

Hybrid LSTM–LightGBM Model for Multiclass DDoS Attack Detection in 5G and IoT Networks

Asma Djama

`djama.asma@univ-medea.dz`

University of Médéa

Mohamed Maazouz

University of Médéa

Hamza Kheddar

University of Médéa

Muhammet Ali Akcayol

Research Article

Keywords: DDoS, IDS, LSTM, LightGBM, SHAP, IoT, 5G

Posted Date: August 27th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10749726/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Hybrid LSTM–LightGBM Model for Multiclass DDoS Attack Detection in 5G and IoT Networks

Asma Djama¹, Mohamed Maazouz¹, Hamza Kheddar¹, and Muhammet Ali Akcayol²

¹ LSEA Laboratory, University of Médéa, Médéa 26000, Algeria
djama.asma@univ-medea.dz; maazouz.mohamed@univ-medea.dz;
kheddar.hamza@univ-medea.dz

² Faculty of Engineering, Department of Computer Engineering, Gazi AI Center,
Gazi University, Ankara 06560, Türkiye
akcayol@gazi.edu.tr

Abstract. The Internet of Things (IoT) devices are spreading fast. This is happening at the time as new high-speed communication networks and 5G infrastructures are being built. Because of this there are a lot more Distributed Denial-of-Service (DDoS) attacks happening. These DDoS attacks are also getting more complicated. This is a problem for the systems that are supposed to detect when someone is trying to break in. The DDoS attacks are a challenge, for these systems to deal with this problem. This research suggests a hybrid intrusion detection approach that combines Long Short-Term Memory (LSTM) networks with the Light Gradient Boosting Machine (LightGBM) classifier for efficient multi-class DDoS attack detection. The LSTM module is employed to capture temporal dependencies and sequential traffic patterns, while LightGBM performs fast and accurate classification based on the extracted feature representations. In addition, SHapley Additive exPlanations (SHAP) are incorporated to enhance the suggested framework's interpretability by determining the key elements influencing the detection process. we use in our model three datasets: CICIDS2017, CIC-DIAD2024 and CICIoT2023. the results show that the framework achieves magnificence in multi-class classification performance, achieving accuracy of 97.80%, and precision of 97.60%, recall of 97.70% and F1-score of 97.60% on the CIC-DIAD2024 dataset, achieve a precision 97.60%, accuracy of 96.80%, recall 97.70%, and F1-score of 97.60% on CICIoT2023. Furthermore, the proposed model reaches an overall accuracy of 99.89% on the CICIDS2017 benchmark dataset. The framework also maintains very low inference latency, making it useful for real time IoT intrusion detection. Experimental results confirm that the combination of gradient boosting for temporal feature learning greatly improves good detection accuracy, robustness, computational activity and the interpretability, and so on making the proposed framework a useful approach for improving the security of future IoT and 5G networks.

Keywords: DDoS, IDS, LSTM, LightGBM, SHAP, IoT, 5G .

1 Introduction

The fast growth of communication networks, particularly the rollout of 5G and high-speed Internet infrastructure, has sharply increased the volume, velocity and variety of network traffic [1]. These advances allow for ultra-low latency and massive connectivity but also introduce new security challenges. DDoS attacks are one of the most dangerous threats communication networks. These attacks are made to stop network services by sending too much traffic to the target system [2]. The DDoS attacks are hard to detect and mitigate by traditional security methods and signature-based security mechanisms because the attacks change over time, generate a large amount of traffic, and use new attack methods [3].

Traditional machine learning based DDoS detection methods depend on hand-crafted features and static properties of the traffic [4]. These methods may perform well in controlled environments but often do not generalise to real world scenarios, especially when dealing with high dimensional data, temporal dependencies and imbalanced traffic distributions [5]. At the same time, deep learning methods have shown strong ability to automatically learn complex different patterns in large network data. Recurrent neural networks (RNNs), and mostly LSTM networks, are well good for modeling sequential and temporal traffic behavior, making them successful for capturing the evolving dynamics of network attacks [6, 7]

Despite the advantages of deep learning models, they are usually accompanied by high computational complexity, long training times and limited interpretability, which can hinder their deployment in real-time network security systems [8]. On the other hand, gradient boosting decision tree models, e.g. LightGBM, have attracted attention due to their high efficiency, scalability and robustness in dealing with large, high-dimensional and imbalanced data [9]. LightGBM offers training and inference very fast with strong classification performance, making it a compelling solution for network intrusion detection tasks [10].

In this paper, we propose a hybrid LSTM-LightGBM based DDoS detection framework to benefit from both deep learning and machine learning. The proposed approach uses the LSTM network to extract discriminative temporal features from network traffic flows, capturing long-term dependencies and sequential behaviour [11]. These learned features are then fed to a LightGBM classifier for perfect multiclass attack classification. This model integrates temporal feature learning and efficient gradient boosting classification to succeed high detection accuracy with reduced computational overhead.

The essential contributions of this work summarised as following we :

- propose a hybrid LSTM-LightGBM framework that can successfully capture temporal and sequential traffic patterns for multiclass DDoS attack detection.
- behavior extensive experiments to estimate the performance of the presented model on a benchmark DDoS dataset.

- Show that the hybrid approach is more accurate and robust than traditional machine learning and standalone deep learning models, and is computationally efficient enough for real-time applications.

The rest of the paper is organised as follows. Section 2 goes through the related work on DDoS detection using machine learning and deep learning. The proposed methodology of hybrid LSTM–LightGBM is discussed in Section 3. Section 4 describes the experimental setup and evaluation results. Finally, Section 5 conclude the paper and presents future research directions.

2 Related Work

The rapid growth of IoT environments has dramatically expanded the attack surface of modern networks, leaving them especially susceptible to DDoS attacks. As a result, the design of efficient IDS capable of accurately identifying DDoS traffic in IoT contexts has attracted considerable research attention in recent years. Existing IDS solutions can be broadly categorized into : traditional machine learning based approaches, and deep learning based approaches, and hybrid models that combine the strengths of both paradigms or combine with method of statistical or optimization or Blockchain.

Early studies on IoT-based DDoS detection primarily relied on traditional machine learning algorithms such as Support Vector Machines, Random Forests, Decision Trees and gradient boosting techniques. These methods demonstrated relatively Offering precise detection without heavy computational costs, they are well-suited for resource-limited IoT devices. Recent work evaluating ensemble models on modern IoT datasets reported promising results. [23] The authors proposed a hybrid intrusion detection framework named DeepCLG, that combines CNN, LSTM, and Leveraging GRU and Capsule Networks to strengthen security and detect attacks in Industrial IoT environments .The framework achieved 99.82% accuracy on the CICIoT2023 dataset and 95.55% accuracy on the UNSW-NB15 dataset. However, combining several deep learning architectures raises the computational cost and model complexity, which could make real-time deployment difficult in IIoT contexts with limited resources. Recently, the study Irankunda et al. Presented an XGBoost-driven CNN-LSTM framework designed for detecting DDoS attacks in Industrial IoT environments in real time [14] . The approach combine with XGBoost-based feature selection with CNN-LSTM networks to extract spatial and temporal characteristics from IoT network. Experimental results proved high detection performance on 3 datasets LR-HR DDoS 2024, UNSW-NB15, and CICIoT2023 datasets, achieving accuracy values of 99.25%, 99.31%, and 93.33%, respectively. However, the integration of multiple deep learning components and feature selection mechanisms increases model complexity and computational requirements, which may limit deployment in resource-constrained IoT environments.

[12]Gaurav et al. proposed an optimized IoT cyberattack detection framework based on Random Forest feature selection and LightGBM classification.

Table 1. Summary of Existing IDS Approaches for IoT DDoS Detection

Reference	Research Objective	Techniques	Environment	Dataset	Advantages	Limitations
[12]	IoT cyberattack detection using optimized machine learning	Random Forest feature selection + LightGBM classifier	IoT networks	IoT traffic dataset	Efficient classification with reduced computational complexity and fast inference	Depends on handcrafted statistical features and cannot capture temporal dependencies of network traffic
[13]	IoT intrusion detection based on spatial-temporal traffic analysis	CNN + LSTM hybrid architecture	IoT networks	CICIoT2023	Combines CNN feature extraction with LSTM temporal learning to improve attack detection performance	High computational cost and increased model complexity for real-time deployment
[14]	Real-time DDoS detection in Industrial IoT	CNN-LSTM + XGBoost	Industrial IoT	LR-HRDDoS2024, UNSW-NB15, CICIoT2023	Combines feature selection with spatial-temporal learning and achieves high detection accuracy	Complex architecture and high computational requirements
[15]	Hybrid DDoS attack detection in Named Data Networking	Multi-feature fusion + Bayesian optimized XGBoost	NDN networks	NDN traffic dataset	Improves classification performance through optimized gradient boosting and feature fusion	Evaluation is limited to NDN environments and depends on manually engineered features
[16]	Anomaly detection in fog computing environments	Autoencoder + Isolation Forest	Fog-IoT networks	Fog computing traffic	Provides unsupervised feature extraction with low computational overhead	Restricted to binary intrusion detection and cannot classify multiple attack categories
[17]	Deep feature extraction for automated attack detection	Autoencoder + XGBoost classifier	Cybersecurity applications	SQL injection dataset	Achieves efficient feature representation and strong classification capability	Designed for textual attack detection rather than IoT network traffic and DDoS analysis
[18]	XAI-enhanced hybrid framework for IoT device identification and attack detection	CNN + XGBoost + SHAP	IoT device identification and attack detection	CIC IoT2024-DIAD	Achieves up to 99.92% accuracy while providing interpretable predictions through SHAP-based feature attribution	Does not explicitly model temporal dependencies in network traffic, limiting its ability to distinguish sequential DDoS attack patterns
[19]	Review of deep learning-based autonomous anomaly detection in SDN-IoT	CNN, RNN, LSTM, Autoencoder, and hybrid DL models	SDN-IoT networks	Multiple benchmark datasets	Provides comprehensive analysis of DL approaches and identifies future research challenges	Survey-based study without experimental validation of a proposed IDS framework
[20]	Explainable and privacy-preserving IDS	LightGBM + Optuna + SHAP	Network intrusion detection	CICIDS2017	Enhances interpretability and privacy while maintaining robustness against adversarial attacks	Lacks temporal feature extraction and sequential traffic modeling
[21]	Federated IoT intrusion detection using advanced hybrid learning	Transformer + LoRA + XGBoost fusion	Federated IoT networks	CICIoT2023	Improves minority attack detection and reduces communication overhead using parameter-efficient learning	Requires federated infrastructure and introduces additional deployment complexity
[22]	Comprehensive review of deep learning-based IDS evolution	CNN, RNN, LSTM, GNN, Autoencoder, Transformer	IoT and cyber networks	Multiple datasets	IDS	Highlights recent advances, challenges, and future directions including XAI and lightweight IDS
This Work	DDoS detection with temporal learning and explainable decisions	LSTM-based feature extraction + LightGBM classifier + SHAP explanation	5G IoT environments	CICIDS2017 + CICIoT2023 + CICIoT-DIAD2024	Combines temporal dependency modeling, efficient gradient boosting classification, cross-dataset evaluation, and explainable AI-based prediction analysis	Requires optimization of the two-stage training pipeline and feature extraction process

The selected features were used to train the LightGBM classifier, which was compared with several conventional machine learning algorithms. The results demonstrated the effectiveness of LightGBM for IoT attack detection while reducing the computational complexity associated with high-dimensional traffic data. But, the proposed approach relies mainly on handcrafted statistical features and does

not model temporal dependencies among sequential network flows, which may limit its capability in detecting evolving .

