iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Intrusion Detection System Using Improved Convolution Neural Network

Sharana H G[1], Prakash O. Sarangamath[2]
Department of MCA Ballari Institute of Technology and Management Ballari

Abstract: ***In the ever-evolving landscape of cybersecurity, the rapid proliferation of network attacks—ranging from simple port scans to sophisticated Advanced Persistent identification of malicious activity within network traffic has become critical. Traditional intrusion detection systems (IDS) often rely on signature-based or shallow learning techniques, which can be ineffective against novel or obfuscated attacks. This research presents an improved Convolutional Neural Network (CNN)-based An Intrusion Detection System (IDS) is a security tool designed to monitor network or system activity for malicious events or policy violations. The core purpose of an IDS is to act as a digital watchdog, identifying potential threats and alerting administrators. detection accuracy while maintaining computational efficiency. The proposed model introduces architectural modifications to standard CNNs, including optimized kernel sizes, adaptive pooling strategies, and feature fusion techniques to better capture temporal and spatial patterns in network traffic data.***

I. INTRODUCTION

The proliferation of digital infrastructure has made robust cybersecurity a necessity, but traditional Intrusion Detection Systems (IDS) are increasingly inadequate against modern, sophisticated threats. These conventional methods, which rely on predefined signatures and rules, are effective for known attacks but fail to identify new and evolving threats. This has led to a significant shift towards using machine learning and deep learning to develop more adaptive and intelligent IDS solutions. Among these advanced techniques, Convolutional Neural Networks (CNNs) have shown particular promise. While originally celebrated for their success in image processing, CNNs possess a unique ability to extract intricate patterns and hierarchical features from data, a capability that can be effectively adapted for network traffic analysis. To overcome the limitations of standard CNNs in handling the temporal and structural complexity of network data, an improved CNN-based IDS is proposed. This system begins with a specialized data preprocessing step that converts raw network flows into a structured format that a CNN can easily interpret. The core innovation lies in enhancing the CNN's architecture itself. By incorporating architectural improvements such as deeper layers, optimized filter sizes, and custom pooling strategies, the model can learn more complex and nuanced representations of traffic patterns. This tailored design allows the system to not only accurately detect established threats but also to generalize and identify previously unseen attacks. The result is a more resilient and powerful IDS that can keep pace with the dynamic nature of cyber threats, providing a crucial layer of defense for modern networks.

II. LITERATURE SURVEY

In modern cybersecurity, traditional Intrusion Detection Systems (IDS), which rely on predefined signatures to spot known threats, are increasingly ineffective against new or slightly altered attacks. This limitation has paved the way for the adoption of machine learning (ML) techniques. While early ML models like Support Vector Machines (SVMs) and Random Forests brought greater adaptability, they often required a laborious process of manual feature engineering and struggled with the vast, complex nature of network data. The emergence of deep learning has introduced Convolutional Neural Networks (CNNs) as a more advanced solution. Initially designed for image recognition, CNNs have been adapted to analyze network traffic by converting data into a visual or sequential format. This approach allows the models to automatically learn intricate patterns from raw data, bypassing the need for manual feature engineering. However, initial CNN models faced their own hurdles, as they weren't optimized for the temporal dependencies and irregular nature of network traffic. To overcome these challenges, the field has moved towards creating more sophisticated and specialized CNN architectures. Researchers have developed improvements such as 1D CNNs for analyzing sequential packet data and hybrid models that combine the spatial feature extraction of CNNs with the temporal analysis capabilities of LSTMs (Long Short-Term Memory networks) or GRUs (Gated Recurrent Units). Additionally, the use of attention mechanisms helps the network focus on the most critical parts of the data. Improvements have also been made to data representation itself, like transforming packet flows into image- like matrices to better suit CNN processing.

The development and evaluation of these advanced models are largely supported by publicly available datasets, such as CICIDS2017 and UNSW-NB15, which serve as crucial benchmarks for measuring their effectiveness.

III. METHODOLOGY

The proposed Intrusion Detection System (IDS) leverages an improved Convolutional Neural Network (CNN) specifically designed for analyzing and classifying network traffic. The process follows a structured five-phase methodology.

1) Data Preparation: The initial phase involves obtaining network traffic data from publicly available datasets like NSL-KDD or CICIDS2017. This data is preprocessed to handle missing values, encode non-numerical features, and normalize continuous values. Crucially, techniques like SMOTE are used to address class imbalance, ensuring the model can effectively detect rare attack types.

2) Data Transformation: Since CNNs require a grid-like input, the tabular network data is transformed. This can be done by reshaping each network record into a 1D array, which allows the CNN to identify spatial correlations between features within a single data point.

