A High-Performance Deep Learning Model for DDoS Attack Detection

Haythem Hayouni, and Wala Ben Rhouma

Original scientific article

***Abstract*—DDoS attacks continue to pose a severe problem in today's computer security due to their ability to significantly impact the network's functionality and deplete computing and communication resources. This paper proposes a deep learning-based approach for reliable DDoS attack detection and classification into distinct classes. The suggested framework goes beyond the state-of-the-art binary classification approach by incorporating the multi-class classification at various levels that help to distinguish particular DDoS attack categories. Three different deep learning models are examined. In the first model, the Multi-Layer Perceptron (MLP) is utilized to extract informative patterns from the flow-based network features. In the second model, the combination of one-dimensional convolutional layers with the Deep Neural Network (CNN1D-DNN) is employed to analyze local patterns and perform traffic classification. Finally, in the third model, the RNN-LSTM architecture is used to analyze the temporal dependencies of the traffic data. Experiments are performed on the CIC-DDoS-2019 dataset, which includes benign traffic and several types of DDoS attacks. The feature selection and balancing techniques are applied in order to minimize the impact of the redundant information and class imbalance problem. Evaluation results under the binary, 7-class, and 13-class detection scenarios show the high detection accuracy that exceeds 99% in all of the tested configurations with the low number of false positives. Comparison with the recently developed DDoS detection techniques confirms the efficiency of the proposed approach for the precise network attack classification.**

***Index Terms*—Distributed Denial of Service (DDoS), Intrusion Detection System (IDS), Deep Learning, Multi-Class Classification, CIC-DDoS-2019 Dataset.**

I. Introduction

Distributed Denial of Service (DDoS) attacks [1] continue to be one of the greatest threats to the availability, reliability, and stability of contemporary networked infrastructures. In contrast to common intrusion attempts that primarily target access to systems or theft of information, DDoS attacks aim at flooding the attacked system or network with excess traffic and, thus, causing denial of service to the intended legitimate users. With the advent of Internet of Things ecosystems and the development of sophisticated strategies of attacking, DDoS attacks became larger in volume, more complicated, and more difficult to detect, thus making intrusion detection systems useless for protection against them.

Recent developments in the field of machine learning and deep learning [2], [3] have offered new opportunities to develop advanced IDS for detecting intricate patterns in the traffic of large amounts of networks. However, many existing techniques still work only on a binary classification and are able to distinguish only between normal and malicious traffic without classifying the specific types of attacks. Classification of different types of DDoS attacks [4] is crucial for the development of fast responding strategies and further forensic investigation of the attacks.

In order to tackle the above mentioned limitations, the following work proposes an advanced framework of multi-class DDoS attack detection based on deep learning algorithms. The research will focus on the analysis of three structured models, namely, a Multi-Layer Perceptron (MLP), a hybrid CNN1D-DNN approach, and an RNN-LSTM model. In this regard, all three aforementioned methods are examined via applying them to the CIC-DDoS-2019 dataset that consists of realistic and diverse traffic patterns involving twelve kinds of DDoS attacks and normal network connections. Thus, it can be considered as a modern and reliable benchmark for assessing the efficacy of various deep learning methods in detecting DDoS attacks.

The main contributions of the research can be highlighted as follows:

- We introduce the design and reasoning behind three deep learning models for DDoS detection and analyze their comparative performance under different classification types, namely, binary, 7-class, and 13-class.
- We apply advanced methods of pre-processing and feature selection, such as SMOTE balancing to deal with class imbalance problem.
- We prove that the suggested MLP model, backed up by per-class precision metrics and AUC-ROC plots is more accurate than the models from recent related literature.
- We compare the method with the state-of-the-art approaches and show its high efficiency and applicability in practice.

The remainder of this paper is organized as follows. Section II provides a review of the related work and a discussion on the existing methodologies concerning this study. Section III gives the description of the dataset, presents the process of feature engineering, and describes the proposed architectures of models. Section IV provides the experimental setup, analysis of the achieved results, and their comparison with the

Manuscript received April 15, 2025; revised July 2, 2025. Date of publication August 26, 2026. Date of current version August 26, 2026. The associate editor prof. Miljenko Mikuc has been coordinating the review of this manuscript and approved it for publication.

Authors are with the IT Department, Higher Institute of Computer Science of Kef, University of Jendouba, Tunisia (e-mails: haythem.hayouni@isikef.u-jendouba.tn, wala.ben-rhouma@gmail.com).

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0054

1845-6421/12/2025-0054 © 2026 CCIS

existing methods. Finally, Section V concludes the paper by summing up the main achievements and providing ideas for future work.

II. Related Works

Detection of DoS and DDoS attacks is one of the major issues for further study because modern networks are becoming more complex. However, along with that, attackers also develop more complicated methods, which make it harder to detect whether some traffic is legitimate or not. In order to solve the problem, different anomaly-based Intrusion Detection Systems were designed to increase the efficiency of attack detection and decrease the number of false positives. Such systems usually use different Machine Learning (ML) and Deep Learning (DL) methods.

Altulaihan et al. [5] developed an anomaly-based IDS designed to detect DoS attacks in the IoT environment using lightweight machine learning algorithms. Specifically, they utilized classifiers like Decision Trees and Random Forests for classifying the flow of traffic into benign and malicious ones. The study emphasized the need for lightweight detection solutions due to the limitations of IoT devices while ensuring good detection accuracy. While their experiments resulted in promising outcomes on benchmark IoT datasets, the analysis of this study was mainly performed in single-class DoS attacks. The study did not explore the issue of distributed attacks and distinguishing between different attack classes; therefore, it cannot be efficiently applied to DDoS volumetric attacks on IoT ecosystem.

A deep learning method was proposed by Mansoor et al. [6] to detect DDoS attacks aimed at the Software-Defined Networking (SDN) controllers. This technique relies on deep learning to classify the traffic in the network as either a legitimate one or malicious one to detect the DDoS attack. Nevertheless, the technique has limited generalizability to other attacks beyond DDoS attack due to its narrow scope that is restricted by experimental setting conditions.

Ahmadzadeh et al. [7] examined a deep convolutional neural network for detecting false data injection attacks. Although the study was in the smart energy context and not in the area of network intrusion detection, Ahmadzadeh et al. proved that time series signals can be transformed into time-frequency representations for use in DCNN-based feature extraction. From the results of the study, DCNN models can detect very subtle manipulations by adversaries that would be impossible to detect with rule-based monitoring systems. Though the study did not concentrate on DDoS detection specifically, it showed how powerful deep learning methods could be at identifying complex patterns of malicious activities in cyber-physical systems.