Hybrid deep learning architectures combining CNN and LSTM models have been investigated to simultaneously capture spatial and temporal characteristics of network traffic. The CNN component extracts discriminative traffic patterns, while the LSTM component models sequential dependencies among network flows. The CNN-LSTM approach reported in [13] demonstrated promising performance on the CICIOT2023 dataset for IoT intrusion detection. However, the integration of multiple deep learning modules increases architectural complexity and computational requirements, which may challenge their deployment in resource-constrained IoT environments. More recently, the CICIOT-DIAD 2024 dataset was introduced to address the limitations of earlier IoT datasets by incorporating more realistic IoT device behaviors and refined DDoS attack scenarios. Using this dataset, [18] Jain et al. proposed an XAI-enhanced hybrid deep learning framework that combines XGBoost and CNN for IoT device recognizing and attack detection. The framework incorporates SHAP to provide interpretable predictions by identifying the most important features used by the model to make each decision . The proposed model achieved up to 99% accuracy on the CIC IoT2024-DIAD dataset, showing the excellent classification performance while keeping the model interpretability. But the framework is primarily designed for IoT device identification, and does not explicitly model over time in network traffic, which are important for detecting DDoS attacks. Recent advances in hybrid intrusion detection have demonstrated the benefits of integrate deep learning feature extractors and machine learning classifiers to enhance detection performance and computational efficiency in IoT environments. Moreover, Explainable and private intrusion detection has recently gained increasing attention due to the need for transparent and trustworthy security solutions. Dudi *et al.* [20] developed a IDS privacy-preserving framework using LightGBM with Optuna optimisation, differential privacy methods and feature attribution based on SHAP. We evaluated the proposed framework on the benchmark dataset CICIDS2017 and attained an 89.4% F1-score. The framework is robust against adversarial perturbations and preserves the data privacy. The main concern of this work is privacy preservation and model interpretability, rather than temporal modelling of network traffic. Hence, the framework does not explicitly model the sequential dependency between traffic flows to differentiate complex and evolving DDoS attack patterns.

In this regard, Yasarathna *et al.* [19] have surveyed the state-of-the-art of autonomous anomaly detection (AAD) in SDN-IoT networks using deep learning. The survey studies different deep learning architectures like CNNs, RNNs, LSTMs, and autoencoders to detect DDoS attacks and other cyber threats. The authors highlighted the strengths of deep learning methods in achieving high detection accuracy and also discussed important challenges related to scalability, real-time processing and deployment in IoT contexts with limited resources. However, as a survey study, it does not introduce or experimentally validate a

new IDS framework, limiting its contribution to the analysis of existing techniques and the identification of future research directions.

[15]Liu et al. proposed an improved XGBoost-based intrusion detection framework for identifying hybrid DDoS attacks in Named Data Networking (NDN). The proposed method integrates multi-feature fusion and Bayesian hyperparameter optimization to enhance attack detection and classification. Experimental results demonstrated that the model achieved an AUC of 0.9746, outperforming conventional machine learning methods, including XGBoost, KNN, AdaBoost, and Decision Tree. However, the framework was evaluated only in an NDN environment and relies on handcrafted network features, which may limit its generalization to heterogeneous IoT networks and emerging attack scenarios. Similarly, Autoencoder-based hybrid approaches have attracted considerable attention for anomaly detection. [16] Sadaf and Sultana proposed an intrusion detection framework, named Auto-IF, for fog computing environments. The proposed approach combines an AE for feature extraction with an Isolation Forest (IF) algorithm for binary intrusion detection, enabling efficient discrimination between normal and malicious network traffic. Experimental results demonstrated that the framework achieved excellent detection efficiency with minimal computational overhead, making it suitable for fog-based IoT environments. However, the model is limited to binary classification and does not support the identification of multiple attack categories, which restricts its applicability to complex real-world intrusion detection scenarios. To further enhance classification performance, several studies combined Autoencoders with ensemble classifiers. For example, [17]An autoencoder-based system called AE-Net was presented by Thalji et al. for automated SQL injection attack detection. In their method, high-level deep features are extracted from SQL queries using an autoencoder, which are subsequently classified using machine learning algorithms. Experimental results show that the XGBoost classifier achieves 99% accuracy and outperforms the existing methods. However, the framework is specifically designed for SQL injection detection based on textual SQL data, which limits its applicability for network traffic analysis and DDoS detection in IoT environment. Transformer based models are also emerging as strong alternatives for Intrusion detection due to their ability to capture long range dependencies via self attention mechanisms. Muthuswamy et al. [21] introduced a hybrid Transformer and XGBoost framework for federated intrusion detection in IoT. We propose a novel architecture combining a Transformer with Low-Rank Adaptation (LoRA), an XGBoost classifier and a learnable fusion head to improve intrusion detection in federated learning. We evaluated the proposed framework on the CICIoT2023 dataset, and it improved the detection performance of minority attack classes and reduced the communication overhead by sharing parameters with LoRA. However, the dependence on federated learning infrastructure and numerous integrated components results in a complicated system with deployment overhead, which might not be suitable for resource-limited IoT environments. Furthermore, in their recent exhaustive survey, Lal and Ashok [22]have talked about the development of deep learning-based network intrusion detection systems, including

CNNs, RNNs, LSTMs, and autoencoders. hybrid CNN-LSTM models, Graph Neural Networks, and Transformer-based approaches. The survey revealed the effectiveness of the Transformer-based models to learn complex traffic dependencies and pointed out emerging research directions including explainable AI, federated learning, adversarial robustness and lightweight hybrid architectures. However, it also noted that the effective balance between detection accuracy, computational efficiency and generalisation is still a challenge.

However, despite some promising results reported in the recent literature, there are some critical limitations. Most existing works only evaluate their models on a single benchmark dataset, such as CICIoT2023 , CICIoT-DIAD2024 , or CICIDS2017 , without exploring the generalisation ability across multiple datasets. In addition, deep learning based approaches usually have good detection accuracy despite its computational complexity, whereas traditional machine learning methods are more efficient but cannot capture the dependence of network traffic in temporal domain. Although recent studies have improved model transparency by implementing explainable AI approaches like SHAP, they generally rely on static feature representations and do not integrate temporal sequence learning. To the best of our understanding, No prior study has combined LSTM-based temporal feature extraction with LightGBM classification while comprehensively evaluating the framework on the CICIoT2023, CICIoT-DIAD2024, and CICIDS2017 benchmark datasets for multi-class DDoS attack detection.

These observations motivate the development of a hybrid IDS framework that leverages the temporal modeling capability of LSTM networks to extract sequential features from IoT traffic, followed by LightGBM for efficient and scalable classification. Such an approach aims to balance detection accuracy, It is appropriate for real-time DDoS detection in contemporary IoT setups due to its computational efficiency and generalisation capability.

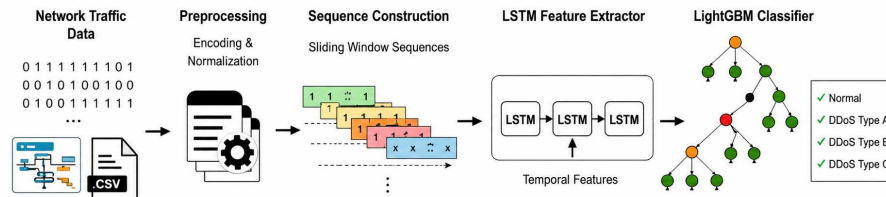


Fig. 1. Overview of the proposed hybrid LSTM–LightGBM framework for binary and multi-class DDoS attack detection in IoT networks

3 Proposed Methodology

For effective multi-class DDoS attack detection in Internet of Things environments, this research suggests a hybrid intrusion detection architecture that combines LSTM networks with Light GBM. The suggested method makes use of LSTM's temporal modelling capabilities to extract sequential traffic patterns and the high classification efficiency of LightGBM to achieve accurate and scalable detection. The four primary phases of the proposed framework's general architecture are depicted in Fig. 1: data preprocessing, temporal sequence construction, LSTM-LightGBM-based categorisation and feature extraction, Algorithm 1 and table 2 outlines the general process of the suggested hybrid LSTM-LightGBM structure.

Algorithm 1: Hybrid LSTM + LightGBM IDS for Multi-class DDoS Detection

Input: Dataset D with features X and labels y , sequence length SEQ_LEN
Output: Trained Hybrid IDS model and predictions $\hat{y}$

- 1 **Preprocessing:** clean dataset, encode categorical features, scale numeric features, encode labels
- 2 **Create sequences:** sliding windows of length SEQ_LEN
- 3 **Split dataset:** stratified train/test split
- 4 **Initialize LSTM:** define LSTM model, optimizer, loss
- 5 **Train LSTM:** forward pass, compute loss, backpropagate, validate
- 6 **Extract features:** LSTM outputs for train/test
- 7 **Train LightGBM:** fit on LSTM features
- 8 **Predict and evaluate:** Accuracy, Precision, Recall, F1, Confusion Matrix, ROC-AUC
- 9 **Output:** trained model and evaluation metrics

3.1 Data Collection and Preprocessing

Network traffic data are collected from multiple CSV files representing heterogeneous IoT traffic sources and attack categories. Each file is treated as a distinct domain to enable cross-domain learning. To ensure scalability and memory efficiency, a fixed number of samples is selected from each file.

During preprocessing, missing and infinite values are removed to improve data quality. Categorical features are transformed using ordinal encoding, but standard scaling is used to normalise numerical features. The attack labels are encoded into numerical form to facilitate supervised learning. This process results in a clean and standardized dataset suitable for sequential modeling.

3.2 Temporal Sequence Construction

DDoS attacks exhibit strong temporal characteristics such as burst behavior and sustained traffic anomalies. To capture these patterns, raw traffic flows are

converted utilising a sliding window approach to create fixed-length sequences. Given a sequence length T , consecutive traffic records are grouped as:

$$X_i = \{x_i, x_{i+1}, \dots, x_{i+T-1}\}$$

where the corresponding label is assigned based on the last element of the sequence. This representation enables the model to learn short-term temporal dependencies across network flows.

3.3 LSTM-Based Feature Extraction

An LSTM network is employed as a temporal feature extractor to model the sequential behavior of network traffic. The LSTM processes each input sequence and updates its internal memory states to capture temporal correlations.

For each input eventually, the LSTM final hidden state is taken out and utilise as a condensed depiction of the traffic sequence. This hidden state encodes discriminative temporal features that characterize normal and attack traffic patterns while reducing the original feature spaces dimensionality is displayed in table 2. To guarantee that the retrieved characteristics are optimised for DDoS attack discrimination, the LSTM is trained under supervision.

3.4 Light GBM Classifier

After temporal feature extraction using LSTM, classification is performed using Light GBM ,Fig 2 illustrates a successful Gradient Boosting Decision Tree (GBDT) implementation. LightGBM’s rapid training speed has led to its widespread use in intrusion detection studies, low memory usage, and strong performance on large-scale and imbalanced network datasets [9, 24].

