SVU-International Journal of Engineering Sciences and Applications (2025) 6(2): 138-146
Print ISSN 0000-0000 | Online ISSN 2735-4571
10.21608/svusrc.2025.374593.1281

Enhancing Network Intrusion Detection with CNN-LSTM

Esraa Mokhtar [1, ✉], Nahla F. Omran[1], Ahmed Abdel-Baset Donkol [2]

Abstract - Intrusion Detection Systems (IDSs) play a vital role in securing modern networks by identifying unauthorized access and malicious activities. However, challenges such as class imbalance and the limited ability of traditional approaches to capture temporal patterns hinder accurate detection, particularly for minority attack classes. This study introduces a hybrid deep learning model that integrates a Convolutional Neural Network (CNN) with Long Short-Term Memory (LSTM) layers and an attention mechanism. To address the class imbalance problem, the model is trained using the Synthetic Minority Oversampling Technique (SMOTE) and Focal Loss. Experimental evaluations conducted on the KDD Cup 99 dataset demonstrate that the proposed CNN-LSTM with Attention model achieves a classification accuracy of 97.09% and an F1-score of 97.46%, significantly outperforming the baseline CNN model. These findings highlight the effectiveness of incorporating temporal modeling and attention mechanisms in enhancing intrusion detection performance, particularly for rare attack types such as Remote to Local (R2L) and User to Root (U2R).

Keywords: Intrusion Detection System (IDS), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Attention Mechanism, KDD Cup 99, SMOTE, Focal Loss, Deep Learning, Network Security.

1 Introduction

With the increasing reliance on internet-based systems and services, cyber threats have become more frequent and increasingly sophisticated. Consequently, ensuring network security has become a top priority for organizations and institutions. Network Intrusion Detection Systems (NIDS) are essential tools for identifying suspicious activities and preventing unauthorized access [1]. However, traditional NIDS approaches, which rely primarily on predefined rules or signatures, often fail to detect novel and evolving attack techniques.

In recent years, machine learning and deep learning techniques have emerged as powerful alternatives [2], capable of learning complex patterns directly from raw network traffic data. Among these, Convolutional Neural Networks (CNNs) are effective at capturing spatial features but struggle to model the temporal dependencies inherent in many intrusion scenarios.

To address this limitation, hybrid architectures incorporating Long Short-Term Memory (LSTM) networks have gained attention for their sequential processing capabilities [3]. Nonetheless, challenges such as dataset imbalance and minority attack classes continue to hinder detection accuracy.

To mitigate these issues, this study incorporates the Synthetic Minority Oversampling Technique (SMOTE) to balance the dataset and applies focal loss to improve the learning of minority classes during model training. The study compares two deep learning-based NIDS approaches: a CNN model enhanced with Stochastic Gradient Pooling, and a hybrid CNN-LSTM model integrated with an attention mechanism.

The aim is to evaluate their performance on the KDD Cup 99 dataset [4] and to demonstrate the benefits of sequential modeling and attention-based feature enhancement. This study offers several key contributions: (1) It presents a hybrid CNN-LSTM model with a soft attention mechanism for detecting complex and rare attack patterns; (2) It tackles class imbalance using SMOTE and focal loss; (3) It provides a detailed comparison against a CNN baseline model; and (4) It analyzes how temporal modeling and attention mechanisms improve classification accuracy, especially for minority attack types. While similar architectures have been proposed in previous

Received: 25 April 2025 / Accepted: 13 October 2025
✉ Corresponding Author: Esraa Mokhtar, esraamokhtar2310@gmail.com

1. Faculty of Computers and Information, South Valley University, Qena, Egypt
2. Department of Electrical Engineering, Faculty of Engineering, South Valley University, Qena, Egypt

studies, this work introduces novel enhancements, including a custom attention mechanism and advanced balancing techniques, leading to improved model robustness and detection performance.

2 Related Work

Recent advancements in deep learning have significantly enhanced Intrusion Detection Systems (IDS), particularly through hybrid architectures that combine convolutional and recurrent neural networks. Several studies have explored the use of CNNs for extracting spatial features from traffic data, while others have demonstrated the efficacy of Long Short-Term Memory (LSTM) networks in capturing temporal patterns within network flows.

Aljawarneh et al. [5] introduced a CNN-RNN hybrid model that improved detection performance, particularly for minority classes. Similarly, Yin et al. [6] highlighted the potential of LSTM networks in temporal analysis, reporting notable improvements over traditional machine learning techniques. Nonetheless, these models often encountered limitations related to class imbalance and lacked sophisticated attention mechanisms to emphasize critical features in long sequences.

To address such challenges, various studies have employed techniques like the Synthetic Minority Oversampling Technique (SMOTE) or incorporated advanced loss functions such as focal loss. For instance, Liu et al. [7] showed that integrating focal loss with CNN architectures enhances sensitivity to rare attack classes. Expanding on this approach, Al-Omar and Trabelsi [8] proposed an attention-based CNN-LSTM model, achieving over 95% accuracy on the UNSW-NB15 dataset and further validating the benefits of attention mechanisms.