Ahmim et al. [8] proposed a hybrid deep learning architecture that was intended to detect DDoS attacks in IoT. The hybrid architecture of Ahmim et al. involved the use of CNN layers to capture local information and the use of LSTM layers to capture the relationship between the packets of the traffic over time. The hybrid architecture of Ahmim et al. was more efficient than single-layer-based architectures, indicating the potentiality of such architecture in IoT where the attack traffic is time-sensitive and not easily noticeable. Nevertheless, they only addressed the issue of binary classification of traffic.

Berríos et al. [9] presented an approach to detect and mitigate DDoS attacks using the machine learning-based framework for analyzing network traffic characteristics. The model incorporates both detection and mitigation techniques to minimize service disruptions, which are highly effective in various cases of DDoS attacks. Nevertheless, the framework can only be used for DDoS attacks; it uses static machine learning models that need to be trained for any new cyberattack, and does not include adaptive, explainable or proactive approaches to tackle the evolving cyberattacks or security challenges in IoT.

Moreover, Alshra'a et al. [10] investigated deep learning-based solutions to the problem of DoS attacks in software-defined networks. The authors considered recurrent architectures like RNN, LSTM and GRU models for sequence prediction of flow-based traffic data and showed that sequential learning could be an efficient approach to capturing complex attacks developing in time. It was shown that embedding DL techniques into SDN controllers allows detecting attacks close to real-time with a small delay. However, the authors did not consider multi-class problem, testing only binary classification of traffic data.

Sudar et al. [11] also considered SDN architecture, but employed classical machine learning techniques for detecting DDoS attacks. The authors developed a framework employing supervised models including Decision Trees and Random Forests for real-time classification of network flows. It was noted by the authors that employing lightweight ML models into SDN controllers is practical for fast reconfiguration of policies. Though the authors presented models with good classification accuracy for binary case, they did not test their scalability for simultaneous detection of different attacks and adaptation to complicated blended DDoS attacks.

Furthermore, Kumari and Mrunalini [12] developed a DoS attack detection system based on classical ML algorithms together with feature selection technique. The aim of the authors was selecting important features to get high accuracy of detection with low computational costs. It was shown that even simple classifiers could provide good results for moderate dataset size after removing irrelevant and redundant features. However, the authors considered binary problems mostly, not testing their solution on multi-class DDoS attacks.

Alanazi et al. [13] presented an ensemble deep learning approach based on LSTM, CNN, and GRU components, utilized in the detection of DDoS attacks within SDN environments. Their ensemble incorporated the use of both spatial feature extraction and temporal dependencies modeling in order to enhance the robustness of the detection system. A high level of binary classification accuracy was obtained on CICIDS2017 dataset, proving that hybrid architectures could provide more efficient solutions than separate networks. Nonetheless, their research was only oriented towards binary detection without addressing the issues related to multi-classification or real-time scalability, making their solution not fully applicable in SDNs exposed to multiple attack types at once.

Kumar et al. [14] presented a deep learning solution based on LSTM networks for the detection of DDoS attack traffic, utilizing CIC-DDoS-2019 dataset, which is used in the current work as well. This research was aimed at the identification of malicious flows in attack traffic and demonstrated the efficiency of sequence-based solutions in the modeling of temporal dependencies of attack traffic. Nonetheless, their research did not address the issue of multi-classification of various attack types. Thus, the current work expands this solution through the development of 7-class and 13-class DDoS detection scenarios.

Shaikh et al. [15] proposed an advanced hybrid deep learning architecture, which involves the utilization of Convolutional Neural Networks, Principal Component Analysis (PCA), and Vision Transformers in the detection of DDoS attacks. CNN was utilized to extract packet-level features of the data, PCA was utilized for reducing the dimensions, and attention mechanisms of the Transformer were used for modeling long-range dependencies. The results showed a significant increase in performance in comparison with the usage of standalone DL models. Nonetheless, their research is oriented mainly on the binary classification task, leaving the multi-class one unexplored.

In the research paper by Wang et al. [16], DDoS-MSCT, a novel architecture combining multiscale convolutional layers with Transformer blocks is introduced for DDoS detection at various granularities. It has shown good performance for binary classification of the attack thanks to the application of attention mechanisms that can help to emphasize the importance of different traffic features at different scales. The authors noted that the Transformer-based modeling allows significantly increasing the sensitivity to advanced attacks. Nevertheless, like many other approaches described above, the evaluation did not include multi-class classification tasks.

The study conducted by Sambangi and Gondi [17] introduces an unconventional machine learning solution for DDoS detection based on the multiple linear regression model. Despite the fact that regression models are not traditionally used in IDS, the study proved that traffic flow trends could be modeled in a very simple manner. The results of the research showed that regression models could help in detecting anomalies in the number of packets and traffic volume. However, such techniques are very limited in terms of the recognition of a broad range of DDoS attacks' strategies and variations and were not tested for multi-class labeling and real-time application.

In the paper by Fouladi et al. [18], an anomaly-based DDoS detection algorithm using sparse coding and frequency domain analysis is investigated. The framework converts the network flows to the frequency domain and uses sparse coding to discover the abnormalities in the traffic signal. The results of the research prove that there is an alternative approach to the traditional packet-based analysis for anomaly detection based on the signal processing. However, the technique was tested only for the binary classification task and its application in combination with deep learning algorithms was not evaluated.

Models for IDS based on deep learning methods were suggested for the DDoS detection in Agriculture 4.0, where the IoT is becoming widely used Ferrag et al. [19]. Their approach included training CNNs, DNNs, and RNNs using CIC-DDoS-2019 dataset for measuring the performance in binary and multi-class settings. While binary classification showed extremely good results with up to 99.9% accuracy, the multi-class setting performance showed quite lower results around 95%. This result is highly relevant for our research because it proves that moving from binary detection to multi-class classification is needed. This work is going to develop the ideas of the mentioned research by using hybrid approaches with feature selection and getting higher precision and better class discrimination in 7-class and 13-class settings.

Table I includes a comparison of the recent studies on DDoS detection that include datasets used, the goals, accuracy values, benefits, and drawbacks.