LightGBM builds a sequential ensemble of decision trees, each of which is trained to fix the mistakes of its predecessors. The definition of the model prediction at iteration m is:

$$F_m(x) = F_{m-1}(x) + \eta h_m(x)$$

where $h_m(x)$ represents the newly added tree and η is the learning rate.

Unlike traditional boosting algorithms, LightGBM introduces several optimization mechanisms:

- Leaf-wise tree growth, which improves accuracy by choosing the leaf with the greatest loss reduction [9].
- Histogram-based feature binning, reducing memory usage and accelerating training.
- Gradient-based One-Side Sampling (GOSS), which eliminates less informative samples and keeps samples with large gradients.
- Exclusive Feature Bundling (EFB), which reduces dimensionality by combining sparse features.

These characteristics make LightGBM particularly suitable for DDoS detection, where traffic data are high-dimensional, highly imbalanced, and generated at high speed. In the proposed hybrid framework, LightGBM operates on LSTM-extracted temporal features to provide accurate and computationally efficient multi-class attack classification.

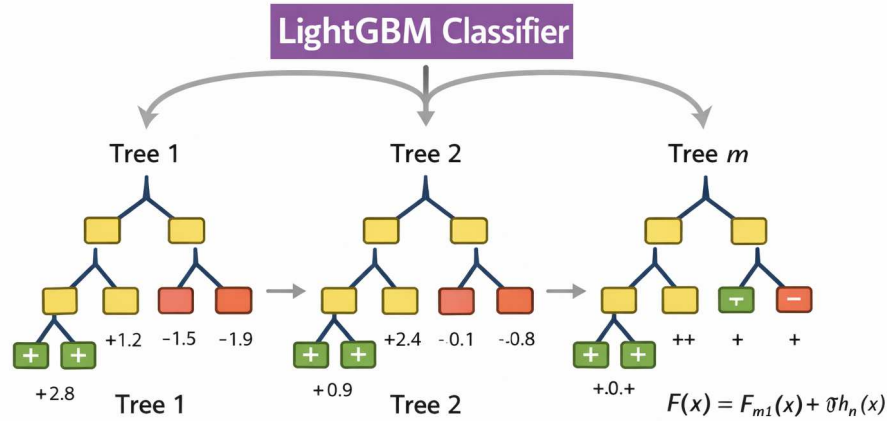


Fig. 2. Structure of LightGBM based on Gradient Boosting Decision Trees

3.5 Model Advantages

The proposed hybrid architecture offers several advantages:

- Effective modeling of temporal dependencies using LSTM.
- Reduced computational complexity through compact feature extraction.
- High classification accuracy and scalability using LightGBM.
- suitability for real-time implementation in IoT contexts with limited resources.

These characteristics make the proposed approach a practical and robust solution for DDoS attack detection in modern IoT networks.

4 Experimental Setup and Evaluation

This section describes the datasets used for validation, the experimental configuration, and the evaluation metrics used to gauge how well the suggested hybrid LSTM-LightGBM intrusion detection framework.

Table 2. Architecture Summary of the Proposed Hybrid LSTM-LightGBM Framework

#	Layer/Module	Units	Output Shape	Function
1	Input Features	–	(None, 40)	Input network traffic features
2	Feature Normalization	–	(None, 40)	Standardize numerical features
3	Sequence Generation	–	(None, 5, 40)	Construct temporal sequences
4	LSTM Layer 1	64	(None, 5, 64)	Learn temporal dependencies
5	Dropout	0.2	(None, 5, 64)	Reduce overfitting
6	LSTM Layer 2	64	(None, 64)	High-level temporal feature extraction
7	Feature Vector	64	(None, 64)	Latent temporal representation
8	LightGBM Classifier	600 Trees	–	Gradient boosting classification
9	Prediction Output	C	(None, C)	Binary or multi-class prediction

Table 3. Overview of the datasets used in this study

Attribute	CIC-IDS2017	CIC-IoT2023	CIC-DIAD2024
Traffic Classes	6 classes	12 classes	12 classes
Benign Samples	366,651	49,995	49,996
Malicious Samples	33,034	396,533	450,533
Input Features	79 network-flow features	40 network-flow features	40 network-flow features
Attack Profile	DDoS, DoS, Slowloris, FTP-Patator, PortScan, and Web Attack–Brute Force	Flooding and fragmentation attacks including TCP, HTTP, ICMP, SYN, UDP, ACK, UDP and ICMP Fragment, PSHACK, RSTFIN, SlowLoris, and SynonymousIP	DoS-UDP, TCP, HTTP, ICMP, and ICMP Fragment, PSHACK, RSTFIN, SlowLoris, and SynonymousIP attacks

4.1 Datasets Description

Three benchmark intrusion detection datasets were taken into consideration in order to assess the efficacy, resilience, and generalisation potential of the suggested hybrid LSTM-LightGBM framework: CICIDS2017 [25], CICIoT2023 [26], and CICDIAD2024 [27]. These datasets were selected because they represent different network environments, including traditional network infrastructures and modern IoT scenarios. The main characteristics Table 3 provides an overview of the adopted datasets, including the quantity of traffic samples and extracted features.

All datasets were processed using a unified preprocessing strategy to ensure a fair comparison between different evaluation scenarios. The original traffic classes were analyzed, and only benign traffic and DDoS-related categories were retained in this study to focus on DDoS attack detection. The selected features were normalized, encoded, and prepared according to the requirements of the proposed hybrid architecture.

CICIDS2017 is a widely adopted intrusion detection dataset that contains realistic network traffic generated from different attack scenarios. It includes both regular operations and a number of malevolent ones, such as DDoS attack. In this work, only benign and DDoS traffic samples were selected from the dataset

Table 4. Distribution of traffic types in the CICIDS2017 dataset

Traffic Type	Category	Samples
BENIGN	Normal	366,651
DDoS	Attack	23,865
FTP-Patator	Attack	5,192
DoS-Slowloris	Attack	2,661
Web Attack-Brute Force	Attack	1,082
PortScan	Attack	234
Bot	Attack	2
Total		399,687

Table 5. Summary of Traffic Types and Samples Of CICIOT DIAD2024

Traffic Type	Category	Samples
DDoS-ACK-Fragmentation.pcap	DDoS	9999
DDoS-HTTP-Flood-.pcap	DDoS	10000
DDoS-ICMP-Fragmentation.pcap	DDoS	10000
DDoS-ICMP-Flood.pcap	DDoS	9999
DDoS-SlowLoris.pcap	DDoS	10000
DDoS-PSHACK-Flood.pcap	DDoS	10000
DDoS-RSTFINFlood.pcap	DDoS	10000
DDoS-UDP-Fragmentation.pcap	DDoS	9999
DDoS-SYN-Flood.pcap	DDoS	10000
DDoS-TCP-Flood.pcap	DDoS	9999
DDoS-SynonymousIP-Flood.pcap	DDoS	10000
BenignTraffic.pcap	Normal	10000

Table 6. Distribution of Traffic Types in the Dataset with Category

Traffic Type	Category	Samples
DDoS-HTTP_Flood-.pcap	DDoS	10000
DDoS-ICMP_Fragmentation.pcap	DDoS	10000
DDoS-PSHACK_Flood.pcap	DDoS	10000
DDoS-SlowLoris.pcap	DDoS	10000
DDoS-SynonymousIP_Flood.pcap	DDoS	10000
DDoS-SYN_Flood.pcap	DDoS	10000
DDoS-RSTFINFlood.pcap	DDoS	10000
DDoS-ACK_Fragmentation.pcap	DDoS	9999
DDoS-ICMP_Flood.pcap	DDoS	9999
DDoS-UDP_Fragmentation.pcap	DDoS	9999
DDoS-TCP_Flood.pcap	DDoS	9999
BenignTraffic.pcap	Normal	9999

to construct the evaluation scenarios. This allows the proposed framework to be assessed specifically for DDoS detection while maintaining realistic network characteristics show table Table 4.

CICIoT2023 is an extensive IoT-focused intrusion detection dataset created with realistic IoT network environments. It contains traffic generated from heterogeneous IoT devices under normal and attack conditions. Among the available traffic categories, DDoS-related attacks were extracted together with benign samples for the experimental evaluation. The detailed distribution of the selected traffic categories and Table 6 displays the quantity of samples used in this investigation.

CICDIAD2024 is a recent IoT intrusion detection dataset designed to represent emerging attack behaviors targeting connected devices and modern network environments. Similar to CICIoT2023, The dataset includes both legitimate and malicious communications produced in various contexts. In this research, only DDoS attack categories and To create the binary and multi-class DDoS detection tasks, benign traffic was taken into account. The distribution of the selected traffic classes used in the experiments is reported in Table 5.

The adoption of these three heterogeneous datasets provides a comprehensive evaluation of the proposed model under diverse traffic characteristics and attack distributions. This test with different sets of data helps us see if the new system can really find DDoS attacks correctly and reliably in all kinds of Internet of Things devices and networks. The system has to be good at finding DDoS attacks in different situations so this test is very important for the proposed framework and its ability to detect DDoS attacks. The proposed framework needs to be able to detect DDoS attacks, in IoT and network environments.

4.2 Experimental Configuration

Every experiment was carried out using Python in a supervised learning setting. The proposed hybrid intrusion detection framework was implemented using TensorFlow/Keras for temporal feature extraction and LightGBM for classification. Data preprocessing, feature normalization, label encoding, and The Scikit-learn library was used to evaluate performance. The experimental hyperparameters are summarized in Table 7. The trials were conducted using Google Colab, which provides cloud-based computing capabilities such as an Intel Xeon CPU, an NVIDIA GPU, and 12 GB of RAM. The proposed framework was implemented using Python, Scikit-learn, and TensorFlow/Keras. For each dataset, the samples were randomly shuffled and split into 80/20 training and testing sections. To guarantee an objective assessment, the testing subset was set aside just for performance evaluation, whereas the training subset was utilised for model learning.

To reduce computational cost while preserving class balance, an equal number of samples was randomly selected from each attack category and the benign traffic class. To ensure a fair and repeatable comparison, the same preprocessing pipeline and experimental parameters were used consistently to the CICIDS2017, CICIoT2023, and DIAD2024 datasets.

Table 7. Experimental hyperparameter settings

Parameter	Value
Programming language	Python
Framework	TensorFlow/Keras + LightGBM
Random seed	42
Optimizer	Adam
Learning rate	0.001
Batch size	128
Training epochs	30
LSTM hidden units	64
LSTM layers	2
Dropout rate	0.2
Sequence length	5
Train/Test split	80% / 20%
Maximum samples per CSV file	10,000
Feature scaling	StandardScaler
Label encoding	LabelEncoder
LightGBM Hyperparameters	
Objective	Multiclass
Number of estimators	200
Learning rate	0.05
Maximum depth	Unlimited (-1)
Number of leaves	31
Feature fraction	0.8
Bagging fraction	0.8
Number of classes	Automatic

The Adam optimiser was used to train the LSTM network with a batch size of 128 and a learning rate of 0.001 over 30 epochs. The extracted temporal feature representations were then used as input to the LightGBM classifier. Two experimental configurations were evaluated throughout this study:

- **LightGBM only:** LightGBM was trained directly on the preprocessed tabular features without temporal modeling [9].
- **Hybrid LSTM–LightGBM (Proposed):** The LSTM network was first employed to learn temporal dependencies from sequential traffic data. The extracted high-level feature representations were subsequently classified using the LightGBM model, forming the proposed hybrid intrusion detection framework [9, 28].