3) Improved CNN Architecture: The core of the system is a customized CNN. It uses multiple 1D convolutional layers to extract both local and broad patterns from the data. Key improvements include the use of residual connections to prevent training issues in deeper networks, batch normalization to stabilize the learning process, and dropout layers to combat overfitting. The final layers use a softmax or sigmoid activation to classify traffic as normal or malicious

4) Training and Evaluation: The model is trained on the prepared dataset using standard deep learning practices. An Adam optimizer is employed to speed up training, and the model's performance is rigorously measured using metrics like accuracy, precision, recall, and F1-score. Early stopping and model checkpointing are used to ensure the best- performing version of the model is saved.

5) Performance Analysis: The final phase involves a comparative analysis of the improved CNN's performance against other models. The system's effectiveness is evaluated by its ability to detect both known and unknown attacks, its false alarm rate, and its inference speed, which is a crucial factor for real-time application.

IV. SYSTEM IMPLEMENTATION

The implementation of an improved Convolutional Neural Network (CNN)-based Intrusion Detection System (IDS) is a comprehensive process that merges network security with deep learning. The system's architecture is a multi-stage pipeline, typically built using Python along with frameworks like TensorFlow or PyTorch. The first step involves Dataset Integration, where benchmark datasets such as NSL-KDD or CICIDS2017 are loaded using libraries like Pandas to provide the raw training data.

Next, the Data Preprocessing Module takes this raw data and prepares it for the CNN. This involves essential steps like cleaning the data to handle inconsistencies, encoding categorical features (like protocol types) into a numerical format, and normalizing all numerical values to a consistent range. A crucial step unique to this approach is reshaping the data into a 1D vector, which allows the CNN to treat the network features as a sequence for spatial analysis.

The core of the system is the CNN Model Construction. The architecture is designed with multiple 1D convolutional layers with varying filter sizes, enabling the network to capture different feature patterns within the data. These layers are followed by Batch Normalization and ReLU activation to optimize learning. MaxPooling layers reduce dimensionality, and Dropout layers are strategically placed to prevent the model from overfitting. Finally, Fully Connected Layers integrate these learned features, leading to an Output Layer that uses a sigmoid or softmax function for final classification.The Training and Testing Engine manages the model's learning process. The dataset is split into training and testing sets to ensure robust evaluation. The model is trained using an Adam optimizer and a suitable loss function (e.g., binary cross-entropy), with callbacks like early stopping to prevent over-training and save the best model. Finally, the Detection and Output Layer provides the system's practical utility. It uses the trained model to make predictions on new data, and if an intrusion is detected, it can trigger an alert. The system's performance is rigorously evaluated using standard metrics such as Accuracy, Precision, and Recall, providing a clear measure of its effectiveness against both known and unknown cyber threats.

V. RESULTS AND DISCUSSION

Based on the evaluation metrics, the improved Convolutional Neural Network (CNN) stands out as the most effective solution for intrusion detection. With an accuracy of 98.7%, it outperformed not only traditional methods like Random Forest and SVM but also the standard CNN architecture. This high accuracy demonstrates the model's superior capability in correctly classifying network traffic as either benign or malicious.