As can be seen from above, a number of traditional or hybrid approaches demonstrate high binary detection accuracy of more than 95% based on well-established or simplified datasets like NSL-KDD, KDDCup 99, or laboratory generated traces. Research papers [5], [8], [10], [11] prove the feasibility of using machine learning or hybrid deep learning techniques for detecting anomalies in IoT and SDN environments. Nevertheless, these studies usually focus on binary classification or specific use-cases and do not help to differentiate between several types of attacks existing together in realistic large networks. Besides, many researches with good accuracy figures use outdated datasets which fail to adequately represent the complexity of current DDoS traffic. Notably, just a few latest papers, like Ferrag et al. [19] and Kumar et al. [20], work with the CIC-DDoS-2019 dataset to simulate realistic conditions; yet, the attention is usually paid to binary classification or the accuracy is notably worse in the case of multi-class analysis. For example, even though Ferrag et al. [19] demonstrated near-perfect binary detection accuracy, the multi-class accuracy decreased to about 95%.

It is obvious from table I that despite good results of conventional and hybrid approaches in binary classification, multi-class detection on recent datasets is hardly studied enough. It becomes clear that the research will be motivated by the need to detect various attacks with the help of combination of three specialized deep learning architectures and feature selection.

III. Proposed Framework

This section presents the suggested deep learning intrusion detection system framework intended to counter the increasing sophistication of cybersecurity attacks. To enhance the threat detection and classification, we used CIC-DDoS-2019 dataset [20] provided by the Canadian Institute of Cybersecurity that simulates real-life DDoS attack instances. The methodology comprises three different datasets for our experiments. For Data 1 and Data 2, we constructed four model structures: LSTM [21], CNN [22], DNN [23], and MLP [24], each consisting of an autoencoder layer to optimize feature selection and decrease dimensionality before classification. We chose the above mentioned models due to their capabilities in working with sequences and effectiveness in various applications. As for Data3, which implies the classification of 13 categories

TABLE I
COMPARISON OF DATASETS, DETECTION FOCUS, REPORTED ACCURACY, ADVANTAGES AND LIMITATIONS OF RELATED WORKS

Paper	Dataset	Focus	Accuracy	Advantages	Limitations
[5]	Custom IoT traffic	ML-based anomaly IDS for IoT DoS	∼95% (binary)	Lightweight, suitable for constrained IoT devices	Single DoS only, no DDoS, no multi-class
[6]	KDDCup 99 / NSL-KDD	DL for DDoS	—	Broad survey of methods, identifies research gaps	No original model, no benchmarks
[7]	PV smart grid signals	DCNN for false data injection	∼97% (binary)	Demonstrates CNN strength for subtle cyber-physical anomalies	Not network DDoS, no multi-class
[8]	IoT dataset	Hybrid CNN-LSTM for IoT DDoS	∼96% (binary)	Combines spatial and temporal learning	Binary only, no multi-class granularity
[9]	KDDCup 99 / NSL-KDD	ML for DDoS detection	∼93% (binary)	Simple models, practical baseline	Outdated data, manual features, binary only
[10]	Custom SDN dataset	RNN/LSTM/GRU for SDN DoS	∼97% (binary)	Sequential learning, practical SDN integration	No multi-class, limited scope
[11]	Mininet SDN dataset	ML for SDN DDoS detection	∼92–95% (binary)	Lightweight, feasible for controller deployment	No DL, no multi-class
[12]	NSL-KDD	ML + feature selection for DoS	∼92% (binary)	Good feature selection, simple classifiers	Not scalable, no DL, no multi-class
[13]	CICIDS2017	Ensemble DL (CNN+LSTM+GRU) for SDN DDoS	99.77% (binary)	Strong binary results, robust hybrid	Older dataset, no multi-class
[14]	CIC-DDoS-2019	LSTM for DDoS detection	∼99% (binary)	Good binary performance, modern dataset	No multi-class, no hybrid design
[15]	CICIDS2017	CNN + PCA + Vision Transformers	∼99% (binary)	Innovative hybrid with attention	Binary only, no detailed multi-class
[16]	NSL-KDD	Multi-scale CNN + Transformer (DDoS-MSCT)	∼98% (binary)	Attention improves feature learning, multi-scale analysis	No multi-class, limited real-time tests
[17]	KDDCup 99	ML (multiple linear regression)	∼90% (binary)	Very lightweight baseline	Not robust for complex threats, no DL, binary only
[18]	Lab dataset	Sparse coding + frequency domain anomaly detection	∼91% (binary)	Unique signal processing approach	No DL integration, binary only
[19]	CIC-DDoS-2019	CNN, DNN, RNN for Agri DDoS	99.9% (binary), ∼95% (multi-class)	Real dataset, covers binary + multi-class	Multi-class accuracy lower, no advanced hybrid

of network traffic, we considered even more complex and specific models such as LSTM for learning dependencies in time, hybrid DNN-CNN for detecting spatial and sequential features and MLP for multi-class classification purposes. All the models were measured by such metrics as accuracy, F1-score, and recall to measure the ability of the models to detect cybersecurity threats with high precision and low false positive rate.

A. Execution Environment and Dataset

This project uses the CIC-DDoS-2019 dataset since it is one of the most complete and realistic datasets that can be used in detecting DDoS attacks. Unlike other older datasets such as NSL-KDD and CAIDA, CIC-DDoS-2019 is more comprehensive and contains more recent and realistic DDoS attacks. This makes it perfect for testing the robustness of the machine learning models under current network conditions. It consists of both PCAP files and preprocessed CSV files where each traffic instance is characterized by over 80 flow-based features, including but not limited to flow duration, packet size, bytes/sec and header information. In terms of the artificial DDoS attacks, there are twelve types of DDoS attacks in the dataset.

A.1. Dataset Splitting and Preprocessing

In order to train and test the model in a reliable way, the data was divided into three sets depending on various classification scenarios (II):

- *Binary Classification (Dataset1)*: The traffic is either *Benign* or *Attack*.
- *7-Class Classification (Dataset2)*: The traffic is split into one benign and six attacks classes.
- *13-Class Classification (Dataset3)*: The traffic is split into one benign and twelve attacks classes.