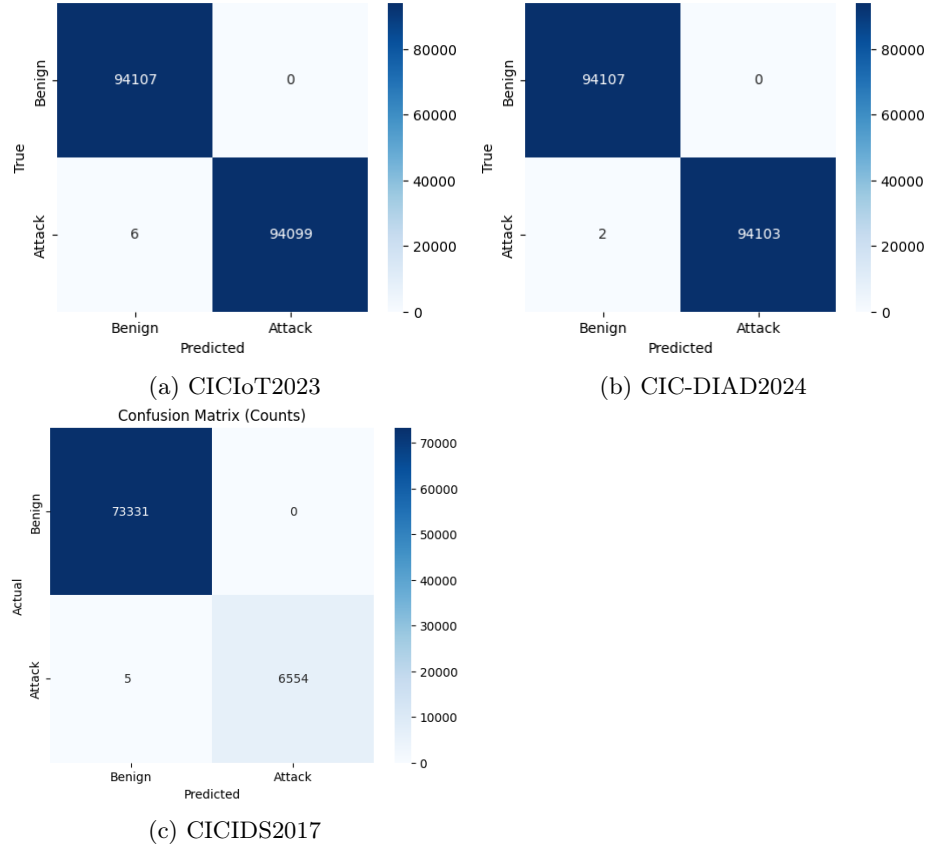


Fig. 3. Normalized confusion matrices of representative baseline models on CIC-DIAD2024 and CIC-IoT2023 and CICIDS2017 of hybrid LSTM–LIGHTGBM model binary classification

4.3 Evaluation Metrics

The suggested framework’s effectiveness is assessed using typical classification metrics used in intrusion detection studies [29, 30]. These metrics include accuracy, precision, recall, and F1-score, defined as:

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

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

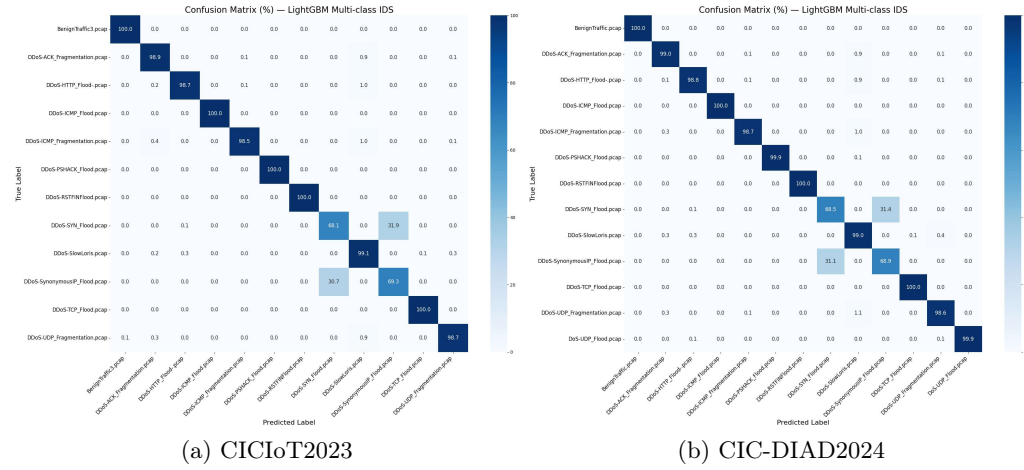


Fig. 4. Normalized confusion matrices of representative baseline models on CIC-DIAD2024 and CIC-IoT2023 with LightGBM only

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

where true positives, true negatives, false positives, and false negatives are represented by TP , TN , FP , and FN , respectively.

In imbalanced DDoS assault circumstances, where accuracy alone may be deceptive, these metrics offer a thorough assessment of detection capability.

4.4 Performance Analysis Strategy

The efficacy of the suggested hybrid strategy is demonstrated by comparing performance results on both datasets before and after adding LSTM. The importance of understanding temporal dependencies for DDoS attack detection is demonstrated by the rise in detection accuracy and F1-score [30].

By examining the training and inference behaviour, the hybrid model's computing efficiency is also examined, suggesting that it is appropriate for large-scale, real-time IoT security deployments. The suggested hybrid LSTM–LightGBM framework is thoroughly evaluated in this section using the CICIoT2023 [26], CICDIAD2024 [27], and CICIDS2017 [25] datasets. When compared to a baseline LightGBM classifier, the findings show both detection performance and computing economy.

5 Results and Discussion

This section gives a complete evaluation of the proposed hybrid LSTM–LightGBM framework using the CICIoT2023 and CIC-DIAD2024 and CICIDS2017 datasets.

The trials are undertaken for both binary and multiclass DDoS attack detection. The suggested model is assessed using multiple performance metrics, including Accuracy, Precision, Recall, F1-score, and ROC-AUC. Furthermore, confusion matrices, ablation experiments, SHAP explainability analysis, and comparisons with recent state-of-the-art methodologies are offered to demonstrate the effectiveness, robustness, and interpretability of the proposed framework.

5.1 Binary Classification Results

The first experiment evaluates the ability of the proposed framework to separate benign traffic from malicious DDoS traffic. For this purpose, For binary classification, every attack type was treated as one attack class, resulting in a binary classification problem. The obtained results of the proposed LSTM–LightGBM framework on the CIC-IoT2023, CIC-DIAD2024, and CIC-IDS2017 datasets are presented in Table 8. Figure 3 presents the confusion matrices ob-

Table 8. Performance Evaluation of the Proposed Hybrid LSTM–LightGBM Model Binary Classification

Data set	CIC-IoT2023	CIC-DIAD2024	CIC-IDS2017
Metric	Value	Value	Value
Accuracy (%)	99.9989	100.0000	100.0000
Precision (%)	100.0000	99.9999	100.0000
Recall (%)	99.9979	100.0000	100.0000
F1-score (%)	99.9989	99.9997	100.0000
AUC	1.0000	1.0000	1.0000

tained by the proposed hybrid LSTM–LightGBM framework for binary classification on the CIC-IoT2023, CIC-DIAD2024, and CICIDS2017 datasets. For both CIC-IoT2023 and CIC-DIAD2024, all benign traffic samples were correctly identified, while only six and two attack samples, respectively, were incorrectly classified as benign. Similarly, on the CICIDS2017 dataset, all benign samples were correctly classified, with only five attack instances misclassified. The strong concentration of values along the main diagonal confirms the excellent discrimination capability of the proposed framework. These observations are consistent with the quantitative results reported in Table 8, where the proposed model achieves nearly perfect Accuracy, Precision, Recall, F1-score, and AUC across the three datasets. In general, the confusion matrices show that the proposed hybrid framework can reduce both false positive and false negative predictions, which indicates its robustness for binary intrusion detection in heterogeneous network environments.

5.2 Multi-Class Classification Results

The findings presented in Table 9 confirm the effectiveness of integrating the LSTM temporal feature extractor with the LightGBM classifier.

Table 9. Multi-class Classification Performance Comparison Before and After Integrating LSTM

Dataset	Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
CIC-DIAD2024	LightGBM Only	94.37	94.40	94.37	94.36
	LSTM-LightGBM (Proposed)	97.8	97.6	97.7	97.6
CIC-IoT2023	LightGBM Only	94.40	94.42	94.40	94.40
	LSTM-LightGBM (Proposed)	96.8	97.6	97.7	97.6
CIC-IDS2017	LightGBM Only	98.556	99.736	98.556	99.057
	LSTM-LightGBM (Proposed)	99.899	99.899	99.899	99.893

For the CIC-DIAD2024 dataset, the proposed LSTM-LightGBM framework improves the accuracy from 94.37% using LightGBM alone to 97.80%. Similarly, the F1-score increases from 94.36% to 97.60%, showing that temporal information extracted by LSTM helps to better distinguish DDoS categories with similar statistical characteristics.

For the CIC-IoT2023 dataset, the proposed framework achieves an overall accuracy of 96.80% compared with 94.40% for LightGBM. The improvement in recall from 94.40% to 97.70% indicates that the hybrid architecture reduces missed detections and improves the recognition of difficult attack patterns.

For CICIDS2017, LightGBM already achieves high performance; however, adding the LSTM module further improves the accuracy from 98.56% to 99.89%. This confirms that temporal sequence modeling provides additional discriminative features even when the statistical characteristics of attacks are already well separated.

Overall, the comparison confirms that the LSTM module provides complementary temporal representations, while LightGBM efficiently performs the final classification. The combination of both models results in a more robust and accurate DDoS detection framework.

5.3 Per-Class Classification Analysis

To provide a more comprehensive evaluation of the proposed hybrid LSTM-LightGBM framework, a class-wise performance analysis is conducted on the CIC-DIAD2024, CIC-IoT2023, and CICIDS2017 datasets. Unlike the overall performance metrics presented previously, the per-class analysis provides detailed insight into the capability of the proposed model to correctly identify each individual attack category as well as benign traffic.

Table 10 presents the classification results for the CIC-DIAD2024 dataset. Overall, the proposed framework achieves excellent performance for most traffic categories, with precision, recall, as well as F1-score values near or comparable to 1.00. The great discriminative ability of the suggested model is demonstrated by the nearly perfect classification of BenignTraffic, DDoS-ICMP_Flood, DDoS-PSHACK_Flood, DDoS-RSTFINFlood, and DDoS-TCP_Flood. The lowest performance is observed for DDoS-SYN_Flood and DDoS-SynonymousIP_Flood,

Table 10. Classification Results per Traffic Type (DIAD2024)

Traffic Type	Precision	Recall	F1-score	Samples
BenignTraffic	1.00	1.00	1.00	1500
DDoS-ACK_Fragmentation	0.99	0.99	0.99	1499
DDoS-HTTP_Flood	0.99	0.98	0.99	1500
DDoS-ICMP_Flood	1.00	1.00	1.00	1500
DDoS-ICMP_Fragmentation	1.00	0.99	0.99	1500
DDoS-PSHACK_Flood	1.00	1.00	1.00	1500
DDoS-RSTFINFlood	1.00	1.00	1.00	1500
DDoS-SYN_Flood	0.85	0.79	0.82	1500
DDoS-SlowLoris	0.96	0.99	0.97	1500
DDoS-SynonymousIP_Flood	0.80	0.86	0.83	1500
DDoS-TCP_Flood	1.00	1.00	1.00	1500
DDoS-UDP_Fragmentation	0.99	0.99	0.99	1500
Accuracy / Avg	0.97	0.97	0.97	17999

with corresponding F1-scores of 0.82 and 0.83. These two attack categories exhibit highly similar traffic characteristics, making them more difficult to distinguish. Nevertheless, the overall average F1-score of 0.97 confirms the resilience of the suggested multi-class DDoS detection framework.

