International Journal of Interpreting Enigma Engineers (IJIEE)
https://ejournal.svgacademy.org/index.php/ijiee/
https://doi.org/10.62674/ijiee.2026.v3i03.002
eISSN: 3048-6300
OPEN ACCESS

A LIGHTWEIGHT HYBRID DEEP LEARNING FRAMEWORK FOR MULTI-CLASS NETWORK INTRUSION DETECTION

Dr. S Murali Mohan[1], Gowtham Reddy Kunduru[2], Dr. Shaik Jaffar Hussain[3], Narendra Mangala[4], Posina Anusha[5]

Original Article

[1]Professor, Dept of ECE, Mother Theresa Institute of Engineering and Technology (Autonomous), Palamaner, AP, India.
[2]Lead Software Engineer, M&T bank Buffalo, New York.
[3]Associate Professor, Department of CSE, Presidency University, Bengaluru, India.
[4]Manager, Sogeti USA, Sogeti USA, 8075 Washington Village Drive, Washington Township, Dayton, Ohio 45458.
[5]Assistant Professor, Department of AI&DS, Annamacharya Institute of Technology & Sciences, Tirupati, India.

*Corresponding Author's Email: [1]muralimohanieee@gmail.com, [2]gowtham.kunduru@gmail.com, [3]jaffar.thebest@gmail.com, [4]narendra.mangala@outlook.com, [5]anusha.ksrm@gmail.com

Abstract

The growing variety of cyberattacks has increased the need for intrusion detection systems that can detect multiple categories of attack with high reliability. We propose a lightweight hybrid framework LHCBA-Net, which integrates one dimensional convolutional neural networks, bidirectional long short term memory and temporal attention for multiclass network intrusion detection in this paper. The model was trained after the CICIDS2017 dataset went through a series of data cleaning, feature engineering, feature selection, class balancing and feature transformation procedures. CNN layers capture local traffic patterns, BiLSTM models bidirectional contextual dependencies, and temporal attention highlights informative intrusion related representations. Experimental results on the test set compared with traditional machine learning and deep learning baselines show that LHCBA-Net achieved 99.08% test accuracy with precision, recall, F1-score and AUC of 0.991, 0.990, 0.990 and 0.998 respectively. Feature-importance and SHAP analyzes provide further support for the interpretation of the learned decision patterns. The results show that the proposed framework is efficient for accurate detection of multi-class intrusions.

Index Terms – Intrusion Detection System, CICIDS2017, 1D-CNN, BiLSTM, Temporal Attention, Multi-class Classification, Network Security.

Introduction

Today's networks are increasingly dependent on a web of interconnected digital services, making them more susceptible to a range of cyber intrusions. Examples of threats that can interrupt services and decrease the reliability of network operations are DoS, DDoS, brute-force attacks, bot activity and port scanning. As the attack behavior becomes more diverse and harder to distinguish from legitimate traffic, the traditional security mechanisms may not provide sufficient detection capability. Therefore, recent research in intrusion detection has moved to machine learning and deep learning techniques capable of analyzing complex traffic characteristics and enabling automated threat identification [1], [2]. This is important especially, because correct separation of attack categories can help in faster and appropriate security responses.

Machine learning and deep learning have become significant techniques to enhance the detection of intrusion in complex network environments. Conventional classifiers can give reliable results but their efficiency is often dependent on the quality of chosen traffic features [3]. Deep learning alleviates this reliance by learning useful representations directly from network data. Convolutional neural networks are good at capturing local relationships among traffic features, while recurrent architectures are able to model sequential behavior in attack patterns [4]. However, perhaps no single learning mechanism can cover all the diversity of intrusion characteristics. Moreover, complex hybrid models may increase the

computational cost, requiring compact architectures that combine complementary learning capabilities with practical efficiency.

Recent work on intrusion detection has shown great advances but still has problems to address multiple types of attacks in a single efficient framework. Some approaches focus on local feature extraction or sequential learning, while others are based on complex multi stage architectures, which increase the computational demand [5]. However, these designs may limit the practical application for lightweight and rapid detection. Moreover, unidirectional sequence modeling may ignore context relations over forward and backward dependencies. A similar problem is that the equal treatment of learned features can also weaken the identification of subtle intrusion patterns [6]. These limitations highlight the need for a compact multiclass framework that incorporates local learning, bidirectional context, and adaptive feature importance.

In an effort to overcome the identified limitations, a lightweight hybrid framework called LHCBA-Net is proposed for multiclass intrusion detection using the CICIDS2017 dataset. The architecture consists of compact convolutional learning, bidirectional sequence modeling, and temporal attention to capture complementary intrusion characteristics with a relatively simple structure. The main contributions of this work can be summarized as follows:

1. To tackle multiclass intrusion detection, a lightweight hybrid architecture, named LHCBA-Net, is proposed by combining 1D-CNN, BiLSTM, and temporal attention into a single framework.
2. We design a compact feature learning structure with only two convolutional layers and one BiLSTM layer, rather than deep or multistage architectures, to learn complementary traffic features.
3. Bidirectional modeling and temporal attention capture contextual dependencies and highlight important intrusion related features.
4. The framework performs multiclass attack classification on CICIDS2017 and compared with machine learning and deep learning baselines using multiple evaluation metrics.

Literature Survey

Recently, conventional ensemble and hybrid learning strategies have been studied to improve network intrusion detection. In this context, Mohan and Ranjeeth Kumar [7] combined behavioral analysis with machine learning classifiers and demonstrated that ensemble based decisions can improve attack recognition but still rely on engineered traffic features. Similarly, Sindhula and Pradeep [8] presented ensemble feature selection for DoS and DDoS detection, improving discrimination in selected attack categories but with limited coverage for wider multiclass threats. Extending this direction, Abdelhalim et al. in [9] proposed a CNN-LSTM framework with recursive feature elimination on CICIDS2017 and showed the advantages of combining local feature extraction and sequence learning. Nevertheless, the binary classification setting limits its direct application to multiple intrusion classes. These results motivate a compact framework for richer feature learning and unified multiclass detection.

More recent work has built on these developments by exploring deeper hybrid and lightweight architectures for more effective intrusion detection. Gautam et al. [10] combined dense layers, BiLSTM, multi-head attention and XGBoost together with high predictive ability but with complex architecture. Similarly, Jishnu et al. [11] proposed a CNN-LSTM model with balancing strategies to improve detection performance over imbalanced traffic classes, although the framework still used conventional unidirectional sequence learning. Meanwhile, Ilahi et al. [12] explored a lightweight quantized intrusion detection approach for IoT environments but the evaluation was still focused on limited attack categories. These studies point to the need for compact multiclass architectures that maintain contextual learning while reducing unnecessary complexity in the model.

More recently, research has also focused on explainability and sophisticated hybrid learning for multiclass intrusion detection. In this context, Dudi et al. [13] combined Light GBM with SHAP to provide interpretable attack classification, however, the approach did not explicitly model spatial and temporal dependencies within network traffic. In the same vein, Ramasamy et al. [14] have suggested a broader hybrid framework with CNN-BiLSTM, adversarial learning and edge cloud for intrusion detection. However, the extensive design of the addition of multiple processing stages can lead to increased architectural complexity. In conclusion, these studies suggest that effective intrusion detection still requires a compact framework that can efficiently learn local patterns, bidirectional contextual information, and discriminative feature importance in performing multiclass classification.

Methods & Materials

A. Dataset Description

CIC-IDS2017 is a flow based intrusion detection benchmark dataset, created for academic cybersecurity research. It was released by the Canadian Institute for Cybersecurity and contains benign traffic and multiple attack types including Botnet, Brute Force, DDoS, DoS, Infiltration, PortScan, and Web Attacks. In the Kaggle version, you will find the original CSV documents and the cleaned Parquet files with predefined data types and no missing records. The dataset includes 8 traffic files with benign and malicious network activities and is therefore suitable for evaluating multiclass intrusion detection models. Dataset link: https://www.kaggle.com/datasets/dhoogla/cicids2017

B. Experimental Setup and Hardware Configuration

We experimentally evaluate LHCBA-Net on the CICIDS2017 network-flow dataset, with a fixed training setting. The network consists of two Conv1D layers with 32 and 64 filters, a BiLSTM layer with 64 units, temporal attention and a Softmax classifier. The model was trained using Adam optimizer with a learning rate of 0.001, batch size of 64 and 50 epochs. The loss function used was categorical cross entropy. The experiments were carried out on a 64-bit machine equipped with an AMD Ryzen 5 220 processor, 16 GB of RAM, and an NVIDIA GeForce RTX 5050 Laptop GPU with 8 GB of memory. The platform also had integrated graphics in the form of AMD Radeon 740M and 477 GB storage.

C. Data Pre-processing

We preprocessed the CICIDS2017 data using a structured pipeline to improve the data consistency, reduce redundant information, and prepare suitable inputs for multiclass intrusion detection. The procedure steps were data cleaning, feature construction, feature selection, class handling, scaling and label preparation before model training.

1) *Data Cleaning:*First, the CICIDS2017 traffic logs were inspected for detection and deletion of inconsistent observations before feature processing. Numerical attributes were coerced to a common data type and infinite values were treated as missing values. Records with nonpositive flow duration or negative packet count were considered invalid and were discarded from further analysis.

$$x_i^* = \begin{cases} x_i, & \text{if } x_i \text{ is valid and finite} \\ NaN, & \text{otherwise} \end{cases}$$

After dealing with invalid observations, the cleaned dataset was scanned for missing or infinite numerical values. This process resulted in a uniform input space for the subsequent feature engineering and model building.

2) *Feature Engineering:*More traffic descriptors were generated from the original CICIDS2017 attributes after data cleaning for better representation of network behavior. Features such as total packets, total bytes, packet rate, bytes per packet, idle variation, active variation, burst ratio, and packet entropy were generated from existing flow statistics.

$$BytesperPacket = \frac{TotalBytes}{TotalPackets + \epsilon}$$

Here ϵ is a small constant to avoid division by zero. These derived attributes provide complementary information on traffic volume, packet behavior, activity patterns and flow characteristics, resulting in a richer feature space for subsequent intrusion classification

3) *Feature Selection:* After the feature construction, irrelevant and redundant attributes were pruned to make the input space more compact. Attributes with very low variance were eliminated with a threshold of 0.001. Attributes with strong correlation (above 0.90) were eliminated to limit duplication. Then, an importance analysis based on Random Forest was performed to rank the rest of variables and keep the 85% most informative features.

$$Var(X_j) < \tau_v \Rightarrow X_j \text{ is removed}$$

where $\tau_v = 0.001$is the variance threshold This process reduced the number of features for training the model to 34 attributes.

4) *Class Balancing:*The training set was heavily imbalanced with benign traffic dominating some minority attack classes. To alleviate this imbalance, a hybrid resampling technique was only applied to the training data. Benign samples were down sampled. DDoS, DoS Hulk and the grouped Other classes were selectively upsampled to increase the number of minority-class representations without changing the test distribution.

$$N_c' = m_c N_c$$

where N_c is the initial number of samples of class c and $m_c$is the class specific resampling factor. This approach resulted in more balanced training for subsequent model training.

5) *Scaling, Normalization, and Label Encoding:* The selected numerical features were transformed with a Quantile Transformer with a normal output distribution to decrease skewness and limit the effect of extreme values. Fitted on training features and applied the same transformation on training and testing data.

$$z_{ij} = \Phi^{(-1)\left(F_{j(x_{ij})}\right)}$$

where F_j is the empirical distribution of feature j and Φ^{-1} is the inverse standard normal function. Finally, label encoding was used to convert class labels into integer indices for training a multiclass model.

D. Proposed Lightweight Hybrid Deep Learning Framework

In order to tackle the problems associated with multi-class network intrusion detection, this research has developed a framework known as LHCBA-Net (Lightweight Hybrid CNN-BiLSTM-Attention). This framework is specially developed for detecting and classifying attacks in the CICIDS2017 data set. Network flows in this data set are characterized by very complex time behavior patterns and many different attacks that include Denial of Service (DoS), Distributed Denial of Service (DDoS), Brute Force, PortScan, Bot, and Web attacks. In contrast to the existing complex deep learning frameworks, LHCBA-Net framework can classify intrusion attacks using low-complexity feature learning, sequential learning, and attention-guided decision making. CICIDS2017 benchmark data set contains realistic network traffic flows collected during five days and consists of several modern cyber-attack types and benign traffic.

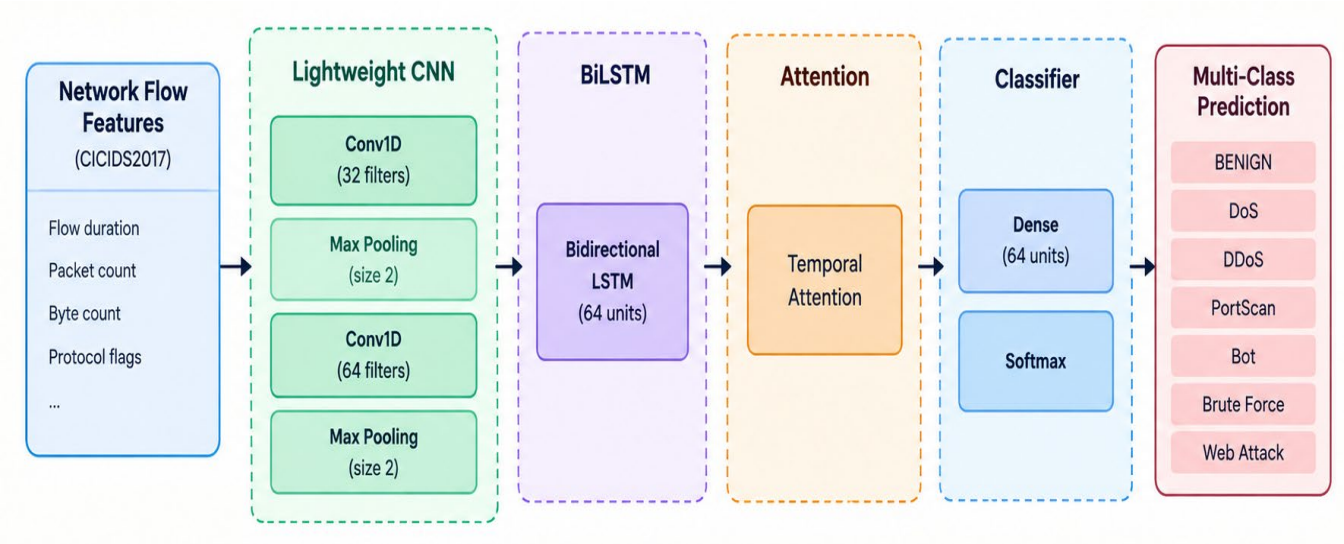

Fig. 1: Graphical representation of the proposed model

- Network Architecture: The suggested framework involves four sequential learning phases: feature representation, local pattern mining, learning temporal dependencies, and attention-based classification. Every phase accomplishes an individual goal to boost the intrusion detection process as a whole.

- Lightweight CNN for Spatial Feature Learning: The first phase uses a light-weight one-dimensional convolutional neural network (1D-CNN) for the learning of discriminatory representation directly from the numeric network flow features. Instead of using many convolutional layers in the CNN architecture, only two convolutional layers are used to reduce the number of trainable parameters. For a given feature vector X, the convolution operation produces feature maps as:

$$F = \sigma\,(W * X + b)$$

  where W is the convolution filter, * stands for the convolution operator, and σ is the ReLU activation function. The process helps to learn the local dependencies between the packet statistics, number of bytes, duration of flows, protocol flags, and other network features.

- Bidirectional LSTM for Temporal Dependency Modeling: Although all network flows have numeric representation, many attacks show sequential dependencies in terms of their feature patterns. Thus, the CNN features obtained are passed through a BiLSTM layer.

  The two memory cells will concurrently examine the features in both forward and reverse directions to allow detection of those contextual relations that would be ignored by unidirectional recurrent neural networks. This is especially useful in discriminating between similar attacks like DoS, DDoS, and PortScan whose statistical profiles somewhat coincide.

  The BiLSTM output can be formulated as:

$$H = [\,\vec{H}\,;\,\overleftarrow{H}\,]$$

  Where the resulting feature vector representation incorporates both forward and backward context in a single feature embedding.

- Attention-Based Feature Refinement: However, each learned feature is not equally important in detecting the intrusion. The attention mechanism focuses on the most meaningful features temporally while neglecting irrelevant features. Rather than considering each hidden feature as equally important, the attention mechanism considers attack-related features more important prior to classification.

  The attention coefficient is calculated as:

$$\alpha = \mathrm{Softmax}(H)$$

  The improved feature representation is then fed into the classifier, allowing the neural network to concentrate on unique features pertaining to each type of intrusion. Such an approach enhances classification performance without significantly increasing the computational burden.
- Multi-Class Classification Layer: In the final phase, there is a fully connected lightweight layer, which is followed by a Softmax classifier. The classifier turns the fine-tuned feature representation into probabilities according to the attack classes that are present in the CICIDS2017 dataset. The attack class is chosen based on choosing the maximum probability from all the available classes.

  This setup aligns with the goal of the proposed conference paper research: accurate multi-class network intrusion detection with the help of lightweight hybrid deep learning algorithm. With the use of CNN to extract features locally, BiLSTM to learn the context dependency, and attention to select the features adaptively, the balance of both capability and lightness has been achieved.

The designed architecture deliberately stays small to minimize the level of computation while achieving efficient detection results. The lightweight architecture is achieved through employing only two layers of convolution and one layer of BiLSTM while the attention mechanism focuses only on useful intrusion patterns. The combination of Adam optimizer with 0.001 learning rate and batch size of 64 ensures smooth convergence during multiclass classification. Table 1 presents the hyperparameter configuration of the proposed model.

Table 1: Hyperparameter Configuration of the Proposed LHCBA-Net

Hyperparameter	Value / Configuration
Model Name	LHCBA-Net (Lightweight Hybrid CNN–BiLSTM–Attention)
Input Type	CICIDS2017 network flow features
Convolution Layers	2 × Conv1D
Conv1D Filters	32, 64
Kernel Size	3
Activation Function	ReLU
Max Pooling Size	2
BiLSTM Units	64
Attention Mechanism	Temporal Attention
Dense Layer	64 neurons
Output Layer	Softmax
Number of Classes	Multi-class intrusion categories
Loss Function	Categorical Cross-Entropy
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Epochs	50
Dropout Rate	0.30
Weight Initialization	He Normal
Evaluation Metrics	Accuracy, Precision, Recall, F1-score, ROC-AUC

Results and Discussions

A. Performance Comparison with Baseline Models

Table 2: Comparison of the proposed LHCBA-Net with the traditional machine learning and deep learning baselines. The proposed model achieved the best test accuracy of 99.08% with precision of 0.991, recall of 0.990, F1-score of 0.990 and AUC of 0.998. The results show that a combined architecture of CNN, BiLSTM and attention are more reliable for multi-class intrusion detection than the individual and hybrid baseline models.

Table 2: Performance Comparison of Proposed with Baseline Models

Model	Train Acc. (%)	Test Acc. (%)	Precision	Recall	F1-Score	AUC
Logistic Regression	84.12	82.95	0.831	0.822	0.826	0.891
Decision Tree	99.61	92.18	0.923	0.918	0.920	0.946
Random Forest	98.84	96.87	0.969	0.967	0.968	0.988
CNN	97.56	95.41	0.955	0.953	0.954	0.981
BiLSTM	98.02	96.14	0.962	0.960	0.961	0.986
CNN–BiLSTM	98.73	97.82	0.978	0.977	0.977	0.992
Proposed LHCBA-Net	99.31	99.08	0.991	0.990	0.990	0.998

B. Training and Validation Performance

Figure 2 shows the training and validation behavior of LHCBA-Net on 50 epochs. The loss curves on both training and validation are decreasing steadily, and the training and validation accuracy curves gradually converge close to 99%, which shows the model learning is stable and converging well. The relatively small gap between the corresponding curves also indicates the limited overfitting in the training process.

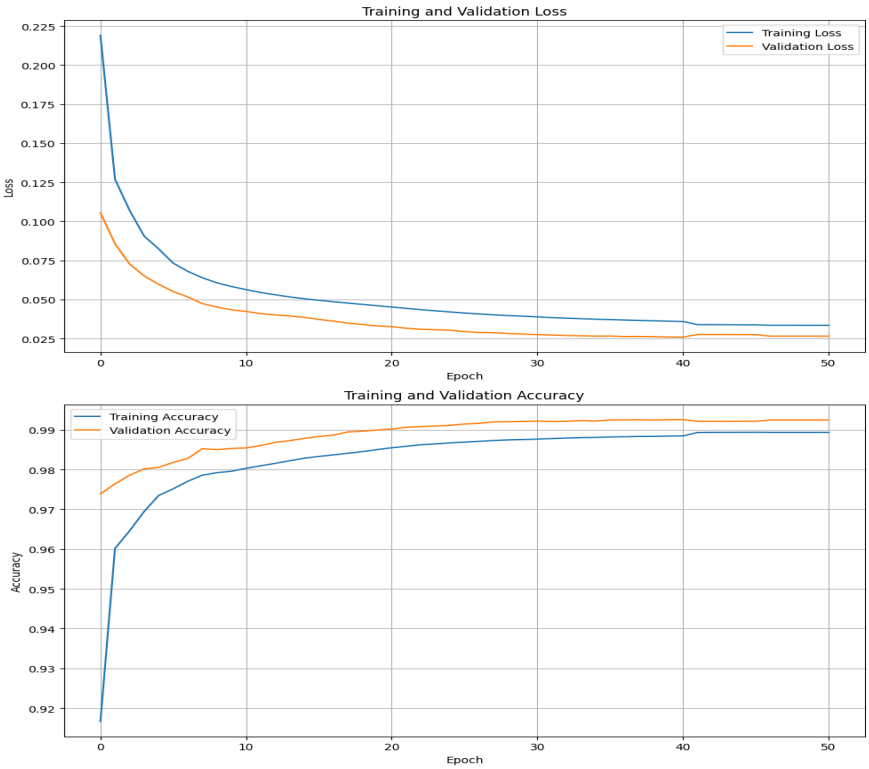

Fig. 2: Training and validation accuracy and loss curves of the proposed model across 50 epochs.

C. Confusion Matrix Analysis

Figure 3. Class-wise prediction performance of the proposed LHCBA-Net. The high concentration of samples along the main diagonal indicates that the evaluated intrusion classes were accurately discriminated with only a small number of misclassifications. The model achieved an overall accuracy of 99.08%, a macro-F1 score of 0.990 and a weighted F1-score of 0.991, indicating a stable performance for the dominant and minority attack classes.

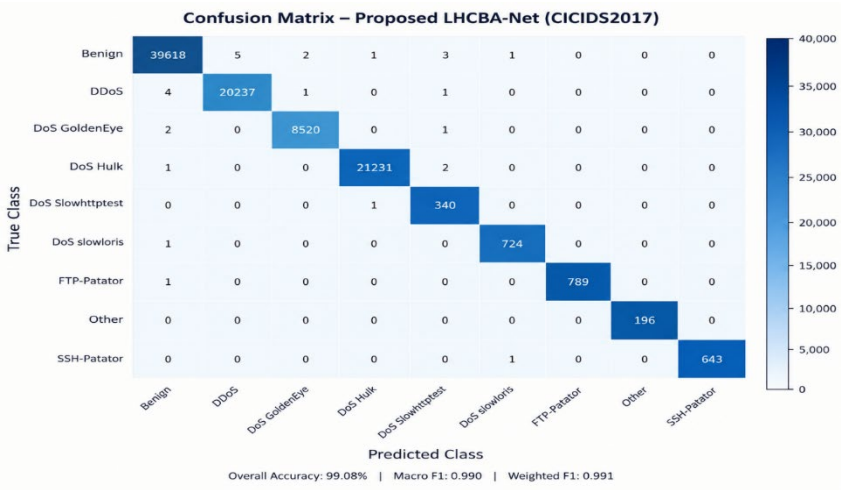

Fig.3 Confusion Matrix of the Proposed Model

D. Feature Importance Analysis

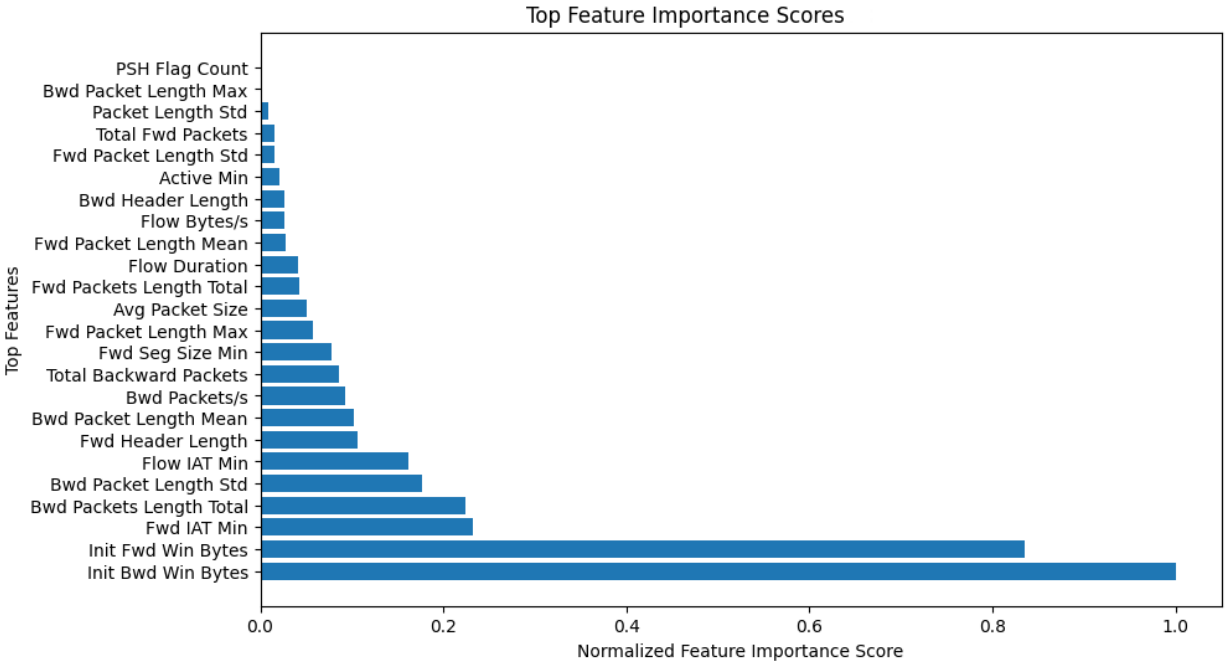

Fig. 4: Feature Importance Analysis of the Top Features Scores

The relative importance of the selected network flow features for intrusion classification is shown in Figure 4. Init Bwd Win Bytes and Init Fwd Win Bytes are the features with the highest normalized importance scores, followed by Fwd IAT Min and Bwd Packet Length Total. The distribution suggests that a small subset of traffic characteristics contributes more strongly to the model's predictions, while several other attributes contribute comparatively less.

E. SHAP-Based Local Interpretation:

Figure 5 illustrates the local SHAP explanation of a correctly classified attack sample. The maximum positive contributions come from the features id.orig_p, conn_state, id.resp_p and duration, which change the prediction from the baseline value of 7.788 to 13.214. The results illustrate the influence of individual traffic attributes on the decision of the model and enhance the interpretability of the intrusion classification process.

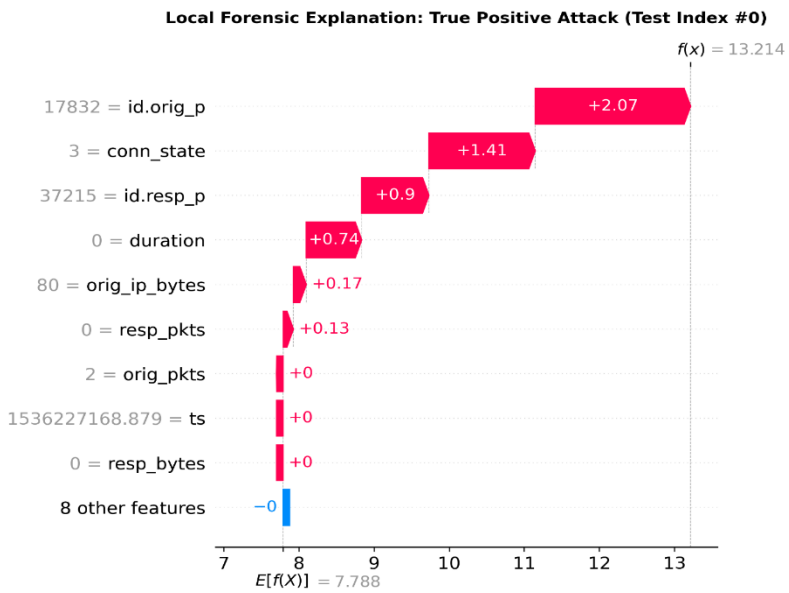

Fig. 5: SHAP Analysis of the Local Forensic Explanation

Conclusion & Future Work

We propose LHCBA-Net, a lightweight hybrid framework for multiclass intrusion detection using CICIDS2017 based on 1D-CNN, BiLSTM and temporal attention. The proposed model achieved a test accuracy of 99.08% and outperformed the evaluated baseline models in terms of precision, recall, F1-score, and AUC, with values of 0.991, 0.990, 0.990, and 0.998, respectively. The results show that the combination of local feature extraction, bidirectional context learning and attention based refinement can improve the discrimination ability of diverse network attacks under the condition of compact architecture. Future work might include real-time deployment, computation profiling, cross-dataset validation, and testing on new and unseen attack patterns. Additional optimization can also be explored in terms of model compression and adaptive learning strategies for resource constrained network environments.

References

1. T. Ahmad and D. Truscan, "Early Detection with Explainability of Network Attacks Using Deep Learning," in 2024 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Toronto, ON, Canada, 2024.

2. Uysal and U. Kose, "Analysis of Network Intrusion Detection via Explainable Artificial Intelligence: Applications with SHAP and LIME," in 2024 Cyber Awareness and Research Symposium (CARS), Grand Forks, ND, USA, 2024.

3. D. Attique, H. Wang, P. Wang, D. Javeed and M. Adil, "EX-DFL: An Explainable Deep Federated-based Intrusion Detection System for Industrial IoT," in 2024 21st International Joint Conference on Computer Science and Software Engineering (JCSSE), Phuket, Thailand, 2024.

4. Mayan, S. Krishanveni and B. Jothi, "AI Enabled Digital Twin Models to Enhance Security in Smart Cities," in 2024 International Conference on Intelligent Computing and Sustainable Innovations in Technology (IC-SIT), Bhubaneswar, India, 2024.

5. Z. Xu and Y. Liu, "Robust Anomaly Detection in Network Traffic: Evaluating Machine Learning Models on CICIDS2017," in 2025 10th International Conference on Electronic Technology and Information Science (ICETIS), Hangzhou, China, 2025.

6. S. Wang, Y. Shi, Z. Duan, G. Zhou and P. Yu, "Research on Lightweight Intrusion Detection Model Based on Improved MobileNetV3," in 2026 IEEE 8th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2026.

7. J. Mohan and R. K. M, "Intelligent Intrusion Detection System Combining Behavioral Analysis and Machine Learning Methods," in 2025 3rd International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2025.

8. R. Sindhula and S. Pradeep, "EFSMDCD: Method for Detecting and Categorizing DoS and DDoS Attacks using Ensemble Feature Selection," in 2025 International Conference on Innovation in Artificial Intelligence and Internet of Things (AIIT), Jeddah, Saudi Arabia, 2025.

9. P. Abdelhalim, A. Abo-alian and N. Badr, "A Hybrid CNN-LSTM-RFE Approach for Network Intrusion System," in 2025 International Conference on Artificial Intelligence Science and Applications in Industry and Society (CAISAIS), Galala, Egypt, 2025.

10. S. Gautam, V. Sharma, D. J. Shah, J. Nariya and P. Panchal, "A Hybrid Approach for Enhanced Security in Network Environments," in 2025 International Conference on Artificial Intelligence and Machine Vision (AIMV), Gandhinagar, India, 2025.

11. J. S., R. B., B. D. and R. C., "Balanced-IDS: A Deep Hybrid Model to Overcome Class Imbalance in Network Intrusion Detection," in 2025 6th International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), Bengaluru, India, 2025.

12. M. R. Ilahi, A. G. Putrada and H. R. P. Sailellah, "R-CICIDS2017: Making the IDS Benchmark Realistic for Quantized Models in IoT Deployments," in 2025 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Bandung, Indonesia, 2025.

13. K. Dudi, M. Singh, D. Kumar, N. Kumar and A. Sharmila, "Explainable and Privacy-Preserving Multi-Class Network Intrusion Detection Using SHAP and LightGBM," in 2025 5th International Conference on Advancement in Electronics & Communication Engineering (AECE), Ghaziabad, India, 2025.

14. G. Ramasamy, T. H. Vardhan and J. Jyoshitha, "AI-Driven Hybrid Intrusion Detection and Prevention with Edge-Cloud Integration and SOC Dashboard," in 2026 8th International Conference on Intelligent Sustainable Systems (ICISS), Tirunelveli, India, 2026.