TABLE II
SUMMARY OF DATASET SPLIT

Subset	Classes	Training Instances	Testing Instances
Dataset1	2	1,500,000	375,000
Dataset2	7	2,500,000	1,070,000
Dataset3	13	4,900,000	2,100,000

The CIC-DDoS-2019 dataset was methodically divided into three datasets corresponding to the increasing levels of classification complexity: Binary, 7-Class, and 13-Class detections. The binary dataset represents a coarse-grained representation of network traffic by distinguishing between benign and attack flows. The 7-Class dataset is a more complicated setting since, along with the benign traffic, the classifier should classify six different types of DDoS attacks. The 13-Class detection task

represents the most complex case when 13 types of traffic, including 12 DDoS attacks, have to be distinguished by the IDS model. For each dataset, 80/20 splitting was used: for the Binary detection (Dataset1), approximately 1.5 million flows were selected for training and 375,000 flows were allocated for testing. Since there were six types of attack classes for the 7-Class setting (Dataset2), a larger number of samples was needed for the training, thus approximately 2.5 million samples were used for training and more than one million samples for testing. As the number of classes increases for Dataset3 (13-Class detection), the amount of both training and testing samples increases: almost five million training instances and more than two million testing instances were selected from the initial dataset. This approach provides sufficient variability in the training set to learn good representations of both benign and malicious traffic. Besides, the splitting of the dataset was performed at the flow-session level to avoid any data leakage between the training and testing sets.

A.2. Execution Environment

All model training, testing, and evaluation processes have been performed in easily available cloud-based environments, such as Google Colab and Kaggle kernels, for reproducibility and convenient use of free GPU and TPU computational resources. In particular, Google Colab has been utilized as the primary environment due to the presence of NVIDIA Tesla T4 GPUs that considerably speed up the deep learning models' training process on huge datasets, like CIC-DDoS-2019. Google Colab provides 12 GB of RAM per session, which has been properly handled by breaking down large CSV files into several smaller chunks to prevent memory overflow while preprocessing and training the models. In addition, Kaggle kernels have been used as an auxiliary platform for other experiments and hyperparameter tuning due to easy access to public datasets and preinstalled Python libraries. All deep learning structures have been implemented in Python 3.10 with the help of TensorFlow 2.x and Keras as frameworks for developing, training, and evaluating the proposed MLP, CNN, and LSTM models. Moreover, scikit-learn has been used for feature selection by applying ExtraTreesClassifier, partitioning of the dataset, and SMOTE-based minority class balancing during training. Data transformation and manipulation have been conducted by Pandas and NumPy, while Matplotlib and Seaborn have been used for visualizing training results, performance metrics, and feature importance.

A.3. Data Setup

The efficiency of deep learning algorithms depends significantly on the accessibility, quality, and processing of the training dataset. In the current research, the CIC-DDoS-2019 dataset is used due to being considered as an adequate representation of modern DDoS attacks with multiple vectors. However, there are two major difficulties associated with this dataset: extremely big file size and class imbalance. Specifically, the total dataset includes 11 huge training files with the combined size more than 22 GB and 7 separate testing files having more than 8 GB. The problem with handling these files arises in cloud computing platforms like Google Colab when one can use only up to 12 GB of RAM for each session. Hence, to overcome these restrictions, the following data preparation approach has been developed. Firstly, large raw CSV files have been broken down into smaller ones to be able to load and process data without exceeding the amount of RAM. Files which have the size larger than 8 GB have been loaded by chunking method. Second, cleaning procedures have been applied in order to delete redundant or empty rows, normalize data formatting, check integrity of extracted flow-based features. Furthermore, to balance strong class imbalance when the number of examples from the majority class (benign traffic) significantly exceeds some attack classes, data balancing methods like SMOTE have been used during preprocessing procedure. This approach allowed having training examples from all classes equally represented in each deep learning algorithm to provide better stability and accuracy of the proposed multi-class detection framework.

A.4. Strategic Deployment of Deep Learning Model

To meet the variety of DDoS detection needs in the real world, the CIC-DDoS-2019 dataset has been split into three subsets of data which are designed to perform classification tasks with different granularity:

- *Subset 1 (Binary Classification)*: The first subset includes a straightforward binary classification problem where benign traffic (*BENIGN*) is classified against malicious DDoS traffic called *Attack*. In this case, the partitions of data used for training and testing purposes are combined into one CSV-based dataset to allow the models to detect the differences between normal traffic and DDoS attacks in the whole input space.
- *Subset 2 (7-Class Classification)*: The second subset corresponds to a more realistic multi-class classification problem since each flow of traffic is assigned to one of the seven classes where there is only one class for benign traffic (*BENIGN*) and six classes for different kinds of DDoS attacks chosen for their prevalence in the data. In this scenario, the autoencoders become significant since they learn feature dependencies and input space reduction and, thus, draw attention to minor but significant differences in attack traffic patterns.
- *Subset 3 (13-Class Classification)*: The third and the most complicated subset includes a division of traffic into 13 classes that correspond to 12 DDoS attacks and 1 class of benign traffic. To be maximally precise in this subset of classification problems, the ExtraTreesClassifier is used to select the most useful and informative flow-based features of traffic patterns.

All the above-mentioned three subsets of classification problems compose a rather complete pipeline for the evaluation of the proposed framework for DDoS detection.

Table III highlights the CIC-DDoS-2019 dataset partitioning into three subsets for three kinds of classification problems. In the first row, we can see that the binary subset corresponds to a classification problem where the task is to discriminate between benign and all kinds of DDoS attacks; here, the autoencoder is needed to minimize feature dimensionality and

speed up the learning process of the MLP, CNN-DNN, and RNN-LSTM classifiers. The second row shows the 7-class subset in which traffic is split into one benign class and six DDoS attacks to check models' capability for multi-class discrimination; in this case, the use of the autoencoder becomes especially valuable since it helps to extract features separating close classes. The third row shows the most complex subset which includes 13 different classes – 12 DDoS attacks and benign traffic.

TABLE III
SUMMARY OF DATASET SUBSETS AND MODEL STRATEGIES

Subset	Classes	Feature Technique	Models Used
Subset 1: Binary	2 (BENIGN, Attack)	Raw features with autoencoder for compression	MLP, CNN–DNN, RNN–LSTM
Subset 2: 7-Class	7 (BENIGN + 6 attacks)	Autoencoder for non-linear feature extraction	MLP, CNN–DNN, RNN–LSTM
Subset 3: 13-Class	13 (BENIGN + 12 attacks)	ExtraTreesClassifier for feature selection	MLP, CNN–DNN, RNN–LSTM

B. Models of Framework for Multi-Class DDoS Detection

In this study, three deep learning architectures are presented for detection and classification of DDoS attacks in realistic traffic environments. Each of the model has been developed to capture a different aspect of flow-based network data and to tackle different challenges posed by multi-class DDoS detection. The first deep learning architecture is that of a Multi-layer Perceptron. It is an excellent choice as a base model for non-sequential deep learning. An MLP utilizes fully connected dense layers in modeling complex non-linear relationships between the input flow-based features and the output classes. Although its architecture is fairly simple, the model performs very well in dealing with high dimensional network data in conjunction with proper feature engineering and tuning. The second deep learning architecture is a hybrid of a 1D CNN and dense layers called CNN1D-DNN. The 1D CNN part in the model allows automatic extraction of local spatial patterns in traffic sequences hence improved feature representation. The third deep learning architecture is an RNN-LSTM which aims to learn temporal dependencies and sequential behavior in network flows.