Table 11 reports the class-wise results obtained on the CICIOT2023 dataset. Similar observations can be made, where most attack categories achieve precision and recall values higher than 0.99. Benign traffic is perfectly recognized, which is particularly important to reduce the number of false alerts in actual intrusion detection systems. As in the CIC-DIAD2024 dataset, DDoS-SynonymousIP_Flood and DDoS-SYN_Flood remain the most challenging classes because of their similar sequential traffic behavior. However, the temporal features learned by the LSTM significantly improve their recognition compared with a standalone LightGBM classifier, leading to a 0.96 total F1-score.

The classification report for the CICIDS2017 dataset is presented in Table 12. The proposed framework achieves excellent detection performance across different attack categories. The BENIGN, DDoS, FTP-Patator, and DoS Slowloris classes obtain recall and precision values near 1.00, suggesting that the hybrid model effectively captures their traffic characteristics. A relatively lower recall is observed for the Web Attack-Brute Force class. This receives a 0.84 F1-score. This behavior is expected because web-based attacks often generate traffic patterns that partially resemble legitimate HTTP requests, making their discrimination more challenging. Nevertheless, the overall accuracy of approximately 99% demonstrates the strong generalization capability of the proposed framework on heterogeneous network traffic.

Overall, the per-class evaluation across the three benchmark datasets demonstrates that the proposed LSTM–LightGBM framework consistently achieves high precision, recall, and F1-score for the majority of traffic classes. The remaining classification errors are mainly concentrated among attack categories

Table 11. Classification Results per Traffic Type (CICIoT2023)

Traffic Type	Precision	Recall	F1-score	Samples
BenignTraffic3	1.00	1.00	1.00	1500
DDoS-ACK_Fragmentation	0.99	0.99	0.99	1499
DDoS-HTTP_Flood-	0.99	0.98	0.98	1500
DDoS-ICMP_Flood	1.00	1.00	1.00	1500
DDoS-ICMP_Fragmentation	1.00	0.99	0.99	1500
DDoS-PSHACK_Flood	1.00	1.00	1.00	1500
DDoS-RSTFINFlood	1.00	1.00	1.00	1500
DDoS-SYN_Flood	0.85	0.79	0.82	1500
DDoS-SlowLoris	0.96	0.99	0.97	1500
DDoS-SynonymousIP_Flood	0.80	0.86	0.83	1500
DDoS-TCP_Flood	1.00	1.00	1.00	1500
DDoS-UDP_Fragmentation	1.00	0.99	0.99	1500
Accuracy / Avg	0.96	0.96	0.96	17999

Table 12. Classification report of the proposed hybrid LSTM–LightGBM model on the CICIDS2017 dataset

Class	Precision	Recall	F1-score	Support
BENIGN	1.00	0.98	0.99	73,303
DDoS	1.00	1.00	1.00	4,805
DoS Slowloris	1.00	0.99	0.99	527
FTP-Patator	1.00	1.00	1.00	1,027
PortScan	1.00	0.98	0.99	48
Web Attack–Brute Force	0.99	0.73	0.84	227
Accuracy	0.99	0.99	0.99	79,937

exhibiting highly similar temporal behaviors, particularly SYN Flood and SynonymousIP Flood. These findings confirm that the integration of LSTM with LightGBM effectively enhances the recognition of sequential attack patterns while maintaining excellent benign traffic detection, making the proposed framework extremely appropriate for real-time, useful IoT intrusion detection.

5.4 Confusion Matrix Analysis

To better illustrate the impact of temporal feature extraction, Figures 4 and 5 present the normalized confusion matrices obtained using the baseline LightGBM classifier and the proposed hybrid LSTM–LightGBM model, respectively.

Analysis of the LightGBM Baseline Figure 4 illustrates the confusion matrices obtained using LightGBM without temporal modeling. For the CICIoT2023 dataset (Figure 4(b)), most traffic categories are correctly identified.

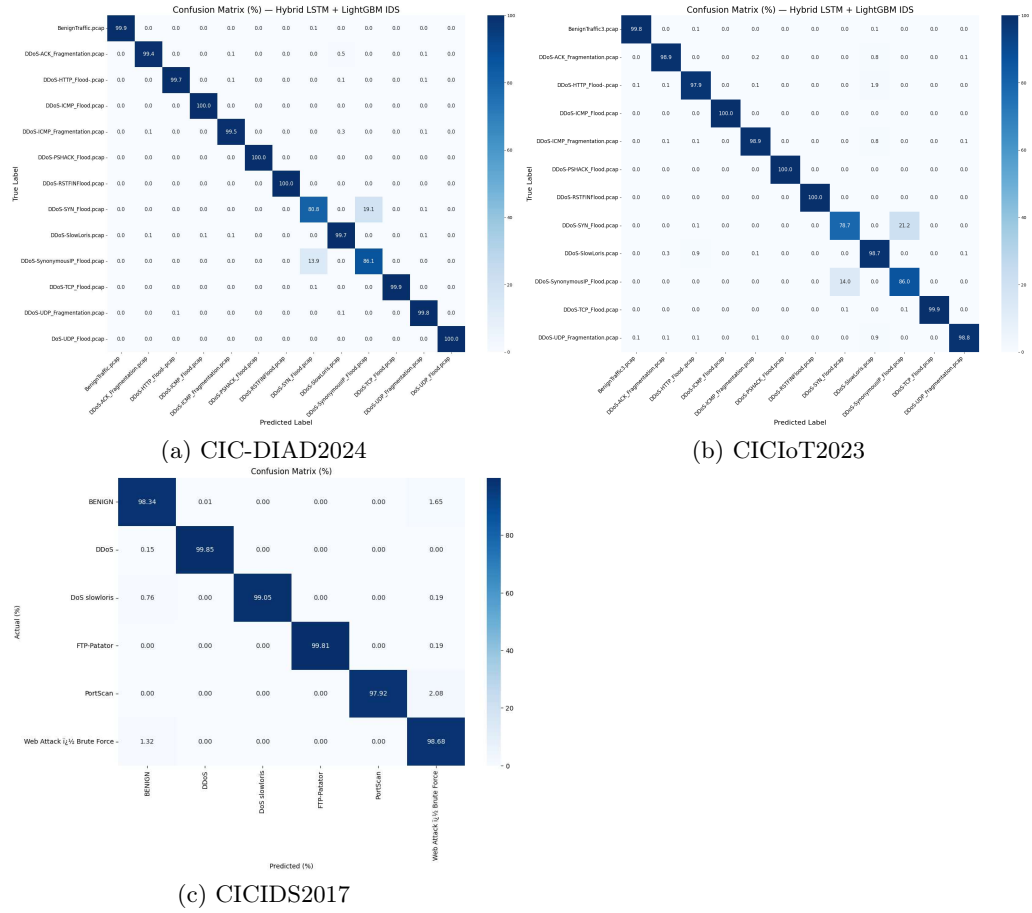


Fig. 5. Normalized confusion matrices of representative baseline models on CIC-DIAD2024 and CIC-IoT2023 with LightGBM and LSTM

However, noticeable confusion exists between *DDoS-SYN_Flood* and *DDoS-SynonymousIP_Flood*, where approximately 19% of SYN Flood samples are incorrectly classified as SynonymousIP Flood. This indicates that the baseline classifier struggles to distinguish attacks exhibiting highly similar statistical characteristics. Similarly, for the CIC-DIAD2024 dataset (Figure 4(a)), although several attack categories such as ICMP Flood, TCP Flood, PSHACK Flood, and RSTFIN Flood are classified almost perfectly, the classifier still exhibits confusion between sequential flooding attacks, particularly SYN Flood and SynonymousIP Flood. These errors reduce the overall recall and F1-score of the baseline model. Overall, the confusion matrices demonstrate that LightGBM effectively learns discriminative tabular features but remains limited when distinguishing attack classes sharing similar temporal behaviors.

Analysis of the Proposed Hybrid LSTM-LightGBM Model Figure 5 presents the confusion matrices obtained using the proposed hybrid LSTM-LightGBM framework. Compared with Figure 4, the incorporation of the LSTM module considerably reduces the confusion between similar attack categories. The temporal information extracted by LSTM enables the classifier to better distinguish attacks exhibiting comparable statistical distributions but different sequential behaviors.

On the CICIOT2023 dataset (Figure 5(b)), the recall of DDoS-SYN_Flood increases substantially, while the confusion with DDoS-SynonymousIP_Flood decreases. Likewise, on the CIC-DIAD2024 dataset (Figure 5(a)), the proposed model achieves nearly perfect recognition for most attack categories with only a few remaining misclassifications.

Regarding the CICIDS2017 dataset (Figure 5(c)), the confusion matrix confirms the robustness of the proposed framework. Benign traffic, DDoS, FTP-Patator, and DoS Slowloris are classified almost perfectly. A small amount of confusion remains between Web Attack-Brute Force and Benign traffic, which is expected because these attacks generate traffic patterns that partially resemble legitimate user activities. Nevertheless, the overall confusion remains very limited, confirming the strong discriminative capability of the proposed hybrid framework.

- Benign Traffic: Remains perfectly detected in both models.
- Sequential Attack Reduction: Misclassification between DDoS-SynonymousIP_Flood and DDoS-SYN_Flood drops with LSTM, proving the benefit of temporal modeling.
- Other DDoS Attacks: Most other DDoS types (ICMP, TCP, PSHACK) are accurately classified in both models; the LSTM provides a slight but important increase in recall and precision.
- Practical Implication: Temporal features extracted by LSTM improve robustness of multi-class detection and reduce false negatives, making the system more reliable for IoT networks.

Summary: Across both datasets:

- LSTM + LightGBM consistently reduces misclassifications among sequential attacks.
- Benign traffic detection remains nearly perfect.
- Overall multi-class detection is significantly improved compared to LightGBM-only.
- Confusion matrices visually confirm the advantage of incorporating temporal features for DDoS detection in IoT environments.

5.5 ROC-AUC Analysis

The suggested LSTM-LightGBM framework’s classification performance under various decision thresholds is thoroughly assessed using the Receiver Operating Characteristic (ROC) curves and the accompanying Area Under the Curve

(AUC) values. The ROC curves for the CICIOT2023, CIC-DIAD2024, and CICIDS2017 datasets are shown in Figures 6, 7, and 8.

