prior machine learning-based IDS research [1], [5].

Figure 1: ROC Curve for ANN Intrusion Detection Model

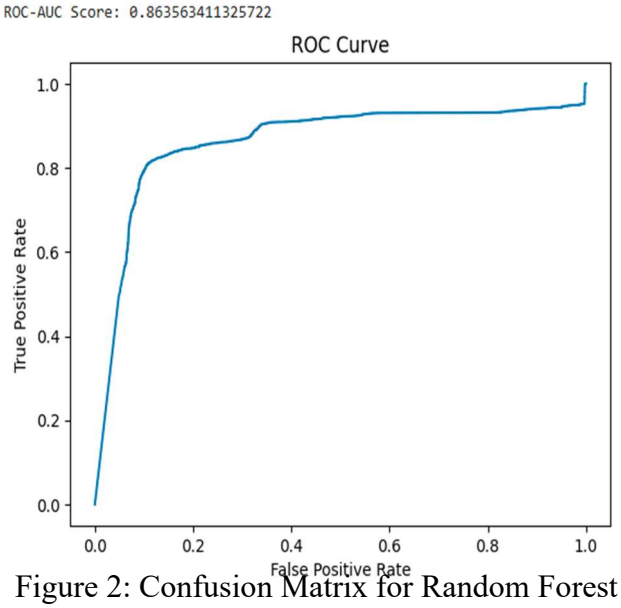
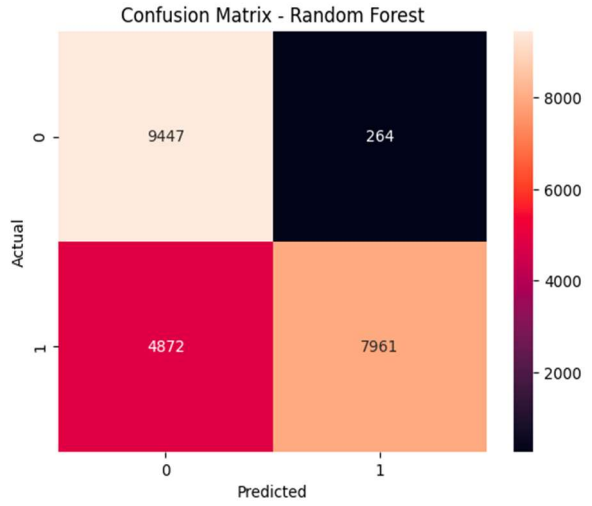


Figure 2: Confusion Matrix for Random Forest Model



Figures 1 and 2 illustrate the ROC curve and confusion matrix, which demonstrate the classification performance and detection capability of the proposed IDS model.

V. MODEL COMPARISON

Model	Accuracy
Artificial Neural Network	78.38%
Random Forest	77.24%
Gradient Boosting	80.72%

VI. CONCLUSION

This study demonstrates that deep learning techniques, particularly Artificial Neural Networks (ANN), are effective for intrusion detection tasks. The proposed model successfully classified normal and malicious network traffic with satisfactory accuracy and strong overall performance These findings highlight the capability of deep learning models to capture complex and nonlinear traffic patterns, thereby improving detection performance compared to traditional intrusion detection approaches [6]. The results are consistent with established intrusion detection frameworks and machine learning-based IDS methodologies discussed in prior research [1], [3], [5].

For future work, more advanced deep learning architectures such as Long Short-Term Memory (LSTM) networks can be explored to better analyse sequential and time-dependent network traffic patterns. Additionally, implementing the proposed model in real-time environments would enhance its practical applicability in operational network security systems. Continuous model refinement and adaptation to evolving cyber threats are essential for maintaining effective intrusion detection performance [4].

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Department of Computer Science,

CKT ACS College, New Panvel, for their guidance, support, and encouragement throughout the completion of this research work.

REFERENCES

[1] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson, 2017.

[2] M. Tavallaee et al., "A Detailed Analysis of the KDD CUP 99 Data Set," Proc. IEEE *Symposium on Computational Intelligence for Security and defence Applications (CISDA)*, 2009.

[3] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, 2007.

[4] S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," Technical Report, Chalmers University, 2000.

[5] S. Mukkamala, A. Sung, and A. Abraham, "Intrusion Detection Using Ensemble of Soft Computing Paradigms," Journal of Network and Computer Applications, 2005.

[6] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, pp. 436–444, 2015.