B.1. Hybrid CNN1D-DNN

The Hybrid CNN1D-DNN model is built to enhance DDoS detection by combining one-dimensional convolutional layers and dense layers. The hybrid architecture exploits the capability of CNN1D to detect the local spatial patterns from flow-based traffic data. In DDoS detection, small scale abnormality in the form of packet bursts, unusual flow lengths, or sudden increases in connection count may manifest as local structure in the traffic record. Convolutional layers act as the feature extractors by searching the local patterns from the input traffic data that may be related to any possible DDoS attacks or anomalies. Following the convolutional layers, DNN layer performs the high-level representation learning and classification task. The dense layers combine the extracted local features to obtain the final predictions on the input being benign traffic or particular class of DDoS attack. By combining the automatic local structure finding and deep abstract feature learning, this hybrid architecture is ideally suitable for the structured sequential traffic data of today's network and IoT environment.

B.2. Multi-Layer Perceptron (MLP)

The MLP model applied to this study is a baseline deep learning architecture for DDoS detection. It consists of multiple fully connected dense layers, where each layer learns non-linear mappings from input features to output label. For our purpose, the MLP architecture includes three dense layers. The number of neurons in the first dense layer is set to 192, which provides a good balance between computational efficiency and representational power. Second dense layer has only 96 units in order to gradually reduce the size of feature space and refine it further. Finally, one more dense layer precedes the classification by the softmax layer. MLP architecture is suitable in the scenario, where input data does not include any explicit temporal ordering but rather preprocessed tabular features.

B.3. Long Short-Term Memory (LSTM)

In the LSTM model, temporal dependencies inherent in the nature of network traffic can be effectively leveraged. The reason behind the idea lies in the fact that the current state of the network can often be predicted based on the past behavior of the traffic flow, which makes the LSTM capable of detecting temporal changes in the evolution of the traffic, which is typical of the sustained and periodic behavior of DDoS attacks. The key element of the LSTM architecture is the presence of the memory cells and gates, which determine the amount of previously known information needed to retain at each step, thus making the LSTM an efficient method to model long-term dependencies in the time-series data. In our case, the LSTM will analyze the sequences of flow features and learn the difference between normal and attack traffic using the temporal characteristics of the traffic features. Such an analysis of the temporal dependencies is especially helpful in cases when the attackers are trying to avoid detection by gradually raising the traffic level and coordinating the activities of distributed sources.

In Fig.1, the architecture of the three proposed deep learning models for DDoS detection is shown. It can be seen that in case of MLP, the non-linear mapping is done through the sequence of the fully-connected layers of the densely-connected dense network. The architecture of the Hybrid CNN1D–DNN model is a combination of the convolutional layers and the dense layers and allows for the detection of subtle anomalies in flow sequences. The LSTM model is based on the memory cells, which allow to capture the temporal dependencies, and thus the system will learn the evolution of the attack patterns over time.

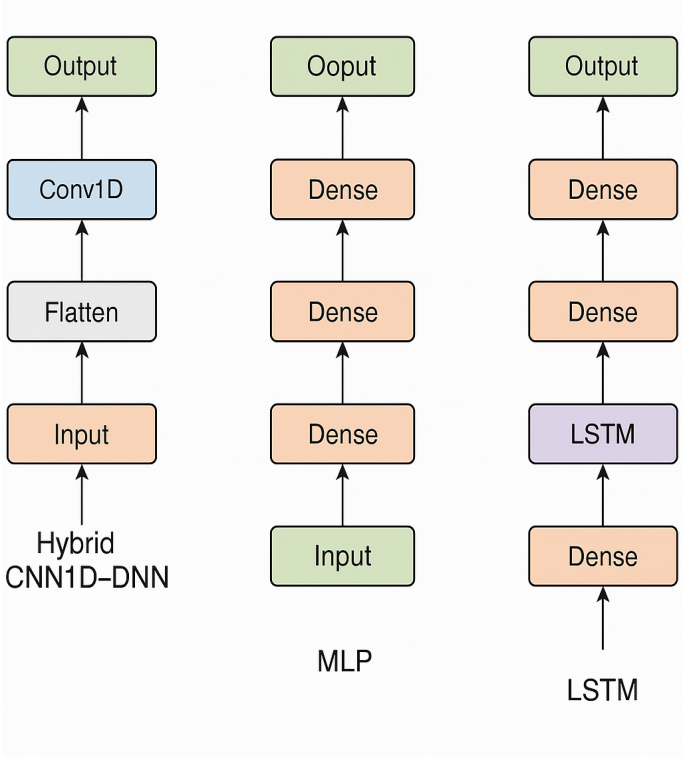


Fig. 1. Architectures of the three proposed deep learning models

IV. Simulation and Performance Evaluation

To analyze the performance of the deep learning models that have been proposed to detect the occurrence of DDoS attacks, this study will use five performance measures which include: accuracy, precision, area under the receiver operating characteristic curve (AUC-ROC), false positive rate (FPR) and the confusion matrix.

A. Performance of Proposed Models

In our experiments, we used three neural network architectures, namely, MLP, Hybrid CNN1D-DNN, and RNN-LSTM, in order to analyze their performance on the task of detecting DDoS attacks using the CIC-DDoS-2019 dataset in three different classification settings: binary, 7-class, and 13-class classification problems. We trained all three neural networks using the identical preprocessed feature set, however, tuning their hyperparameters separately in order to show their individual strengths in pattern recognition from network flows. The MLP architecture is oriented towards non-sequential feature learning via dense layers. The hybrid CNN1D-DNN architecture combines one-dimensional convolution with dense layers in order to learn both local sequential dependencies and hierarchical features from the data. Finally, the RNN-LSTM architecture uses long short-term memory units in order to capture temporal dependencies across network flows.