Almost all traffic classes’ ROC curves for the CICIOT2023 dataset (Figure 6) are concentrated close to the upper-left corner of the graph, demonstrating exceptional discrimination abilities. The Benign Traffic class achieves an AUC value very close to 1.00, reflecting an extremely low false positive rate. Likewise, ROC curves for attack classes like DDoS-ICMP_Flood, DDoS-TCP_Flood, DDoS-PSHACK_Flood, and DDoS-RSTFINFlood are almost perfect. While DDoS-SYN_Flood and DDoS-SynonymousIP_Flood remain the most challenging classes because of their similar traffic characteristics, the proposed LSTM-LightGBM framework significantly improves their separability compared with the standalone LightGBM classifier by exploiting temporal dependencies between consecutive network packets.

Figure 7 presents the ROC curves obtained on the CIC-DIAD2024 dataset. Similar trends can be observed, where the majority of traffic classes achieve AUC values close to 1.00. ICMP, Benign Traffic Excellent discrimination capability has been obtained for Flood, TCP Flood, UDP Fragmentation, PSHACK Flood and RSTFIN Flood. The LSTM’s learned temporal features greatly reduce overlaps between sequential attack types, particularly for DDoS-SYN-Flood, DDoS-SlowLoris, and DDoS-SynonymousI-Flood, which results in higher true positive rates while maintaining very low false positive rates.

Figure 8 shows the ROC curves of the CICIDS2017 dataset. The proposed framework exhibits excellent generalisation ability, where most attack categories achieve AUC values close to 1.00. The classes of BENIGN, DDoS, FTP-Patator, DoS Slowloris and PortScan are well separated from malicious traffic, supporting the power of the hybrid architecture. The ROC performance for the Web Attack-Brute Force class is slightly lower because the malicious HTTP requests are similar to legitimate web traffic. Nevertheless, the achieved AUC is still high which indicates a good classification performance even in difficult attack scenarios.

Overall, the ROC analysis confirms that the proposed hybrid LSTM-LightGBM framework consistently exhibits superb discrimination performance over the three benchmark datasets. AUC values close to 1.00 for most traffic classes, suggest that adding temporal feature extraction to the LightGBM classifier improves significantly the detection of complex DDoS attacks, while maintaining a very low false positive rate.

5.6 Ablation Study

The ablation study is performed to evaluate the contribution of the LSTM module for the proposed hybrid framework. The competitive results in Table 9 are analysed from an ablation perspective by comparing the standalone LightGBM classifier and the proposed LSTM-LightGBM model. The findings unequivocally show that adding the LSTM module constantly raises the baseline performance LightGBM classifier across all three benchmark datasets. While LightGBM efficiently exploits statistical traffic features, it cannot explicitly model the tempo-

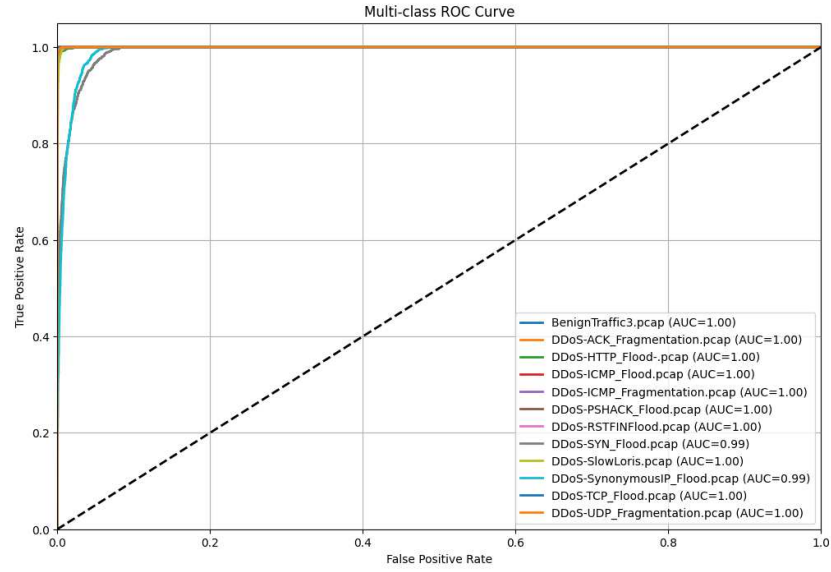


Fig. 6. ROC curves for each class on CICIoT2023 using LSTM + LightGBM

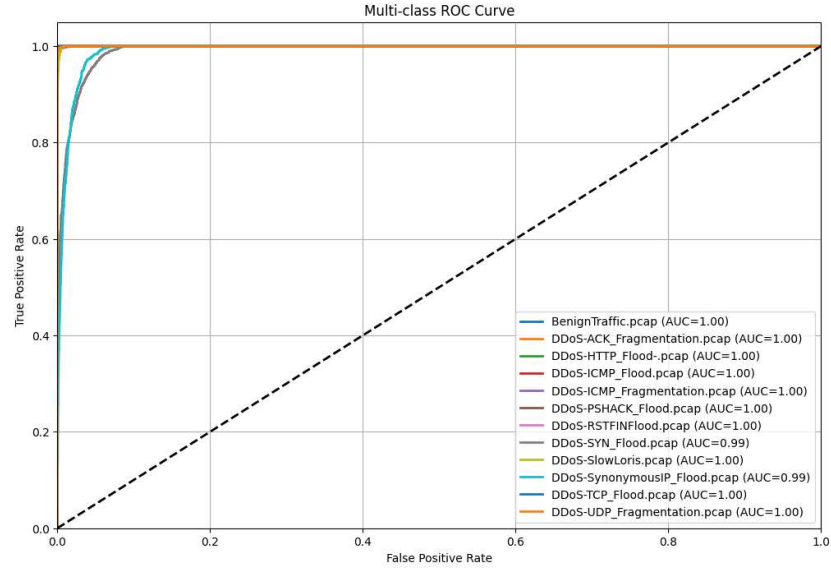


Fig. 7. ROC curves for each class on DIAD2024 using LSTM + LightGBM

ral dependencies that characterize sequential DDoS attacks. The addition of the LSTM encoder addresses this limitation by learning temporal relationships be-

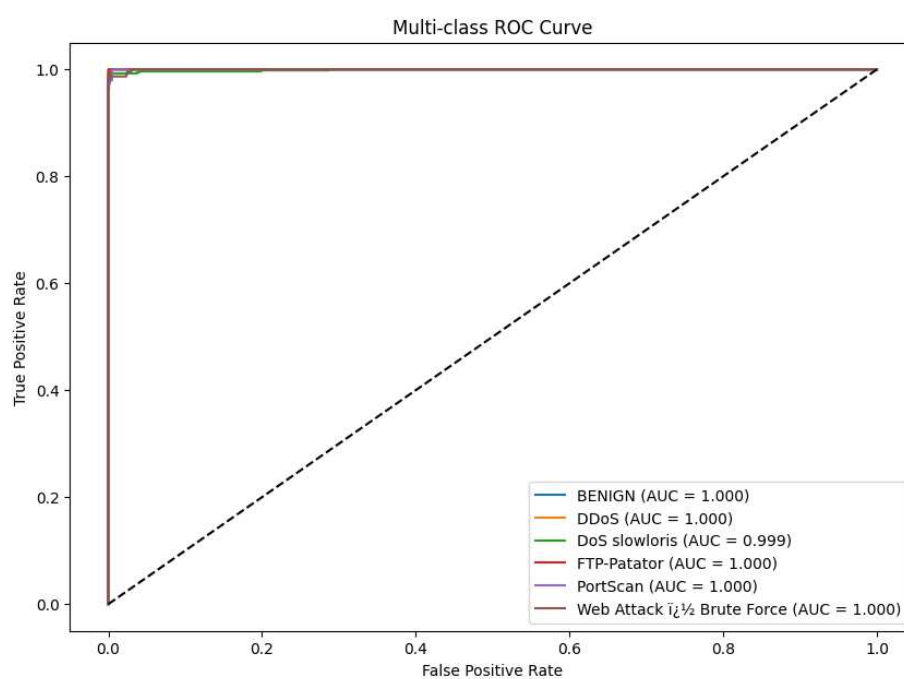


Fig. 8. ROC curves for each class on CICIDS2017 using LSTM + LightGBM

tween consecutive network flows, thereby providing more discriminative feature representations.

The most significant performance improvement is observed on the CIC-DIAD2024 dataset, where the classification accuracy increases from 94.37% to 97.80%. A similar improvement is obtained on the CICIOT2023 dataset, where the accuracy rises from 94.40% to 96.80%, together with a substantial increase in recall. These improvements indicate that temporal feature learning effectively reduces the confusion between attack classes sharing similar statistical characteristics, particularly DDoS-SYN_Flood and DDoS-SynonymousIP_Flood.

Although the standalone LightGBM classifier already achieves excellent performance on the CICIDS2017 dataset, incorporating the LSTM module further improves the overall accuracy from 98.56% to 99.89%. This result demonstrates that temporal sequence modeling provides complementary information even when the statistical features are already highly discriminative.

Overall, the ablation study confirms that the LSTM module is an essential component of the proposed framework. By capturing temporal dependencies in network traffic, it enhances the discriminative capability of the LightGBM classifier, reduces false classifications among similar attack categories, and improves the robustness and generalization ability of the proposed intrusion detection system.

5.7 SHAP Explainability Analysis

Although the proposed hybrid LSTM-LightGBM framework achieves excellent classification performance, understanding the factors that influence its predictions is equally important for practical systems for detecting intrusions. SHapley Additive exPlanations (SHAP) are used to measure each feature’s contribution to the final LightGBM classification decisions in order to enhance the interpretability of the suggested model. Figures 9, 10, and 11 illustrate the global SHAP feature importance obtained for the CICIDS2017, CICIOT2023, and CIC-DIAD2024 datasets, respectively.

For the CICIDS2017 dataset (Figure 9), the SHAP analysis demonstrates that the categorisation process is dominated by a comparatively limited subset of features. In particular, flow-based attributes such as *Destination Port*, *Avg Bwd Segment Size*, and *Packet Length statistics* exhibit the highest SHAP values, indicating their strong discriminative power. Many other features do not contribute much. This means that some features are not really needed and the model is good at looking at the important parts of the network.

Figure 10 shows the results of the SHAP analysis for the CICIOT2023 dataset. The CICIOT2023 dataset importance is mainly due, to the latent features that the LSTM module generates. The LSTM module is what makes these features important (e.g., *LSTM_feature_**). This indicates that temporal patterns learned from sequential traffic data play a crucial role in detecting DDoS attacks. Some of the learned representations have much higher SHAP values, which means they are dominant features, while the rest of the features provide supplementary information. This suggests that the LSTM is able to learn meaningful

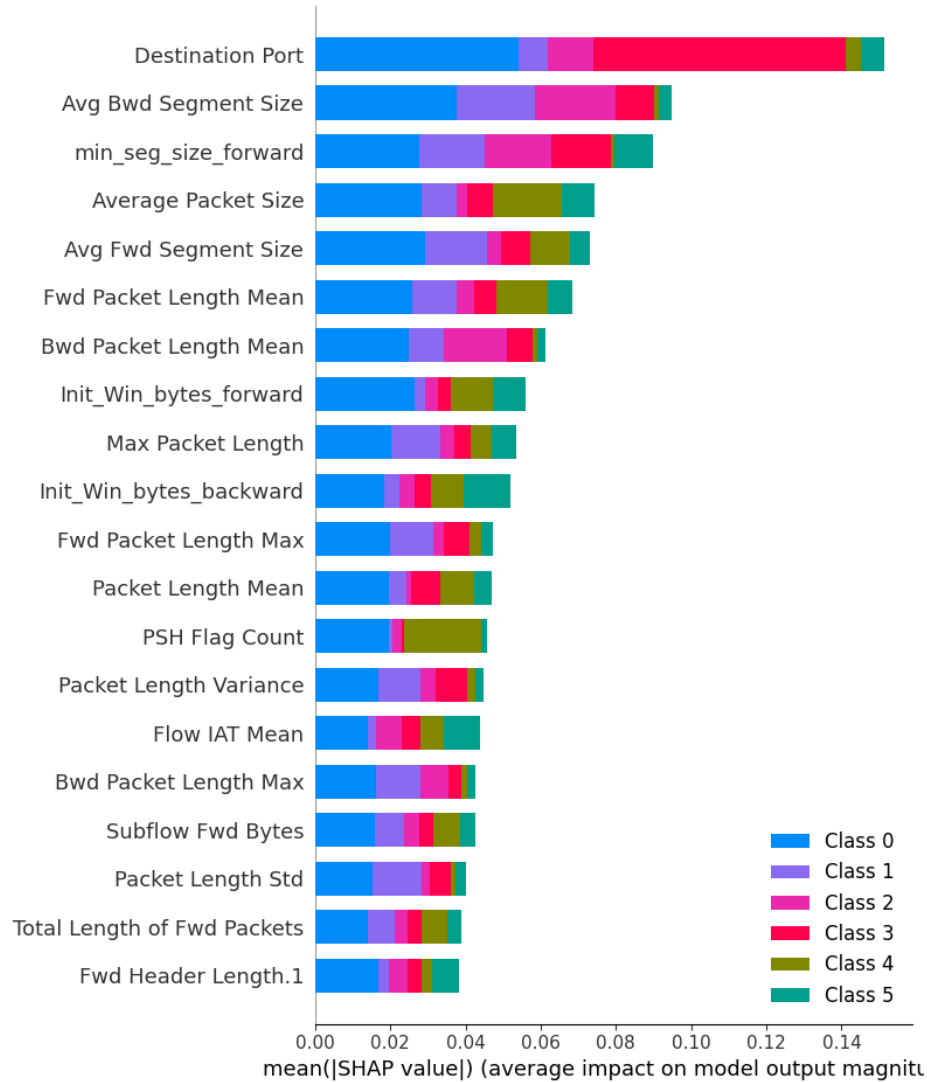


Fig. 9. SHAP summary plot highlighting the contribution of LSTM-derived features to multi-class DDoS attack detection on the CIC-IDS2017 dataset

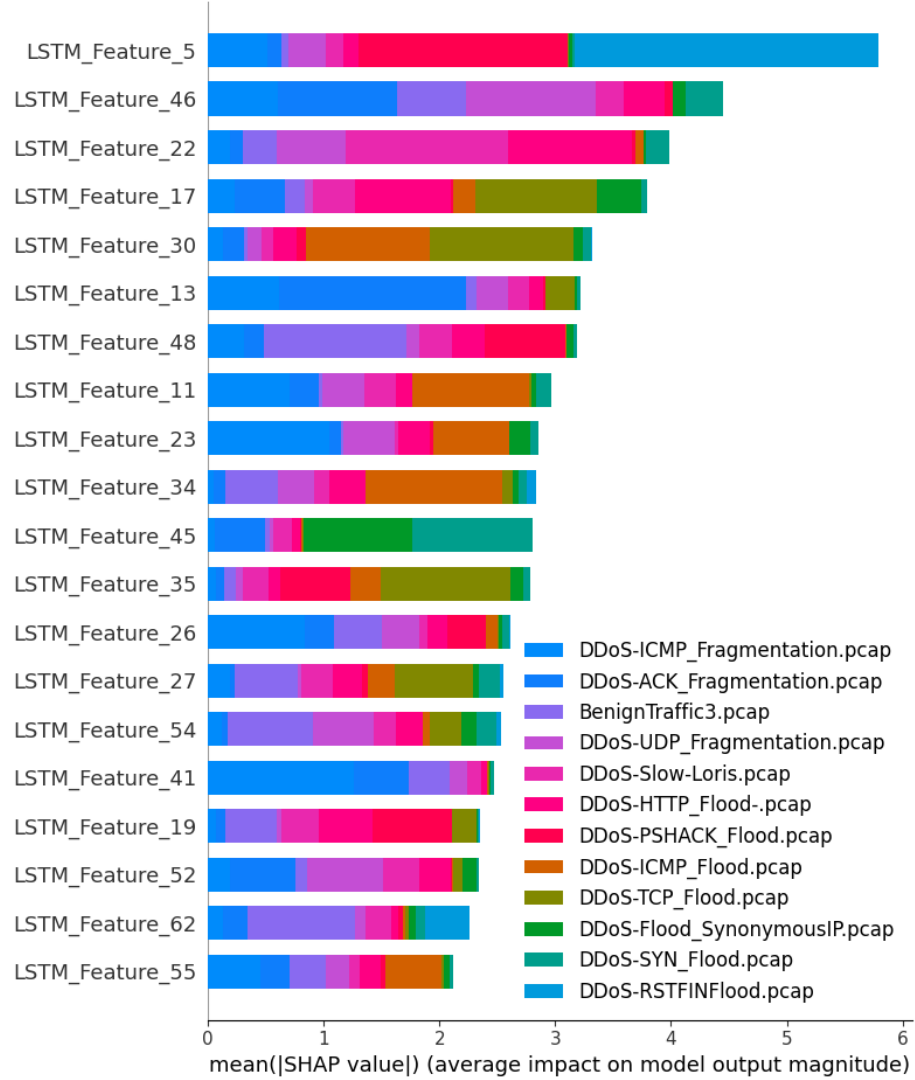


Fig. 10. SHAP summary plot highlighting the contribution of LSTM-derived features to multi-class DDoS attack detection on the CIC-IoT2023 dataset

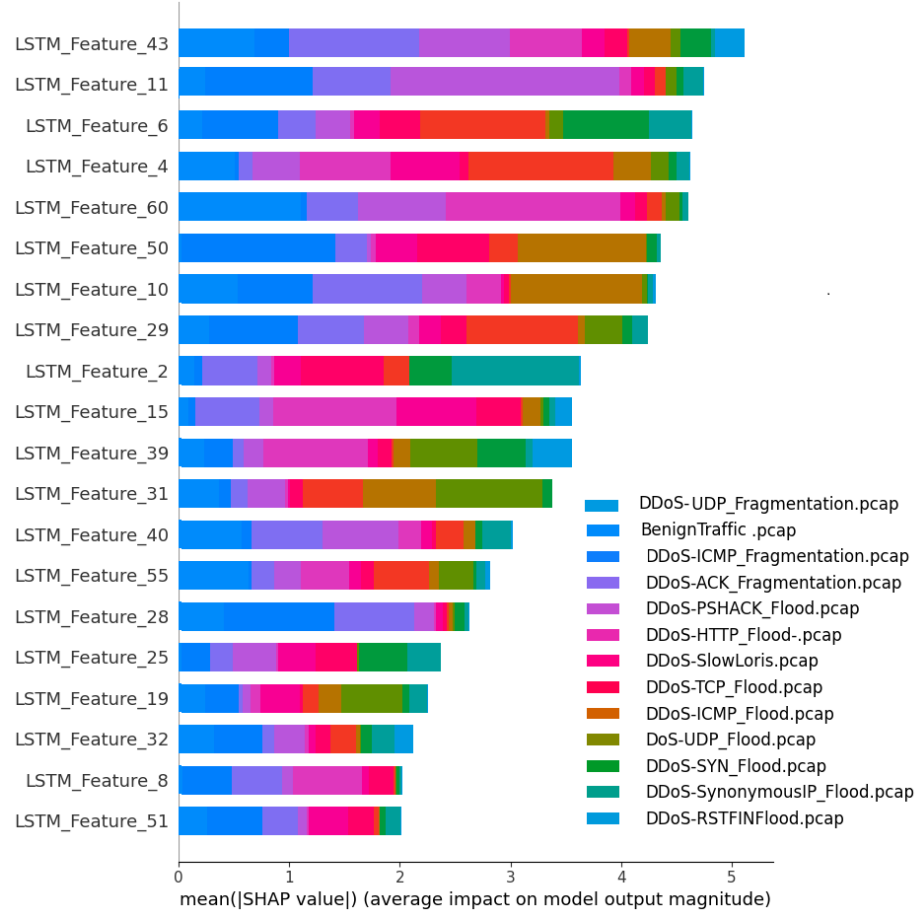


Fig. 11. SHAP summary plot highlighting the contribution of LSTM-derived features to multi-class DDoS attack detection on the CIC-DIAD2024 dataset

Table 13. Comparison of Proposed Method with State-of-the-Art

Study	Dataset	Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
DL-DDoS-IoT (2019) [30]	CICIoT2023	LSTM	95.8	95.5	95.8	95.5
Arya et al. (2026) [31]	Bot-IoT	PCA-LightGBM	99.9	99.9	99.9	99.87
Islam et al. (2020) [32]	UNSW-NB15	LightGBM	96.17	96.54	96.17	97.20
Abid et al. (2025) [33]	CICIoT2023	CNN+LightGBM	95.2	95.2	–	95.1
Dudi et al. (2025) [20]	CICIDS2017	LightGBM + SHAP	91.2	–	–	89.4
Mgungile et al. (2025) [34]	CICIoT-DIAD2024	CNN+LSTM	88.3	86.0	90.0	–
Proposed Method	CICIoT-DIAD2024	LSTM + LightGBM	97.8	97.6	97.7	97.6
Proposed Method	CICIoT2023	LSTM + LightGBM	96.8	97.6	97.7	97.6
Proposed Method	CICIDS2017	LSTM + LightGBM	99.89	99.89	99.89	99.89

temporal dependencies that can improve the performance of the LightGBM classifier.

Similarly, in the case of the CIC-DIAD2024 dataset (Figure 11), the SHAP results follow a similar trend, highlighting that only a fraction of the LSTM-generated features play a significant role in the classification. The distribution of SHAP values demonstrates that different features are activated for different attack categories, indicating the model can capture diverse traffic behaviours. The presence of positive and negative contributions across classes also indicates the model’s ability to distinguish among multiple attack types.

In general, SHAP analysis of the three datasets reveals that: (i) The proposed framework relies on a compact set of high-impact features consistently, (ii) LSTM-based representations play a central role in complex IoT scenarios, and (iii) The learned feature importance patterns are stable across heterogeneous datasets. The experimental results demonstrate that the LSTM-LightGBM model has high detection accuracy and transparent and interpretable decisions, improving its reliability for real-world IoT intrusion detection applications.

5.8 Comparison with State-of-the-Art

The suggested hybrid LSTM-LightGBM framework is contrasted with a number of contemporary machine learning and deep learning techniques for DDoS intrusion detection in Table 13. Although the compared methods are evaluated on different benchmark datasets, the comparison provides a general indication of the suggested framework’s competitiveness and efficacy.