Sinha et al. [9] proposed a hybrid LSTM-CNN model applied to the BoT-IoT dataset, attaining a classification accuracy of 99.87%, which reinforced the strength of combining spatial and temporal features in intrusion detection. Yang et al. [10] advanced this line of research by integrating Inception-CNN, BiGRU, and attention layers, achieving robust performance across imbalanced attack categories. Meanwhile, Jouhari and Guizani [11] emphasized real-time efficiency by introducing a lightweight CNN-BiLSTM model tailored for IoT environments, delivering high accuracy with minimal computational overhead.

Building upon prior contributions, our study presents a novel CNN-LSTM architecture that integrates a custom soft attention mechanism between stacked LSTM layers, and employs both SMOTE and focal loss to address class imbalance. The objective is to enhance the detection of underrepresented attack types, such as Remote-to-Local (R2L) and User-to-Root (U2R), using the KDD Cup 99 dataset.

Unlike existing studies that often focus on individual techniques, this work uniquely combines four critical components—CNNs for spatial feature extraction, LSTMs for temporal modeling, attention for feature refinement, and dual imbalance mitigation—into a cohesive deep learning framework. To the best of our knowledge, this combination has not been jointly explored in previous IDS research. The proposed model demonstrates enhanced capability in detecting rare and subtle intrusion patterns, positioning it as a robust and novel contribution in the field.

3 Methodology

This section outlines the steps followed in building and evaluating the proposed intrusion detection models. It includes data preprocessing, feature selection, handling class imbalance, and the architecture details of the CNN and CNN-LSTM models.

The methodological choices in this study were guided by the nature of intrusion detection data. CNN was selected for its ability to capture local spatial patterns in traffic features, making it suitable for processing structured input representations. LSTM networks were chosen to model temporal dependencies inherent in sequential traffic flows, enabling better recognition of patterns across time steps. An attention mechanism was integrated to prioritize the most relevant time features, enhancing focus on informative parts of the input. To address the severe class imbalance in the dataset, the SMOTE technique was employed to synthetically oversample minority classes, and focal loss was used to penalize hard-to-classify examples. These combined techniques aimed to improve the robustness and generalization ability of the detection model.

3.1 Data preprocessing

To begin, the training and testing datasets were loaded and merged for consistent preprocessing. Duplicate records were removed to avoid bias. Non-numeric features were encoded using label Encoding. The original 22 attack types and the "normal" label were grouped into five categories: Normal, Denial of Service (DoS), Probing (Probe), R2L, and U2R. Feature values were normalized using StandardScaler to improve model performance and convergence [12].

3.2 Feature selection

To improve efficiency and model generalization, Information Gain (Mutual Information) was used to select the top 20 features with the highest predictive power. This selection reduced dimensionality and eliminated redundant data [13].

3.3 Class imbalance

The original KDD dataset exhibited a pronounced class imbalance, with the majority of instances belonging to the Normal and DoS categories.

Table 1. Class distribution before and after SMOTE, showing balanced categories.

Class	Before SMOTE	After SMOTE
DoS	55,994 (39.82%)	75,942 (20.00%)
Normal	75,942 (54.01%)	75,942 (20.00%)
Probe	6,112 (4.35%)	75,942 (20.00%)
R2L	2,497 (1.78%)	75,942 (20.00%)
U2R	70 (0.05%)	75,942 (20.00%)

As shown in **Table 1**, classes such as R2L and U2R are severely underrepresented, accounting for only 1.78% and 0.05% of the samples, respectively. To address this issue, the Synthetic Minority Oversampling Technique (SMOTE) was applied exclusively to the training data, while the test set remained unchanged to ensure unbiased evaluation [14]. SMOTE generates synthetic samples for minority classes by interpolating between an instance x_i and one of its nearest neighbors x_{nn}:

$$x_{new} = x_i + \delta \times (x_{nn} - x_i), \ \delta \in [0,1]$$

This process increases the number of samples in rare classes until each class contains 75,942 instances, achieving balanced class representation across all categories. Importantly, the test set distribution remained unchanged to ensure a realistic and unbiased evaluation of the model's generalization performance, thereby avoiding data leakage between training and evaluation phases.

In addition to SMOTE, the model was trained using focal loss, a modified cross-entropy loss that emphasizes hard-to-classify samples. It is formulated as:

$$FL(p_t) = -\alpha t (1 - pt)^{\gamma \log(pt)}$$

Where p_t is the predicted probability for the true class, α_t is a balancing factor, and γ is the focusing parameter that controls the weight given to hard examples. Focal loss is particularly beneficial for underrepresented attack types such as R2L and U2R.

As depicted in **Fig. 1**, the combined use of SMOTE and focal loss effectively mitigated the class imbalance problem. This strategy enhanced the model's robustness, promoted fairer training, and significantly improved detection performance for minority attack categories, especially R2L and U2R, which are often the most challenging to classify.

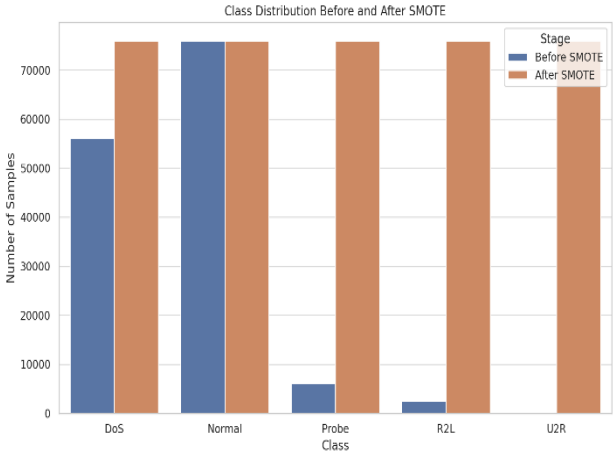

Fig. 1. Class distribution before and after SMOTE, showing balanced representation of rare classes

3.4 CNN model with stochastic gradient pooling

The CNN model used several convolutional layers followed by Stochastic Gradient Pooling (SGP). The architecture was trained with focal loss, class weighting, and SMOTE-balanced data. The confusion matrix and performance results are shown in **Fig. 2.**

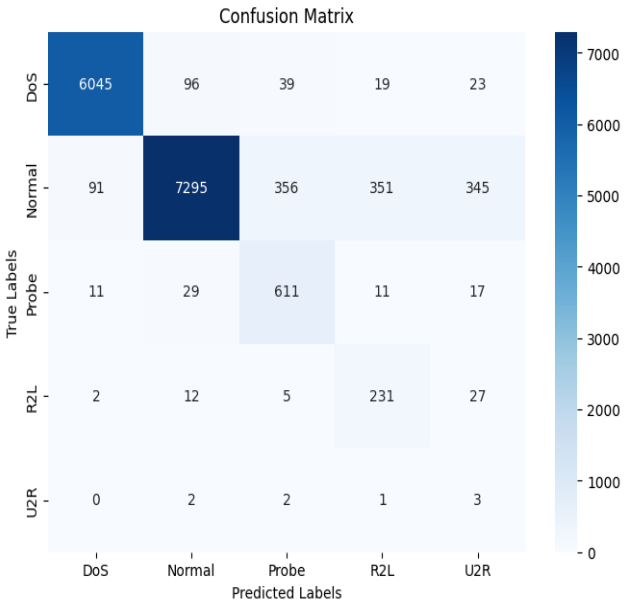

Fig. 2. Confusion matrix of the baseline CNN model, highlighting poor detection of R2L and U2R

As seen in **Fig. 2**, the CNN model performs well in identifying the majority classes (DoS and Normal), but exhibits reduced accuracy for minority classes such as R2L and U2R. This suggests the model's limited ability to capture temporal and contextual patterns associated with rare attacks [15-16].

3.5 CNN-LSTM model with attention mechanism

To better capture the temporal behavior in network traffic, a second model was developed based on a hybrid architecture that integrates CNN and LSTM layers, augmented with a custom attention mechanism [17]. The attention mechanism employed in this study consists of a soft attention [18] layer placed between two stacked LSTM layers. The first LSTM layer is configured with *return_sequences=True* to produce a sequence of hidden states. The attention layer then computes context vectors by assigning weights to each time step, emphasizing the most informative parts of the input sequence. This output is fed into a second LSTM layer to refine temporal features before reaching the final classification stage. This design allows the model to capture essential temporal dependencies, which are crucial for detecting subtle intrusion patterns that traditional methods often fail to recognize.

The performance of the CNN-LSTM model with attention is illustrated in **Fig. 3**, which illustrates improved classification accuracy for minority classes such as R2L and U2R. This supports the effectiveness of the proposed architecture in handling subtle and underrepresented intrusion patterns.