Table IV presents the accuracy of classification of network flows provided by all three models in the three tasks. In the case of binary classification, the MLP showed the best performance with 99.80% accuracy followed by Hybrid CNN1D-DNN and RNN-LSTM, with 99.75% and 99.70% accuracies, respectively. These results confirm that all three models provide effective recognition of DDoS attacks in the simple attack-versus-benign setting. For 7-class classification problem, CNN1D-DNN model showed slightly better performance compared to other two models, providing 97.10% accuracy, which indicates the usefulness of convolutional component in distinguishing between different attack classes. RNN-LSTM showed good performance (97.08%) which proves the effectiveness of temporal modeling of DDoS attack streams, while MLP provided good results (96.09%). Finally, in 13-class classification problem, MLP again provided the best result (99.62%), being beneficial due to dense architecture and optimized feature selection procedure. The second and third place went to CNN1D-DNN and RNN-LSTM models with 98.74% and 97.24% accuracy, respectively.

TABLE IV
Accuracy of Proposed Models for Binary, 7-Class, and 13-Class Classification

Model	Task	Accuracy
MLP	Binary	99.80%
Hybrid CNN1D-DNN	Binary	99.75%
RNN-LSTM	Binary	99.70%
MLP	7-Class	96.09%
CNN1D-DNN	7-Class	97.10%
RNN-LSTM	7-Class	97.08%
MLP	13-Class	99.62%
CNN1D-DNN	13-Class	98.74%
RNN-LSTM	13-Class	97.24%

B. Detailed Precision for 13-Class Detection

In order to measure how well each type of attack is classified, Table V shows the class level precision rate achieved using the proposed MLP approach for detecting 13 different types of DDoS attack classes. It can be seen that the precision level of the vast majority of the classes is extremely high. The proposed model is able to achieve perfect precision (1.00) when classifying benign traffic and major amplification based attacks, such as DrDos DNS, LDAP, MSSQL, NTP, SNMP, SSDP and UDP. Very high precision (greater than 0.99) can also be obtained when classifying SYN Flood and TFTP attack classes, which are typically used in volumetric attacks, showing the model's ability to classify both reflective and direct flooding attacks without producing many false positive results. However, there is a slight decrease in precision (to 0.99) when dealing with DrDos NetBIOS and UDP-Lag attacks due to the fact that the model may occasionally mistake some other class for these classes because they have almost identical flow features. However, the most problematic attack class is the WebDDoS attack class, which is characterized by much lower precision (0.58).

C. False Positive Rates

Table VI presents the False Positive (FP) rates attained by the three proposed deep learning algorithms in different classification cases. From Table VI above, it is clear that MLP has a very low false positive rate that starts from 0.6% in the case of binary classification while staying below 1.2% in the more complicated 13-class classification. In a similar vein, Hybrid CNN1D-DNN and RNN-LSTM algorithms have FP

TABLE V
CLASS-LEVEL PRECISION FOR MLP ON 13-CLASS TASK

Class	Precision
BENIGN	1.00
DrDos DNS	1.00
DrDos LDAP	1.00
DrDos MSSQL	1.00
DrDos NTP	1.00
DrDos NetBIOS	0.99
DrDos SNMP	1.00
DrDos SSDP	1.00
DrDos UDP	1.00
Syn	1.00
TFTP	1.00
UDP-Lag	0.99
WebDDoS	0.58

rates below 1.6% in all examined scenarios. It is significant to note that the low false positive rates of the proposed deep learning models are quite relevant as it shows that the high detection rates and AUC values of the models are not realized at the cost of classifying a lot of benign network traffic into the attack class. In a real-life intrusion detection system (IDS), many false positives lead to the generation of security alerts that are unnecessary in addition to increasing the work burden of the network administrators, which eventually leads to alarm fatigue. In conclusion, it is necessary to have a low FP rate in order to guarantee the reliability and efficiency of the IDS.

TABLE VI
FALSE POSITIVE RATES OF PROPOSED MODELS ON THE CIC-DDOS-2019 DATASET

Model	Binary Task FP Rate (%)	7-Class Task FP Rate (%)	13-Class Task FP Rate (%)
MLP	0.6	0.9	1.2
Hybrid CNN1D-DNN	0.7	1.1	1.4
RNN-LSTM	0.8	1.2	1.6

D. Confusion Matrix Analysis

Figure 2 shows the confusion matrix of the proposed MLP classifier for the 13-class DDoS classification problem including benign traffic and 12 types of attacks from the CIC-DDoS-2019 dataset. The high concentration of the values in the main diagonal of the table is an indicator of the proper classification of most samples for all the traffic types. First of all, the MLP performs well at the classification of common attacks like DrDoS DNS, LDAP, NTP, MSSQL, SNMP, UDP, SYN, and TFTP; thus, it demonstrates high capability in recognizing their traffic flow patterns. BENIGN traffic is properly classified with very few wrong decisions, and it proves the low level of false positives of the proposed method. There are only some misclassifications of DrDoS NetBIOS and UDP-Lag attacks that might happen because of similar flow and protocol patterns of these types of traffic. WebDDoS is considered to be the most difficult class among others due to higher level of confusion because of the similarity in traffic patterns to benign or other DDoS attacks.

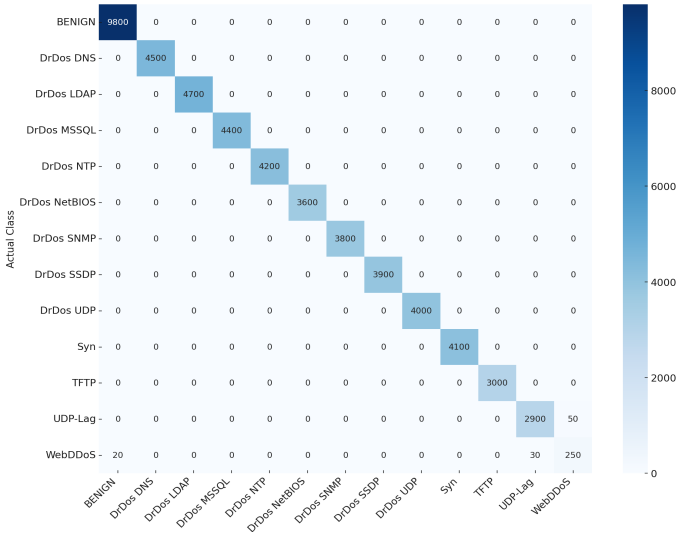


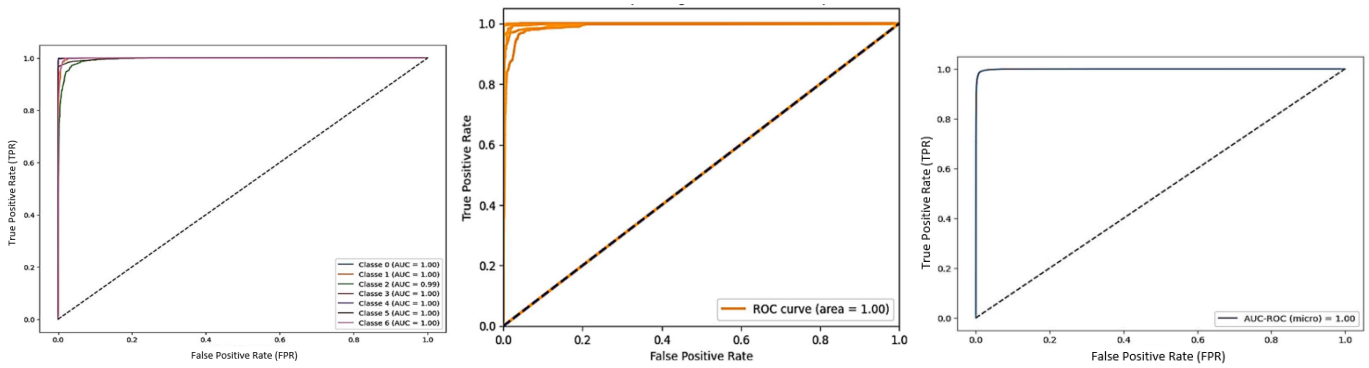
Fig. 2. Confusion Matrix Showing Class-Level Predictions for Proposed MLP

E. AUC-ROC

The ROC curves of the proposed three deep learning models, including MLP, Hybrid CNN1D-DNN, and RNN-LSTM, trained using the CIC-DDoS-2019 dataset are shown in Fig.3. The ROC curve depicts the TPR-FPR relationship for different classifier decision thresholds and is an effective way to evaluate the discrimination capability of the models under consideration. As can be seen from Fig.3, all three models demonstrate very good discrimination capability, as their ROC curves are very close to the upper left corner of the figure. This implies that the proposed models have relatively high attack detection capability and produce only a small number of false alarms, which is a required property of a reliable DDoS detection system. In terms of discrimination capability, the MLP model outperforms the other two models in the sense of achieving the highest AUC value and having the best balance between the rate of detection and generation of false alarms. The Hybrid CNN1D-DNN and RNN-LSTM models also show good ROC performance and therefore confirm their good capacity to learn the relevant patterns from network traffic. The obtained ROC values are consistent with the previously found accuracy and precision values.

F. Benchmark Comparison

Table VII shows a comparative benchmarking of the proposed MLP method with other relevant state-of-the-art algorithms, as well as the class level precision of 13 classes of DDoS attacks. These include the CNN-based model by Ferrag et al. [19], the ensemble LSTM-CNN-GRU method by Alanazi et al. [13], and the CNN-LSTM hybrid model by Ahmim et al. [8]. The table indicates that the proposed MLP algorithm yields an accuracy of 99.62% for the 13 classes problem, and thus performs better than Ahmim et al.'s, which yields an accuracy of 80.34% for multi-class classification, and performs much better than Ferrag et al.'s CNN accuracy of 95% in multi-class detection. Although Ferrag et al. and Alanazi et al. have attained slightly higher accuracy in the



(a) CNN-dataset2 (b) MLP-dataset2 (c) RNN-LSTM-dataset2

Fig. 3. Results of AUC-ROC for each model.

binary classification problem of 99.95% and 99.77%, respectively, their results demonstrate the well-known fact about the tradeoff between the simpler binary classification and the more informative multi-class classification needed for response planning. Moreover, the proposed MLP method has a very low false positive rate of 0.87% and an extremely high AUC-ROC of 0.998, which is an indication of very good separation of the classes and does not lead to unnecessary false alarms.

TABLE VII
BENCHMARK COMPARISON OF PROPOSED MLP WITH OTHER RELATED WORKS

Model/Reference	Accuracy	FPR	AUC-ROC
Ferrag et al. Multi-class (CNN) [19]	95%	2–5%	0.970
Alanazi et al. Binary (Ensemble LSTM+CNN+GRU) [13]	99.77%	0.80%	0.995
Ahmim et al. Multi-class (CNN+LSTM) [8]	80.34%	4–6%	0.860
MLP (Proposed, 13-Class)	99.62%	0.87%	0.998

V. CONCLUSION AND FUTURE WORK

The aim of the presented paper was the design and evaluation of a deep learning based model for accurate detection and multi-class classification of Distributed Denial-of-Service attacks using realistic large-scale network traffic from the CIC-DDoS-2019 dataset. Three architectures – MLP, Hybrid CNN1D-DNN and RNN-LSTM – were considered to analyze various learning techniques for detecting complex patterns. The achieved results prove the ability of the proposed models to detect relevant features of network traffic and get high detection performance at low levels of false positives. The detection accuracy was higher than 99% and proved the possibility of applying of the developed models in practical networks. The comparative analysis with recent approaches proves the efficiency of the suggested model for fine-grained DDoS detection. In contrast to several recent works, where binary DDoS classification was considered, the current work presents the results of the consideration of multiple DDoS attack types.

For the future research it would be necessary to incorporate online learning and retraining into this framework in order to solve the problem of concept drift in the changing environment. Moreover, integration of the presented models into the software-defined networking and edge computing environments can provide low latency detection in distributed networks. Future research can also focus on using transformer architectures and self-supervised learning.

REFERENCES

[1] O. Ebrahem, S. Dowaji, and S. Alhammoud, "Towards a minimum universal features set for IoT DDoS attack detection," *Journal of Big Data*, vol. 12, p. 88, 2025. https://doi.org/10.1186/s40537-025-01146-1

[2] F. S. de Lima Filho, F. A. F. Silveira, A. de M. Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," *Security and Communication Networks*, vol. 2019, Article ID 1574749, 15 pages, 2019. https://doi.org/10.1155/2019/1574749

[3] F. Salatino, M. G. Spina, M. Tropea, and F. De Rango, "Detecting DDoS Attacks Through AI Driven SDN Intrusion Detection System," in *Proc. 2024 IEEE 21st Consumer Communications & Networking Conf. (CCNC)*, Las Vegas, NV, USA, 2024, pp. 990–993. https://doi.org/10.1109/CCNC51664.2024.10454798

[4] K. A. Dhanya, S. Vajipayajula, K. Srinivasan, A. Tibrewal, T. S. Kumar, and T. G. Kumar, "Detection of Network Attacks Using Machine Learning and Deep Learning Models," *Procedia Computer Science*, vol. 218, pp. 57–66, 2023. https://doi.org/10.1016/j.procs.2022.12.401

[5] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors*, vol. 24, no. 2, p. 713, 2024. https://doi.org/10.3390/s24020713