On the CIC-DIAD2024 dataset, the suggested model obtains an accuracy of 97.80%, outperforming the recent CNN-LSTM model of Mgungile *et al.* by a considerable margin while also providing higher F1-score, recall, and precision. This enhancement shows the value of fusing LightGBM’s potent classification power with temporal feature extraction. The suggested framework outperforms the CNN-LightGBM framework introduced by Abid et al. and the LSTM-based model proposed by Ge et al. on the CICIoT2023 dataset, achieving an accuracy

of 96.80% and an F1-score of 97.60%. These results indicate that the extracted temporal representations enable the proposed model to better capture complex DDoS traffic patterns and reduce the confusion between similar attack categories.

For the CICIDS2017 dataset, the proposed system achieves an overall accuracy of 99.89%, demonstrating excellent generalization capability on a widely used intrusion detection benchmark. Although some existing methods report competitive findings on other datasets such as Bot-IoT and UNSW-NB15, direct numerical comparisons should be interpreted with caution because the datasets differ in terms of traffic characteristics, attack types, feature distributions, and evaluation protocols.

Besides outstanding detection performance, the proposed framework also achieves very low inference latency, which is only 0.077 ms, 0.069 ms and 0.0000004 ms per prediction on CIC-DIAD2024, CICIOT2023 and CICIDS2017 datasets respectively. The computational efficiency of the proposed framework makes it fit for real time intrusion detection in resource constrained IoT environments.

In general, the comparative analysis indicates that the combination of LSTM-based temporal feature extraction and LightGBM provides a good balance between detection accuracy, robustness, interpretability, and computational efficiency, making the proposed framework a competitive solution for multi-class DDoS detection in different IoT network environments.

5.9 Discussion

In addition to its excellent detection performance, the proposed framework achieves very low inference latency, which is only 0.077 ms, 0.069 ms, and 0.0000004 ms per prediction on the CIC-DIAD2024, CICIOT2023, and CICIDS2017 datasets, respectively. The computational efficiency of the proposed framework makes it appropriate for real time intrusion detection in resource-constrained IoT contexts.

In general, the comparative analysis indicates that the combination of LSTM-based temporal feature extraction and LightGBM provides a good balance between detection accuracy, robustness, interpretability, and computational efficiency, making the proposed framework a competitive solution for multi-class DDoS detection in various IoT network environments.

6 Conclusion

The paper presented a hybrid intrusion detection framework based on the combination of LSTM networks and the LightGBM classifier for accurate and efficient multi-class DDoS attack detection in IoT environments. The proposed framework utilises LSTM's ability to model temporal data to learn sequential traffic representations. LightGBM performs efficient and accurate classification based on the extracted features.

Experiments on the benchmark datasets, CICIOT2023, CIC-DIAD2024, and CICIDS2017, demonstrate the superiority of the proposed approach compared

to the standalone LightGBM classifier. The hybrid framework is superior in accuracy, precision, recall, and F1-score on all datasets. Moreover, the confusion matrix and ROC-AUC and per-class analysis confirms its strong ability to distinguish challenging DDoS attack categories with low false positive rates. The ablation study confirms the importance of temporal feature extraction, and the SHAP-based explainability analysis provides transparent and interpretable insights into the decision-making process of the model.

The proposed framework offers not only excellent detection performance but also very low inference latency, allowing it to be used in real-time applications in real cybersecurity infrastructures. The combination of high detection accuracy, computational efficiency and explainability makes the proposed model a promising solution for the protection of modern IoT ecosystems such as smart cities, industrial IoT, healthcare IoT and next generation 5G/6G communication networks. Moreover, the framework can be deployed on IoT gateways, edge computing platforms, SDN controllers, or cloud-based intrusion detection systems to offer scalable and intelligent network protection.

Future work will involve improving the generalisation across datasets, testing the framework on real-world operational traffic, extending the model to detect a wider range of cyberattacks beyond DDoS, and exploring more advanced sequence-learning architectures such as Transformers, Mamba-based models, and Graph Neural Networks. Moreover, adaptive online learning, concept drift mitigation, encrypted traffic analysis and zero-day attack detection will be investigated to improve the robustness and long-term applicability of the proposed intrusion detection framework.

7 Declarations

7.1 Funding

This research received no external funding.

7.2 Ethics Declaration

Ethics declaration: not applicable.

7.3 Competing Interests

The authors declare that they have no competing interests.

7.4 Data Availability

The datasets used in this study are publicly available benchmark datasets and were obtained from their respective public sources. No new datasets were generated during the current study.

References

1. R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, “A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.
2. S. Karnani, N. Agrawal, and R. Kumar, “A comprehensive survey on low-rate and high-rate ddos defense approaches in sdn: taxonomy, research challenges, and opportunities,” *Multimedia Tools and applications*, vol. 83, no. 12, p. 35253–35306, 2024.
3. S. Malliga, P. Nandhini, and S. V. Kogilavani, “A comprehensive review of deep learning techniques for the detection of (distributed) denial of service attacks,” *Information Technology and Control*, vol. 51, no. 1, pp. 180–215, 2022.
4. M. Shafiq, Z. Tian, and Y. Sun, “Detection of ddos attacks in iot environments using machine learning,” *IEEE Access*, vol. 8, p. 82164–82175, 2020.
5. M. Tavallae, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the kdd cup 99 data set,” in *2009 IEEE symposium on computational intelligence for security and defense applications*. Ieee, 2009, pp. 1–6.
6. A. Graves, “Long short-term memory,” *Supervised sequence labelling with recurrent neural networks*, pp. 37–45, 2012.
7. D. Hamouda, M. A. Ferrag, N. Benhamida, H. Seridi, and M. C. Ghanem, “Revolutionizing intrusion detection in industrial iot with distributed learning and deep generative techniques,” *Internet of Things*, vol. 26, p. 101149, 2024.
8. J. Zhao, Y. Liu, Q. Zhang, and X. Zheng, “Cnn-attbilstm mechanism: A ddos attack detection method based on attention mechanism and cnn-bilstm,” *IEEE Access*, vol. 11, p. 136308–136317, 2023.
9. G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, “Lightgbm: A highly efficient gradient boosting decision tree,” *Advances in neural information processing systems*, vol. 30, 2017.
10. P. Shukla, C. R. Krishna, and N. V. Patil, “Eiot-ddos: embedded classification approach for iot traffic-based ddos attacks,” *Cluster Computing*, vol. 27, no. 2, pp. 1471–1490, 2024.
11. A. Kumar, B. Sharma, and A. Noonian, “Secure blockchain based intrusion detection for iot networks,” *Discover Computing*, vol. 28, no. 1, p. 226, 2025.
12. A. Gaurav, B. B. Gupta, and K. T. Chui, “Optimized cyber attack detection in iot networks using feature selection and lightgbm,” in *2024 27th International Symposium on Wireless Personal Multimedia Communications (WPMC)*. IEEE, 2024, pp. 1–5.
13. N. Alyassiri, M. M. S. Altufaili, and F. A. Nama, “Hybrid cnn–lstm framework for ddos detection in 5g-enabled iot environments,” *Wasit Journal for Pure sciences*, vol. 5, no. 1, pp. 38–52, 2026.
14. A. F. Al-zubidi, A. K. Farhan, and S. M. Towfek, “Predicting dos and ddos attacks in network security scenarios using a hybrid deep learning model,” *Journal of Intelligent Systems*, vol. 33, no. 1, p. 20230195, 2024.
15. L. Liu, W. Yu, Z. Wu, and S. Peng, “Xgboost-based detection of ddos attacks in named data networking,” *Future Internet*, vol. 17, no. 5, p. 206, 2025.
16. K. Sadaf and J. Sultana, “Intrusion detection based on autoencoder and isolation forest in fog computing,” *IEEE Access*, vol. 8, p. 167059–167068, 2020.
17. N. Thalji, A. Raza, M. S. Islam, N. A. Samee, and M. M. Jamjoom, “Ae-net: Novel autoencoder-based deep features for sql injection attack detection,” *IEEE access*, vol. 11, p. 135507–135516, 2023.

18. P. Jain, A. Rathour, A. Sharma, and G. S. Chhabra, "Bridging explainability and security: an xai-enhanced hybrid deep learning framework for iot device identification and attack detection," *IEEE Access*, vol. 13, p. 127368–127390, 2025.
19. T. L. Yasarathna, M. Liyanage, and N.-A. Le-Khac, "Deep learning based autonomous anomaly detection for security in sdn-iot networks," *IEEE Open Journal of the Communications Society*, 2025.
20. 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)*. IEEE, 2025, pp. 329–334.
21. H. N. Muthuswamy, M. S. Suthagar, and V. Natarajan, "Hybrid transformer and xgboost model for federated iot intrusion detection," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*. IEEE, 2026, pp. 1–6.
22. P. S. Lal and A. Ashok, "Deep learning-based network intrusion detection systems: A comprehensive survey of methods, evolution, and research perspectives," in *2026 7th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*. IEEE, 2026, pp. 379–385.
23. Q. Gulzar and K. Mustafa, "Enhancing network security in industrial iot environments: a deepcplg hybrid learning model for cyberattack detection," *International Journal of Machine Learning and Cybernetics*, vol. 16, no. 7, pp. 4797–4815, 2025.
24. J. Vidhubala and R. Kayalvizhi, "Lightgbm-based multi-class botnet detection framework for iot networks," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*. IEEE, 2026, pp. 1–6.
25. A. Djama, M. Maazouz, H. Kheddar, A. Gueriani, and A. Toubal, "Hybrid deep neural networks and long short-term memory for distributed denial of service attacks classification," in *2025 International Conference on Intelligent Computer Systems, Data Science and Applications (IC2SDA)*. IEEE, 2025, pp. 1–6.
26. E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023.
27. M. Rabbani, J. Gui, F. Nejati, Z. Zhou, A. Kaniyamattam, M. Mirani, G. Piya, I. Opushnyev, R. Lu, and A. A. Ghorbani, "Device identification and anomaly detection in iot environments," *IEEE Internet of Things Journal*, vol. 12, no. 10, p. 13625–13643, 2024.
28. S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
29. A. Djama, M. Maazouz, H. Kheddar, M. Rahim, and B. Bengherbia, "High performance detection of ddos attacks with hybrid cnn-lstm architecture," in *2025 International Conference on Intelligent Computer Systems, Data Science and Applications (IC2SDA)*. IEEE, 2025, pp. 1–6.
30. M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for iot networks," in *2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC)*. IEEE, 2019, p. 256–260.
31. H. Arya, N. Kandhoul, S. K. Dhurandher, and I. Woungang, "Adaptive sliding window and lightgbm-based ddos attack detection framework for iot networks," *Peer-to-Peer Networking and Applications*, vol. 19, no. 1, p. 16, 2026.
32. M. K. Islam, P. Hridi, M. S. Hossain, and H. S. Narman, "Network anomaly detection using lightgbm: A gradient boosting classifier," in *2020 30th international telecommunication networks and applications conference (ITNAC)*. IEEE, 2020, pp. 1–7.

33. T. Abid, A. Ahmin, F. Maazouzi, D. Chefrou, I. Ullah, M. Ahmin, and R. Al-mukhlifi, “A novel iot threat detection using gwo feature selection and cnn-enhanced lightgbm,” *Journal of Cloud Computing*, vol. 14, no. 1, p. 72, 2025.
34. J. Mgungile and Ö. Tonkal, “Scalable intrusion detection in iot networks: A big data analytics approach,” *Turkish Journal of Engineering*, vol. 10, no. 1, pp. 230–243, 2025.