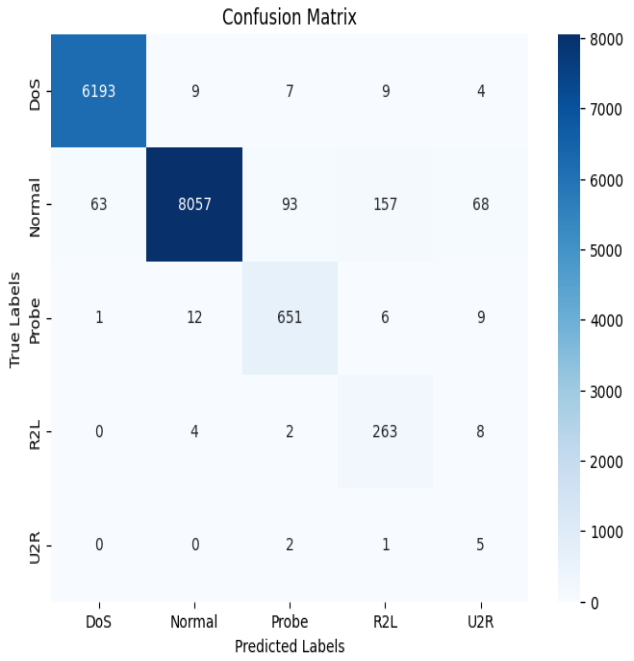

Fig. 3. Confusion matrix of the CNN-LSTM model, showing improved detection of R2L and U2R

The architecture of the proposed CNN-LSTM model comprises several convolutional layers, followed by LSTM units and a custom attention mechanism. The convolutional layers are designed to extract spatial features from the input sequences, while the LSTM units capture temporal dependencies within the data. The attention layer is applied after the LSTM output to emphasize the most informative components [19] of the sequence prior to final classification. This integration enhances the model's capacity to detect complex and subtle patterns in network traffic, which is particularly beneficial for identifying intrusions belonging to minority classes.

Figure 4 illustrates the architecture of the CNN-LSTM model with attention, highlighting its core components: convolutional layers for spatial feature extraction, LSTM units for learning temporal relationships, and an attention mechanism to focus on critical time steps before classification.

To optimize model performance, hyperparameters such as learning rate, batch size, number of epochs, and dropout rate were manually tuned based on validation performance. Several configurations were evaluated iteratively, and the final settings were selected to minimize overfitting while ensuring convergence. Due to computational constraints, an exhaustive grid search was not used; instead, tuning was performed through empirical experimentation on a held-out validation set.

3.6 Implementation details

The models were implemented using TensorFlow and Keras frameworks, following recent implementations of deep LSTM architectures in traffic video analytics [20]. The CNN architecture includes two convolutional layers with 64 and 128 filters, respectively, each followed by MaxPooling and Dropout (rate 0.4). The CNN output is reshaped and passed to two stacked LSTM layers with 128 units each. A soft attention mechanism is applied between the LSTM layers [21] to focus on informative time steps. The final classification layers consist of two dense layers with 256 and 128 units using ReLU activation, followed by Dropout (rates 0.4 and 0.3), and a Softmax output layer for multi-class prediction.

The training was conducted with the following setup:

- Optimizer: Adam
- Learning rate: 0.0005
- Loss function: focal loss
- Batch size: 128
- Epochs: 100 (with early stopping)
- Validation split: 10% of the training data
- SMOTE: Applied only on training data to balance class distribution

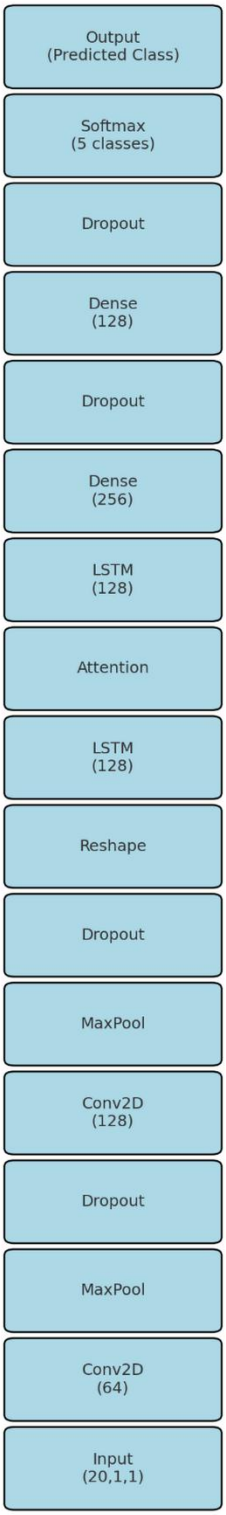

Fig. 4. Architecture of the proposed CNN-LSTM model with attention

3.7 Evaluation metrics

To evaluate the performance of the proposed models, several standard metrics for multi-class classification were employed. Let the confusion matrix be defined in terms of the following variables:

- *TP*: True Positives (correctly classified positive instances).
- *TN*: True Negatives (correctly classified negative instances).
- *FP*: False Positives (negative instances incorrectly classified as positive).
- *FN*: False Negatives (positive instances incorrectly classified as negative).

Based on these values, the metrics are formulated as follows:

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)}$$

Accuracy provides a global indicator of the model's overall correctness across all classes.

$$Precision = \frac{TP}{(TP+FP)}$$

Precision reflects the reliability of positive predictions, which is crucial in IDS to minimize false alarms.

$$Recall\ (Sensitivity) = \frac{TP}{(TP+FN)}$$

Recall quantifies the ability to capture actual attacks, ensuring that intrusion attempts are not overlooked.

$$\text{F1-score} = \frac{2\times(Precision \times Recall)}{(Precision+Recall)}$$

The F1-score balances Precision and Recall, making it particularly useful in imbalanced datasets such as intrusion detection.

These metrics were computed for each class, and macro-averaging was employed to provide an overall performance assessment across all classes, treating each class equally regardless of its prevalence.

These evaluation metrics serve as direct indicators of the effectiveness of the proposed methodology [13], [19]. The high accuracy and F1-score achieved by the CNN-LSTM model with attention underscore its strong generalization capability and its effectiveness in detecting both majority and minority classes.

Moreover, the model's precision and recall values highlight its capacity to reduce false positives and accurately identify true positives, particularly in rare attack scenarios such as R2L and U2R. These results underscore the importance of incorporating temporal modeling (via LSTM), attention mechanisms, and class imbalance

handling techniques (via SMOTE and focal loss) to improve detection performance in complex intrusion detection settings.

While this study primarily focused on standard metrics such as accuracy, precision, recall, and F1-score, future work may include additional evaluation measures—such as ROC-AUC and PR-AUC—for a more comprehensive assessment. Although not implemented in this study, future experiments will incorporate ROC-AUC and PR-AUC metrics to provide a more nuanced evaluation, especially in imbalanced scenarios. Furthermore, in-depth analysis based on confusion matrices can yield valuable insights into class-wise prediction behavior and overall model robustness.

4 Experimental Results

The CNN-LSTM model was evaluated on an independent test dataset following training on a SMOTE-balanced dataset with focal loss.

4.1 Model convergence

As part of the training strategy, the Focal loss function was employed to mitigate class imbalance and enhance optimization. The training and validation curves of the model exhibit consistent convergence, as illustrated in **Fig. 5.** The accuracy curves indicate stable learning behavior with no signs of overfitting. Similarly, the loss curves display a smooth and continuous decline, as shown in **Fig. 6**, confirming the effectiveness of the optimization process over the training run.

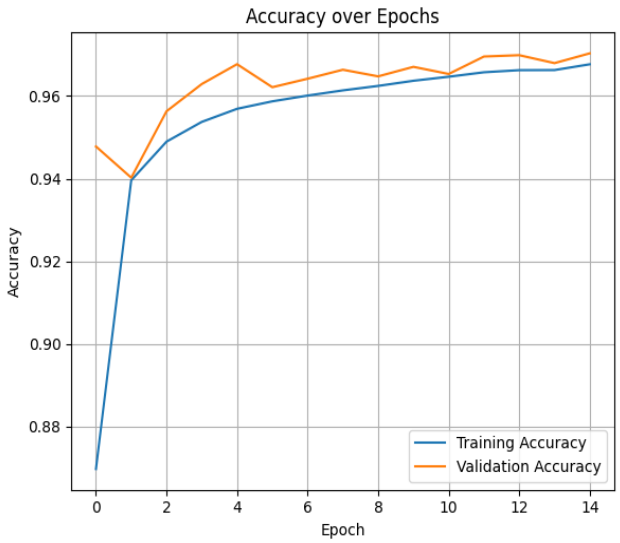

Fig. 5. Training and validation accuracy over epochs, showing consistent convergence

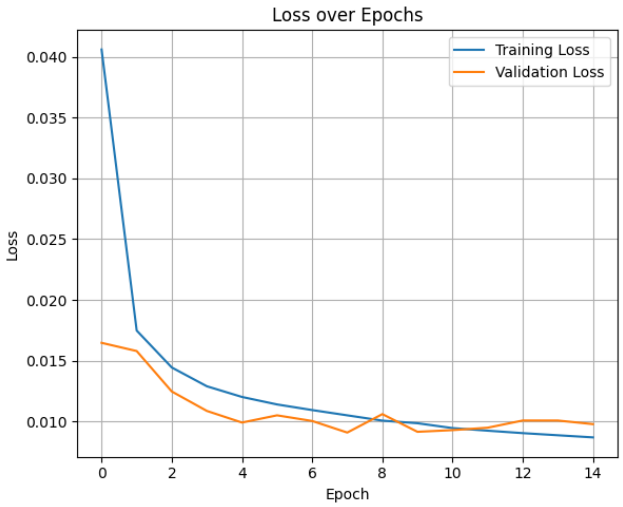

Fig. 6. Training and validation loss over epochs, indicating effective optimization

4.2 Test set performance

Both the baseline CNN model and the proposed CNN-LSTM model with attention were evaluated on the same unseen test set to provide a fair comparison of their generalization performance [13]. The CNN model served as a baseline, whereas the CNN-LSTM model incorporated temporal learning and an attention mechanism to enhance detection performance, particularly for minority attack types.

Table 2 compares the baseline CNN model with the proposed CNN-LSTM with attention. The proposed model shows improvements across all metrics, proving the benefit of adding temporal features and attention to intrusion detection. The CNN-LSTM significantly outperforms the baseline CNN, especially in recall and F1-score, which are crucial for detecting rare attacks such as R2L and U2R.

It also maintains high accuracy for all categories, with strong gains in R2L and U2R detection, and solid performance on Normal, DoS, and Probe traffic.

Overall, the CNN-LSTM with attention achieves a final accuracy of 97.09%, compared to 90.79% for the baseline CNN, highlighting its effectiveness in handling class imbalance and improving detection of rare intrusions.

Table 2. Test performance comparison between CNN and CNN-LSTM models.

Metrics	CNN	CNN-LSTM
Accuracy (%)	90.79 %	**97.09 %**
Precision (%)	95.44 %	98.08 %
Recall (%)	90.79 %	97.09 %
F1 Score (%)	92.62 %	97.46 %

4.3 Error analysis

To gain deeper insight into the model's limitations, an error analysis was performed by examining the distribution of False Positives (FP) and False Negatives (FN) across each class in the test set. A detailed breakdown of these errors is provided in **Table 3**.

Table 3. Error analysis showing false positives and false negatives per class.

Class	False Positives	False Negatives
DoS	58	31
Normal	38	374
Probe	92	36
R2L	188	22
U2R	94	3

Classification errors per class are summarized in **Table 3.** The Normal class shows a high number of false negatives (FN), indicating frequent misclassification of benign traffic as attacks, possibly due to overlapping feature patterns. In contrast, the R2L and U2R classes exhibit elevated false positives (FP), suggesting that normal connections were sometimes mistaken for rare intrusions.

As illustrated in **Fig. 7**, while most classes have low error rates, misclassifications are most prominent in the Normal class, followed by R2L and U2R, highlighting areas for further refinement.

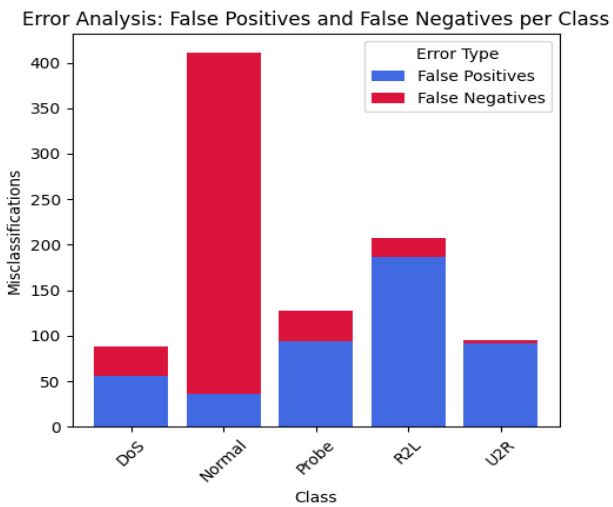

Fig. 7. Class-wise error distribution of the CNN-LSTM model, highlighting false negatives in Normal and false positives in R2L and U2R

These results demonstrate that while the model performs well in detecting various attack types, especially rare ones such as U2R, further refinements are necessary to reduce false positives and enhance the distinction between normal and malicious traffic.

The following section discusses the implications of these findings and examines the key factors contributing to the model's performance.

5 Discussion

The experimental results confirm the significant benefits of incorporating temporal modeling and attention mechanisms within deep learning architectures for intrusion detection. Compared to the baseline CNN model, the proposed CNN-LSTM with attention yields notable improvements across all key evaluation metrics, particularly for minority attack classes such as R2L and U2R.

The integration of SMOTE and focal loss effectively addresses class imbalance by oversampling minority classes and emphasizing hard-to-classify instances during training. These enhancements contribute to improved generalization on unseen test data, as reflected in the higher accuracy, recall, and F1-score achieved by the model. The LSTM layers capture sequential dependencies in network traffic, while the attention mechanism refines the model's focus on critical time steps, ultimately enhancing its classification capability.

5.1 Interpretation of results

The CNN-LSTM model demonstrated strong generalization capability, as evidenced by the smooth convergence of training and validation curves and its superior classification performance on the test set. It consistently achieved high true positive rates across most categories. Most notably, it identified U2R attacks—the rarest class—more accurately than the baseline CNN, which frequently misclassified such instances [22], consistent with findings in recent hybrid deep learning studies [9], [10], [11]. This highlights the effectiveness of temporal sequence modeling and attention mechanisms in capturing subtle patterns associated with rare attack types.

While the primary comparison in this study focuses on the CNN-LSTM model with attention versus a baseline CNN model, it is worth noting that previous research has explored classical machine learning approaches for intrusion detection, including Support Vector Machines (SVM), Random Forests (RF), and k-Nearest Neighbors (k-NN). However, these traditional models often fall short in capturing complex temporal and contextual dependencies, particularly in imbalanced datasets [2], [5], [16]. In contrast, the proposed deep learning architecture demonstrates significant improvements in detecting rare and nuanced attack types, as demonstrated by the consistently higher accuracy and F1-scores. This suggests that integrating temporal modeling and attention mechanisms offers a more

robust and scalable alternative to traditional classifiers in contemporary intrusion detection systems.

5.2 Error Patterns and Class Behavior

Despite the model's overall strong performance, error analysis revealed notable misclassification patterns. The normal class had the highest number of false negatives, indicating frequent confusion with certain attack types, possibly due to overlapping feature distributions between benign and malicious traffic.

Conversely, the R2L and U2R classes exhibited elevated false positive rates, likely influenced by synthetic patterns introduced through SMOTE. Although SMOTE effectively rebalanced class distributions, it may have contributed to overfitting in rare classes [14].

These findings highlight the need for improved feature engineering and more selective oversampling strategies to reduce false alarms and enhance the model's ability to distinguish between normal and attack traffic.

6 **Conclusion**

This study presented a comparative analysis between a baseline CNN model and an enhanced CNN-LSTM architecture with an attention mechanism for network intrusion detection using the KDD Cup 99 dataset. Both models addressed class imbalances through SMOTE and were trained using focal loss to improve sensitivity to hard-to-classify samples.

Experimental results showed that the CNN-LSTM model consistently outperformed the baseline CNN across all key evaluation metrics, achieving an accuracy of 97.09% and an F1-score of 97.46%. The inclusion of LSTM layers enabled the model to capture temporal dependencies in network traffic, while the attention mechanism improved its focus on the most informative features.

Notably, the proposed model demonstrated significant improvements in detecting rare attack types such as R2L and U2R, which are typically difficult for conventional classifiers. Error analysis further confirmed a reduction in misclassification rates across both majority and minority classes.

Overall, the CNN-LSTM with attention architecture proved to be a robust and effective solution for building intelligent, data-driven intrusion detection systems capable of handling class imbalance and identifying subtle attack patterns.

In addition, potential real-time applications of the proposed CNN-LSTM model are envisioned. For example, the model could be integrated into intrusion detection modules of IoT gateways or cloud-based network monitoring systems, where low latency and high throughput are essential. Future work will focus on deploying the model within real-time streaming frameworks to evaluate inference latency, computational efficiency, and scalability under realistic network traffic conditions.

7 **Limitations and Future Work**

Although the proposed CNN-LSTM with attention model demonstrated strong performance across most evaluation metrics, several limitations should be acknowledged. First, reliance on the KDD Cup 99 dataset—despite its widespread use—poses a challenge to generalizability, as it does not adequately represent modern network traffic or recent attack types. Second, while SMOTE effectively rebalanced the dataset, it may have introduced synthetic patterns that contributed to higher false positive rates, particularly in minority classes such as R2L and U2R. Third, the model was evaluated in an offline setting, without consideration of real-time deployment constraints such as inference latency and resource consumption. Furthermore, cross-validation techniques such as k-fold cross-validation will be applied in future work to improve the robustness of performance evaluation.

Future evaluations will also consider more contemporary and representative datasets such as CICIDS2017 and UNSW-NB15 to improve generalizability to modern attack scenarios. Additionally, incorporating online learning capabilities or deploying the model within streaming architectures could facilitate assessment under real-time operational conditions. Further optimization of the attention mechanism and refinement of oversampling strategies may help reduce false alarms and enhance generalization of evolving attack patterns. Incorporating cross-validation techniques is also recommended to provide more reliable and robust performance estimates.

References

[1] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid deep neural network for network intrusion detection system," IEEE Access, vol. 10, pp. 99837–99849, 2022. doi: 10.1109/ACCESS.2022.3206425

[2] V. G. S. Vaishalini, A. Ramathilagam, R. Palanikumar, P. Raghavan, P. Gopikannan, and K. Manikandan, "Comprehensive survey of deep learning-based intrusion detection and prevention systems for secure communication in the Internet of Things," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 3, pp. 1822–1828, 2024.

[3] Y. Zhang, R. C. Muniyandi, and F. Qamar, "A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance," Applied Sciences, vol. 15, no. 3, p. 1552, Feb. 2025. doi: 10.3390/app15031552

[4] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, "The 1999 DARPA off-line intrusion detection evaluation," Computer Networks , vol. 34, no. 4, pp. 579–595, 2000, doi: 10.1016/S1389-1286(00)00139-0

[5] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, “Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model,” Journal of Computational Science , vol. 25, pp. 152–160, 2018. doi: 10.1016/j.jocs.2017.03.006

[6] C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” IEEE Access, vol. 5, pp. 21954–21961, 2017. doi: 10.1109/ACCESS.2017.2762418

[7] Z. Liu, P. Jiang, L. Zhang, and X. Niu, “A combined forecasting model for time series: Application to short-term wind speed forecasting,” Applied Energy, vol. 259, p. 114137, 2020. doi: 10.1016/j.apenergy.2019.114137

[8] B. Al-Omar and Z. Trabelsi, "Intrusion Detection Using Attention-Based CNN–LSTM Model," in Artificial Intelligence Applications and Innovations (AIAI 2023), I. Maglogiannis, L. Iliadis, J. MacIntyre, and M. Dominguez, Eds. Cham, Switzerland: Springer, 2023, IFIP Advances in Information and Communication Technology, vol. 675, pp. 492–503. doi: 10.1007/978-3-031-34111-3_43

[9] P. Sinha, D. Sahu, S. Prakash, T. Yang, R. S. Rathore, and V. K. Pandey, "A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning," Scientific Reports, vol. 15, Art. no. 9684, Mar. 2025. doi: 10.1038/s41598-025-94500-5

[10] K. Yang, J. Wang, and M. Li, "An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN," Scientific Reports, vol. 14, Art. no. 19339, Aug. 2024. doi: 10.1038/s41598-024-19339-y

[11] M. Jouhari and M. Guizani, "Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices," in Proc. 2024 Int. Wireless Commun. and Mobile Comput. Conf. (IWCMC), Ayia Napa, Cyprus, May 2024. doi: 10.1109/IWCMC61514.2024.10592352

[12] Y. M. Assem, A. Bedair, M. H. Essai, and S. Ali, "Robust deep convolutional neural network-based classifiers," SVU-Int. J. Eng. Sci. Appl., vol. 4, no. 1, pp. 41–47, Jun. 2023, doi: 10.21608/SVUSRC.2022.161642.1073

[13] M. Abdelsattar, A. AbdelMoety, and A. Emad-Eldeen, "Comparative analysis of machine learning techniques for fault detection in solar panel systems," SVU-International Journal of Engineering Sciences and Applications, vol. 5, no. 2, pp. 140–152, Dec. 2024. doi: 10.21608/SVUSRC.2024.279389.1198

[14] M. A. Talukder, M. M. Islam, M. A. Uddin, K. F. Hasan, S. Sharmin, S. A. Alyami, and M. A. Moni, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," Journal of Big Data, vol. 11, Art. no. 33, Feb. 2024. doi: 10.1186/s40537-024-00886-w

[15] P. Phalaagae, A. M. Zungeru, A. Yahya, B. Sigweni, and S. Rajalakshmi, "A hybrid CNN-LSTM model with attention mechanism for improved intrusion detection in wireless IoT sensor networks," IEEE Access, vol. 13, pp. 57322 - 57341, 2025. doi: 10.1109/ACCESS.2025.3555861

[16] Z. Hajirahimi and M. Khashei, "Hybrid structures in time series modeling and forecasting: A review," Engineering Applications of Artificial Intelligence, vol. 86, pp. 83–106, 2019. doi: 10.1016/j.engappai.2019.08.018

[17] D. Yu, H. Kong, J. C.-H. Leung, P. W. Chan, C. Fong, Y. Wang, and B. Zhang, "A 1D convolutional neural network (1D-CNN) temporal filter for atmospheric variability: Reducing the sensitivity of filtering accuracy to missing data points," Applied Sciences, vol. 14, no. 14, p. 6289, 2024. doi: 10.3390/app14146289

[18] K. C. Mondal, N. Biswas, and S. Saha, "Role of machine learning in ETL automation," in Proceedings of the 21st International Conference on Distributed Computing and Networking (ICDCN '20), Kolkata, India, Feb. 2020, Article no. 57, pp. 1–6. doi: 10.1145/3369740.3372778

[19] M. R. Delavar, "Hybrid machine learning approaches for classification and detection of fractures in carbonate reservoir," Journal of Petroleum Science and Engineering, vol. 208, p. 109327, 2022. doi: 10.1016/j.petrol.2021.109327

[20] M. A. Abdelwahab, "Robust traffic congestion recognition in videos based on deep multi-stream LSTM," SVU-International Journal of Engineering Sciences and Applications, vol. 3, no. 1, pp. 91–97, Jun. 2022. doi: 10.21608/SVUSRC.2022.133083.1046

[21] M. Abdelsattar, A. A. A. Rasslan, and A. Emad-Eldeen, "Detecting dusty and clean photovoltaic surfaces using MobileNet variants for image classification," SVU-International Journal of Engineering Sciences and Applications, vol. 6, no. 1, pp. 9–18, Jun. 2025. doi: 10.21608/SVUSRC.2024.308832.1232

[22] C. Ji, H. Yu, and W. Dai, "Network traffic anomaly detection based on spatiotemporal feature extraction and channel attention," Processes, vol. 12, no. 7, p. 1418, Jul. 2024. doi: 10.3390/pr1207141