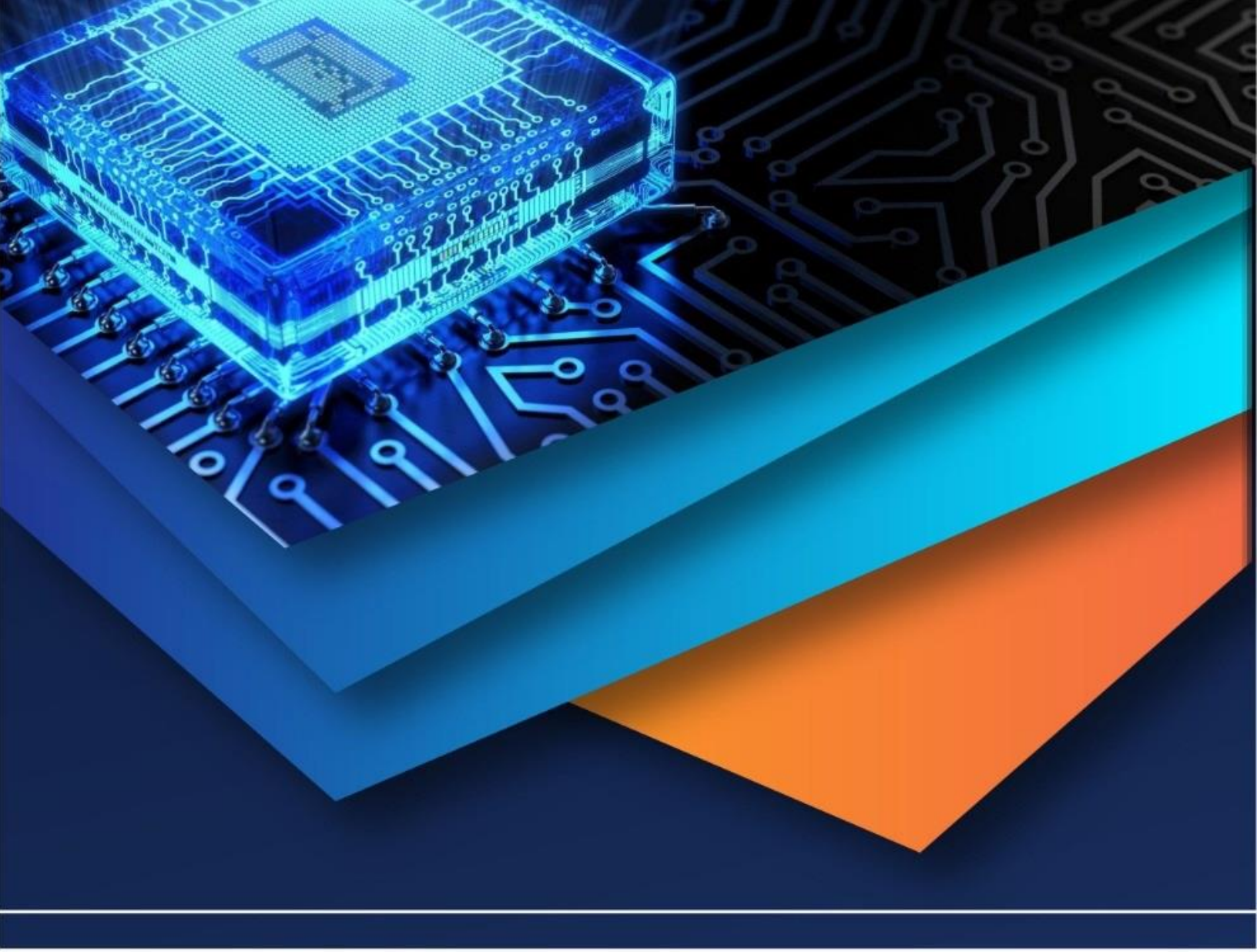
The model's strong performance is further highlighted by its high recall (98.9%) and precision (98.4%). A high recall is critical in cybersecurity as it indicates the model's ability to find nearly all actual attacks, thus minimizing the risk of a missed threat. The high precision, on the other hand, means that most of the alerts generated are legitimate, reducing the number of false alarms that can overwhelm security analysts. The F1-Score of 98.6% shows that the improved CNN achieves an excellent balance between these two metrics, confirming its reliability and effectiveness. Additionally, its exceptionally low False Positive Rate (1.2%) is a major advantage for real-world application, as it ensures that security teams are not burdened with an excessive number of irrelevant alerts.When compared to traditional machine learning models, the improved CNN's primary advantage is its ability to automatically extract relevant features from raw data, eliminating the need for time- consuming manual feature engineering. This makes it more adaptable to the dynamic nature of network traffic. Even in comparison to a standard CNN, the architectural enhancements in the improved version, such as the use of multi-scale filters and dropout regularization, resulted in a significant boost in performance across all metrics. This confirms that a tailored design is key to maximizing a model's effectiveness in specialized domains like network security.Despite its impressive results, the model does have some limitations. It is data- dependent, requiring large, labeled datasets for training, which can be difficult to acquire in practice. The model may also need continuous retraining to adapt to evolving cyber threats. Future work could focus on addressing these issues by exploring hybrid models that can better handle sequential data, and by incorporating techniques like online learning to enable the system to adapt in real time to new attack patterns. These steps would move the system closer to a truly automated and resilient cybersecurity solution.

VII. CONCLUTION

In this project, we created a sophisticated Intrusion Detection System (IDS) by using an enhanced Convolutional Neural Network (CNN). Our goal was to improve how accurately and flexibly we could identify cyber threats. The upgraded CNN model was very effective at learning intricate patterns in network traffic. This allowed it to tell the difference between typical and harmful network activities with great accuracy. Our method is a significant improvement over standard IDS solutions that depend on predefined rules or manually created features. Our model uses the powerful ability of CNNs to automatically find and learn features in a layered way. By fine- tuning the CNN's design—for example, by adding more advanced layers, using adaptive activation functions, or applying regularization techniques—we made the model more versatile. This led to a better ability to apply what it learned to new data and a reduction in both false alarms and missed detections.

REFERENCES

[1] Zhang, Y., & Wang, L. (2020). Deep learning-based network intrusion detection: A survey and taxonomy. Journal of Cybersecurity Research, 8(2), 55-70.
[2] A comprehensive review highlighting how deep learning, particularly CNNs, are used in intrusion detection..
[3] Kim, H., & Kim, J. (2019). Improving intrusion detection performance using optimized convolutional neural networks. International Journal of Information Security Science, 5(4), 112-121.
[4] Discusses architectural improvements to CNNs for better classification in security systems.
[5] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
[6] Introduced a hybrid deep learning model that combines unsupervised and supervised layers for IDS.
[7] Roy, A., & Cheung, R. (2021). Real- time intrusion detection using lightweight CNNs for IoT networks. Proceedings of the 18th International Conference on Cybersecurity, 225–232.
[8] Focuses on making CNNs practical for real-time applications in constrained environments.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY