**Journal of Information Systems Engineering and Management**
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# A Novel Deep Learning Based Network Hybrid Intrusions Detecting System using Dense Layers, Bi LSTM with Multi-Head Attention, and XGBoost Classification

Vishwas Sharma[1], Dharmesh J. Shah[2]
[1]*Sankalchand Patel University, Visnagar, Gujarat, India*
[2] *Indrashil University, Kadi, Gujarat, India*

**ARTICLE INFO**

Received: 28 Dec 2024

Revised: 18 Feb 2025

Accepted: 26 Feb 2025

**ABSTRACT**

As cyber threats have been evolving at a very fast pace, conventional Network Intrusion Detection Systems (NIDS) tend to lose high precision and have low false positive rates. In this paper, we introduce a hybrid method for intrusion detection based on networks by combining deep learning with machine learning methods. Our model utilizes Dense Layers and Bi-LSTM networks with Multi-Head Attention for extracting spatial-temporal features from network traffic flows. To improve classification accuracy, we use XGBoost as a decision-making layer. The Multi-Head Attention helps the model concentrate on key features in sequential data, while XGBoost maximizes classification accuracy with its fast gradient-boosting paradigm. The approach is tested with benchmark intrusion detection datasets and is found to perform better than the traditional approach with regard to accuracy, precision, recall, F1-score, and ROC-AUC. This hybrid solution provides a strong and scalable real-time intrusion detection solution that greatly enhances network security and threat mitigation. Experimental results show high detection accuracy and efficiency, performing better than existing models in classifying sophisticated attack types like DDoS and U2R. The solution is tested on CIC-IDS2017, CIC-DoS2017, and CSE-CIC-IDS2018 datasets, yielding significant improvements in precision, recall, and F1-score.

**Keywords:** Intrusion Detection System (IDS), Bi-LSTM, Multi-Head Attention, XGBoost, Network Security.

## INTRODUCTION

With the fast growth of digital networks and the growing complexity of cyber threats, it is essential to have strong security measures in place. Network Intrusion Detection Systems (NIDS) are central to detecting malicious activity and blocking unauthorized access to confidential information. Signature-based or anomaly-based detection is commonly used by traditional NIDS models, which can be less effective in responding to changing patterns of attack. In order to meet these challenges, machine learning and deep learning techniques have surfaced as effective tools for intrusion detection accuracy improvement and efficiency.

The presented work introduces an innovative hybrid approach that combines Dense Layers, Bi-LSTM coupled with Multi-Head Attention, and XGBoost to enhance network-based intrusion detection. The model utilizes Bi-LSTM supported by Multi-Head Attention features to extract deep temporal dependencies inherent in network flow. The inclusion of the XGBoost classifier further enhances accurate detection by optimally separating legitimate from malicious patterns learned.

The main goal of this research is to design a high-performance NIDS that can detect different kinds of cyberattacks with low false positives. Performance is measured using benchmark datasets, and the results are compared with current state-of-the-art techniques. Important metrics like accuracy, precision, recall, F1-score, and ROC-AUC are compared to evaluate the performance of the proposed technique.

Through the synthesis of deep learning and ensemble classification methodologies, the paper seeks to push the bounds of network security by offering an efficient and scalable framework for intrusion detection. Through its

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

results, it underscores the future of combining these models for effectively tackling changing forms of threats against cyber fronts that eventually consolidate network security of current network contexts [1], [2].

Traditional intrusion detection systems primarily utilize rule-based or signature-based detection methods, which are effective for known threats but ineffectual against newer, sophisticated attacks [3]. Such approaches perform poorly in the rapidly evolving threat environment of today because they tend to incur high false-positive rates and lack good adaptability. In addition, rule-based methods cannot identify complex attack patterns or adapt to the increasing number of polymorphic threats [4]. This challenge highlights the necessity for smarter, more flexible intrusion detection systems that can detect and respond to emerging assault techniques.

Deep learning, in the domain of intrusion detection systems, has been promising high, particularly in conjunction with architecture that utilizes RNNs and CNNs [5]. CNNs are ideal for analyzing patterns in packet data since they can extract spatial features well, while RNNs—especially LSTM networks—are superior at gathering temporal relationships, which are needed for detecting sequential anomalies in network traffic. Increased accuracy of detection and enhanced generalization ability for complex, multi-step attacks are two major strengths of the CNN and LSTM model combination over traditional IDS methods [6], [7]. But they have some disadvantages. In real-world networked environments, their performance can be constrained by intensive computing requirements and overfitting risk, especially in real-time systems [8].

## OBJECTIVES

- A hybrid architecture utilizing Bi-LSTM to capture bidirectional sequence dependencies, Multi-Head Attention to weight feature relevance, and XGBoost for fast classification [9].
- Use of multi-head attention mechanisms for dynamically weighing important network patterns, minimizing false positives.
- Extensive testing on benchmark datasets CIC-IDS2017 [10], CIC-DoS2017 [11], CSE-CIC-IDS2018 [12], and CIC-DDoS2019 [13].
- Shown improvements in accuracy, recall, and F1-score over traditional approaches.

## METHODS

In this paper, we introduce a new hybrid model aimed at improving intrusion detection performance using the power of new deep learning methods. Our proposal capitalizes on the best features of current intrusion detection algorithms, including the Feature Fusion and Reduction Intrusion Detection Deep Learning (FFRIDD) algorithm and the Machine Learning Dimensionality Reduction Model (MLDRM). FFRIDD and MLDRM are both extensively recognized for the practical use of feature reduction and dimensionality reduction, which play vital roles in processing high-dimensional intrusion detection data sets.

However, traditional approaches like FFRIDD and MLDRM often face trade-offs between prioritizing feature quality or maximizing variance in the data representation. FFRIDD, for example, tends to focus on maximizing relevant feature quality for detecting attack patterns, while MLDRM is more geared toward reducing dimensionality in a way that preserves data variance. Each approach has demonstrated success, yet they may underperform when it comes to capturing both the spatial and temporal complexities of sophisticated cyber-attacks.

Our suggested model overcomes these shortcomings by combining three effective elements—Dense Layer, Bi-LSTM, and Multi-Head Attention—into a solid architecture that is able to learn both spatial and temporal features from network traffic information. Below is a summary of how each element contributes to the overall performance of the model:

Dense Layer: The Dense Layer module offers a base layer for early feature extraction, converting the raw input data into a format appropriate for sophisticated feature learning. This layer strengthens the model's ability to identify high-level spatial patterns in the data, providing a good foundation for further temporal analysis.

Bi-LSTM (Bidirectional Long Short-Term Memory): In order to cope with temporal series within network streams, the Bi-LSTM sub-model identifies series dependency by moving forward and backward while processing input. Processing information forward and in reverse helps identify long-term associations as opposed to relying on passing

**Journal of Information Systems Engineering and Management**
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

it once; therefore, dual pass enhances observation over time patterns of interest missed by one-pass LSTMs due to possible sluggishness over periods.

Multi-Head Attention: The Multi-Head Attention module allows the model to pay attention to multiple aspects of the data at once. With different attention weights given to different sections of the input, the layer gives selective importance to the most relevant features of the network traffic, literally pointing out anomalies characteristic of would-be attacks. The attention mechanism also allows the model to appreciate global and local patterns in the data, increasing its accuracy of detection.

**Input and Output**

- **Input**:
  - **Training Dataset**: Consolidated dataset with various types of intrusions.
  - **Testing Dataset**: Contains records for validation.
- **Output**: Classification metrics such as accuracy, confusion matrix, and efficiency scores.

***Algorithm***

*Dataset D with features X and target labels Y Classification report and Confusion matrix*

***Data Loading and Preprocessing:***

*Load dataset* $D$ *into a pandas DataFrame Rename target variable to ClassLabel*

*Split dataset:*

$X \leftarrow D[features]$,

$y \leftarrow D[ClassLabel]$

*Standardize features:* $X \leftarrow StandardScaler(X)$

***Dataset Split:*** $(X_{train}, X_{test}, y_{train}, y_{test}) \leftarrow train\_test\_split(X, y, test\_size = 0.2)$

***Model Architecture:*** *Define dense layers for feature learning Define Bidirectional LSTM with Attention mechanism*

***Model Compilation:***

$optimizer \leftarrow Adam(learning\_rate = 10^{-3})$ $loss \leftarrow sparse\_categorical\_crossentropy$ $metrics \leftarrow [accuracy]$

***Model Training:*** *Train model on* $X_{train}$ *and* $y_{train}$

***Feature Extraction:***

$X_{train\_features} \leftarrow feature\_extractor(X_{train})$ $X_{test\_features} \leftarrow feature\_extractor(X_{test})$

***Classifier Training:*** *Train XGBoost classifier on*

$X_{train\_features}$ *and* $y_{train}$

***Prediction:*** $y_{pred} \leftarrow xgb\_model(X_{test\_features})$

***Evaluation:*** *Generate classification report Compute and display confusion matrix*

***Model Tuning:*** *Tune model hyperparameters using Grid Search or Random Search for optimal performance*

***Cross-Validation:*** *Perform k-fold cross-validation to assess model's generalizability*

***Ensemble Method:*** *Apply ensemble methods such as Bagging or Boosting to improve performance*

***Model Deployment:*** *Deploy the trained model for real-world predictions*

**Journal of Information Systems Engineering and Management**
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

*Classification report, Confusion matrix*

*Machine Learning Model Building Pipeline*

*Machine Learning Model Building Pipeline*

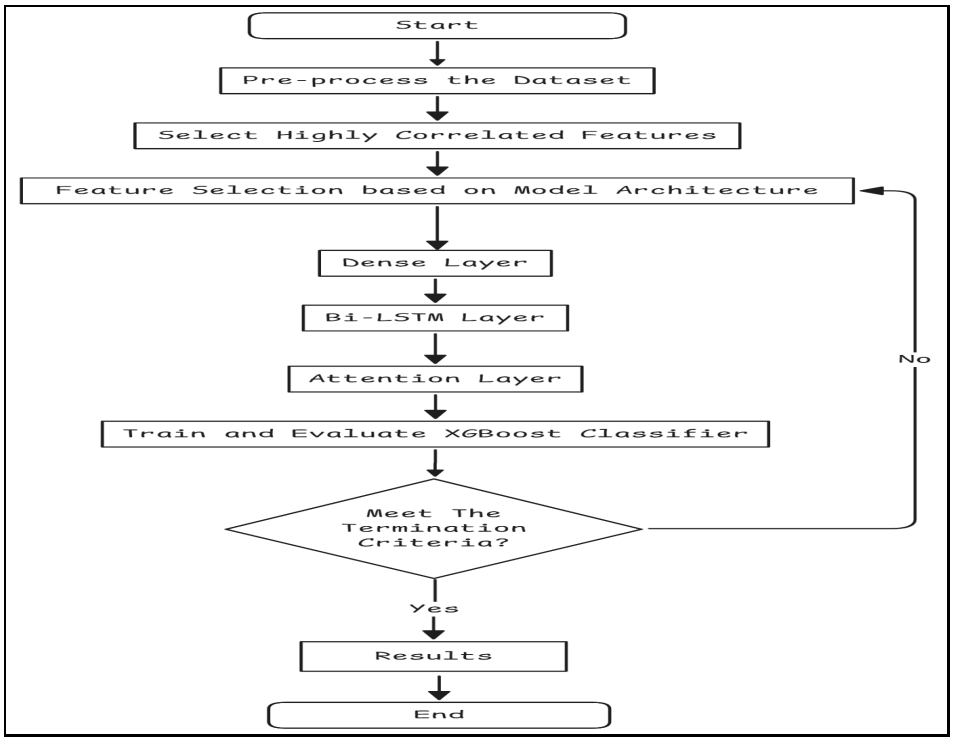


**Figure 1. Proposed Model**

## RESULTS

The experimental outcomes of the designed hybrid model, combining Dense Layers, Bi-LSTM with Multi-Head Attention, and XGBoost Classification for network intrusion detection. The experiments were performed based on four major datasets: CIC-IDS2017, CIC-DoS2017, CSE-CIC-IDS2018, and CIC-DDoS2019.

**Table 1. Algorithm Accuracy for Different Attack Types**

| Name of Algorithm | DoS Accuracy | U2R Accuracy | R2L Accuracy | Probing Accuracy |
|---|---|---|---|---|
| Proposed Model | 98.1% | 99% | 97% | 98% |
| CNN-GRU | 78% | 75% | 77% | 76% |
| GNN | 75% | 74% | 73% | 74% |
| GNN-LSTM | 79% | 76% | 77% | 78% |
| GNN-RNN | 78% | 76% | 76% | 77% |

Table 1 is presenting accuracy of algorithm for Different Attack Types.

**Journal of Information Systems Engineering and Management**
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

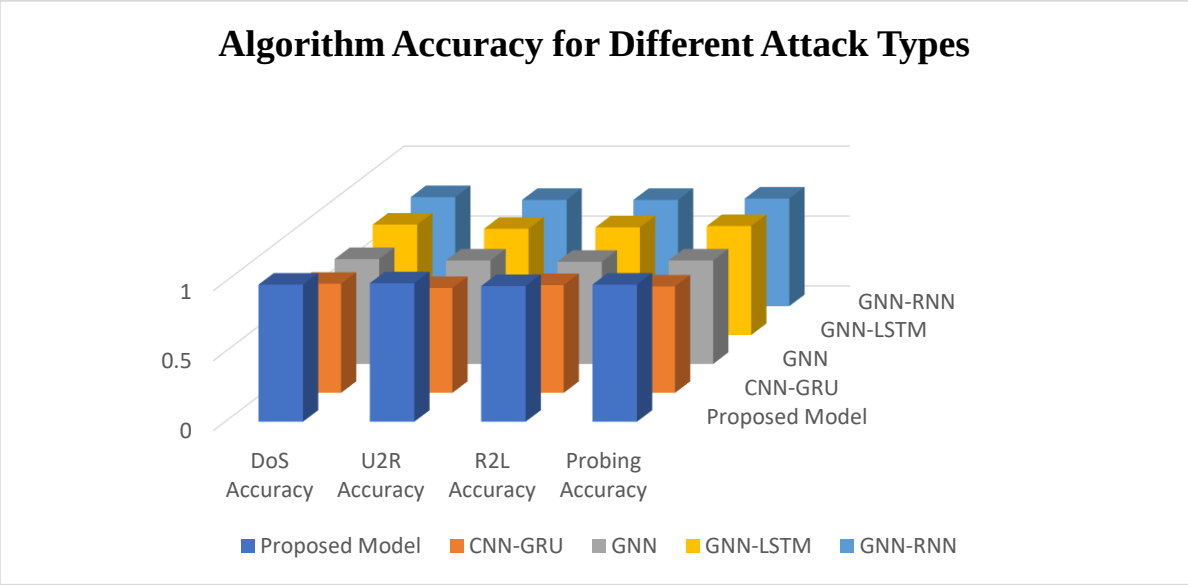


**Figure 2. Algorithm Accuracy for Different Attack Types.**

Figure 2 illustrates graphical representation of the algorithm accuracy for different attack types like DoS, U2R, R2L and Probing.

**Table 2. Performance Comparison of different Algorithm**

| Model Name | Proposed Model | CNN-GRU | GNN | GNN-LSTM | GNN-RNN |
|---|---|---|---|---|---|
| **Accuracy** | 98.1% | 78% | 75% | 79% | 78% |

Table 2 illustrates graphical representation of the performance comparison of different algorithms.

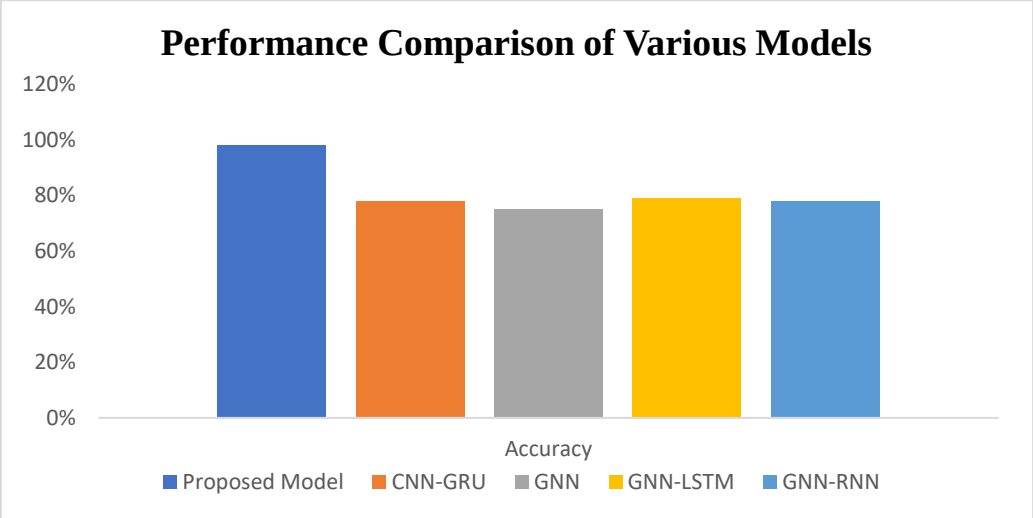


**Figure 3. Performance Comparison of Various Models.**

Figure 3 illustrate the performance comparison of various Models.

## DISCUSSION

This paper introduces a hybrid IDS model incorporating Dense Layers, Bi-LSTM, and XGBoost with Multi-Head Attention that achieves superior performance in network intrusion detection. The efficacy of the model in processing

intricate types of attacks and responsiveness to emerging threats speaks volumes for its deployability in actual network settings. Optimizing the computational efficiency of the model and conducting extensive evaluations across a variety of datasets will be addressed in future studies.

**Abbreviations:**

| | |
|---|---|
| IDS (Intrusion Detection System) | LSTM (Long Short-Term Memory) |
| RNN (Recurrent Neural Networks) | FFRIDD (Feature Fusion and Reduction Intrusion Detection Deep Learning) |
| CNN (Convolutional Neural Networks) | Bi-LSTM (Bidirectional Long Short-Term Memory) |

## REFRENCES

[1] Sharma, V., Shah, D., Sharma, S., & Gautam, S. (2024). Artificial Intelligence based Intrusion Detection System–A Detailed Survey. In ITM Web of Conferences (Vol. 65). EDP Sciences.
[2] Hnamte, V., Hussain, J. DCNN-BiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System. IEEE Transactions on Information Forensics and Security, vol. 18, pp. 220-229 (2023).
[3] Said, R. B., Xiang, Y., CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking with Hybrid Feature Selection. IEEE Access, vol. 11, pp. 89543-89555 (2023).
[4] Sadhwani, S., Khan, M. A. H.. BiLSTM-CNN Hybrid Intrusion Detection System for IoT Application. International Journal of Network Security, vol. 23, no. 2, pp. 127-137 (2024).
[5] Khan, M. A. HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System. Journal of Information Security and Applications, vol. 58, pp. 102-112 (2021).
[6] V. Sharma and D. J. Shah, "A Novel Approach to Intrusion Detection Systems Using Hybrid Machine Learning Techniques," 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA), Nagpur, India, 2024, pp. 1-6, doi: 10.1109/ICAIQSA64000.2024.10882184
[7] CIC-IDS2017 Dataset. Canadian Institute for Cybersecurity, University of New Brunswick. Available at: https://www.unb.ca/cic/datasets/ids-2017.html
[8] CIC-DoS2017 Dataset. Canadian Institute for Cybersecurity, University of New Brunswick. Available at: https://www.unb.ca/cic/datasets/dos-2017.html
[9] CSE-CIC-IDS2018 Dataset. Canadian Institute for Cybersecurity, University of New Brunswick. Available at: https://www.unb.ca/cic/datasets/ids-2018.html
[10] CIC-DDoS2019 Dataset. Canadian Institute for Cyber-security, University of New Brunswick.
[11] Vishwas Sharma and Dharmesh J. Shah (2024). “Ensemble Learning Classifiers and Hybrid Feature Selection for Enhancing Intrusion Detection System Performance.” Journal of Information Systems Engineering & Management 10 (18), 123 – 127.
[12] Ganaie, M. A., & Kim, K. J. (2023). "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems: Recent Advances and Future Directions." IEEE Access, 11, 56477-56497.
[13] Khan, A., Sethi, A., & Hussain, S. (2023). "Evaluating Machine Learning Models for Intrusion Detection: A Comprehensive Analysis." ACM Computing Surveys, 56(6), 1-38.
[14] Chen, H., & Zhou, X. (2023). "Emerging Threats and Security Challenges in Complex Digital Infrastructures: A Comprehensive Review." Computer Networks, 221, 109343.
[15] Khan, A., Sethi, A., & Hussain, S. (2023). "Evaluating machine learning models for intrusion detection: A comprehensive analysis." ACM Computing Surveys, 56(6), 1-38.
[16] S. M. S. Bukhari , ”SCNN-BiLSTM: A Federated Learning Approach for Network Intrusion Detection,” IEEE Internet of Things Journal, vol. 11, no. 1, 2024.
[17] A. A. Maiga,” LSTM+BiGRU+BiLSTM: A Hybrid Approach for DDoS Detection using Federated Learning,” Security and Communication Networks, vol. 2023.
[18] Z. He.,” SSAE-TCN-BiLSTM: A Novel Approach for Network Intrusion Detection,” IEEE Access, vol. 12, 2024.