[6] A. Mansoor, M. Anbar, A. A. Bahashwan, B. A. Alabsi, and S. D. A. Rihan, "Deep learning-based approach for detecting DDoS attack on software-defined networking controller," *Systems*, vol. 11, no. 6, Art. no. 296, Jun. 2023. https://doi.org/10.3390/systems11060296

[7] M. Ahmadzadeh, A. Abazari, M. Ghafouri, A. Ameli, and S. M. Muyeen, "A Deep Convolutional Neural Network-Based Approach to Detect False Data Injection Attacks on PV-Integrated Distribution Systems," *IEEE Access*, vol. 12, pp. 2803–2816, 2024. https://doi.org/10.1109/ACCESS.2023.3348549

[8] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," *IEEE Access*, vol. 11, pp. 119862–119875, 2023. https://doi.org/10.1109/ACCESS.2023.3327620

[9] S. Berríos, S. Garcia, P. Hermosilla, and H. Allende-Cid, "A Machine-Learning-Based Approach for the Detection and Mitigation of Distributed Denial-of-Service Attacks in Internet of Things Environments," *Applied Sciences*, vol. 15, no. 11, Art. no. 6012, 2025. https://doi.org/10.3390/app15116012

[10] A. S. Alshraa, A. Farhat, and J. Seitz, "Deep Learning Algorithms for Detecting Denial of Service Attacks in Software-Defined Networks," *Procedia Computer Science*, vol. 191, pp. 254–263, 2021. https://doi.org/10.1016/j.procs.2021.07.032

[11] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj, and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN Using Machine Learning Techniques," in *Proc. 2021 Int. Conf. Comput. Commun. Informat. (ICCCI)*, Coimbatore, India, 2021, pp. 1–5. https://doi.org/10.1109/ICCCI50826.2021.9402517

[12] K. Kumari and M. Mrunalini, "Detecting Denial of Service Attacks Using Machine Learning Algorithms," *Journal of Big Data*, vol. 9, p. 56, 2022. https://doi.org/10.1186/s40537-022-00616-0

[13] F. Alanazi, K. Jambi, F. Eassa, M. Khemakhem, and A. Basuhail, "Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network," *Intelligent Automation & Soft Computing*, vol. 33, no. 2, pp. 923–938, 2022. https://doi.org/10.32604/iasc.2022.024668

[14] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS Detection Using Deep Learning," *Procedia Computer Science*, vol. 218, pp. 2420–2429, 2023. https://doi.org/10.1016/j.procs.2023.01.217

[15] J. Shaikh *et al.*, "Advancing DDoS Attack Detection with Hybrid Deep Learning: Integrating Convolutional Neural Networks, PCA, and Vision Transformers," *International Journal on Smart Sensing and Intelligent Systems*, vol. 17, no. 1, 2024. https://doi.org/10.2478/ijssis-2024-0040

[16] B. Wang, Y. Jiang, Y. Liao, and Z. Li, "DDoS-MSCT: A DDoS Attack Detection Method Based on Multiscale Convolution and Transformer," *IET Information Security*, vol. 2024, Article ID 1056705, 2024. https://doi.org/10.1049/2024/1056705

[17] S. Sambangi and L. Gondi, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression," *Proceedings*, vol. 2020, no. 63, p. 51, 2020. https://doi.org/10.3390/proceedings2020063051

[18] R. F. Fouladi, O. Ermis, and E. Anarim, "Anomaly-Based DDoS Attack Detection by Using Sparse Coding and Frequency Domain," in *Proc. 2019 IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Istanbul, Turkey, 2019, pp. 1–6. https://doi.org/10.1109/PIMRC.2019.8904393

[19] M. A. Ferrag, L. Shu, D. Haddad, and K.-K. R. Choo, "Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0," *Electronics*, vol. 10, no. 11, p. 1257, 2021. https://doi.org/10.3390/electronics10111257

[20] M. C. P. Saheb, M. S. Yadav, S. Babu, J. J. Pujari, and J. B. Maddala, "A Review of DDoS Evaluation Dataset: CICDDoS2019 Dataset," in *Energy Systems, Drives and Automations (ESDA 2021)*, J. R. Szymanski, C. K. Chanda, P. K. Mondal, and K. A. Khan, Eds. Singapore: Springer, 2023, vol. 1057, *Lecture Notes in Electrical Engineering*. https://doi.org/10.1007/978-981-99-3691-5_34

[21] A. H. M. Almawgani, "RNN-LSTM Model for Reliable Optical Transmission in Flexible Switching Network Systems," *Wireless Networks*, vol. 30, pp. 1575–1589, 2024. https://doi.org/10.1007/s11276-023-03599-9

[22] R. Pandey, S. Uziel, T. Hutschenreuther, and S. Krug, "Towards Deploying DNN Models on Edge for Predictive Maintenance Applications," *Electronics*, vol. 12, no. 3, p. 639, 2023. https://doi.org/10.3390/electronics12030639

[23] L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma, J. Santamaría, M. A. Fadhel, M. Al-Amidie, and L. Farhan, "Review of Deep Learning: Concepts, CNN Architectures, Challenges, Applications, and Future Directions," *Journal of Big Data*, vol. 8, no. 1, p. 53, 2021. https://doi.org/10.1186/s40537-021-00444-8

[24] A. Ostovar, D. D. Davari, and M. Dzikuc, "Determinants of Design with Multilayer Perceptron Neural Networks: A Comparison with Logistic Regression," *Sustainability*, vol. 17, p. 2611, 2025. https://doi.org/10.3390/su17062611



Haythem Hayouni is an Assistant Professor of Computer Science at the Higher Institute of Computer Science of Kef, University of Jendouba, Tunisia. He obtained his Master's degree in Computer Science from the National School of Computer Science (ENSI), University of Manouba, Tunisia, in 2012 and his Ph.D. in Information and Communication Technologies from the Higher School of Communications of Tunis (SupCom), University of Carthage, Tunisia, in 2018. His research interests are in cryptography, cybersecurity, wireless sensor networks, machine learning, and Internet of Things (IoT). His areas of expertise are IoT communication, blockchain, encryption, security, OS, Network Virtualization, Deep Learning, and distributed applications. Now he works on security in networks and applications, detection of attacks, wireless sensor networks, real-time Quality of Service (QoS), Deep learning, and quantum cryptography.



Wala Ben Rhouma is a PhD student at Polytechnique Montreal, Canada. She obtained her Master's degree in Computer Science from the Higher Institute of Computer Science of Kef, University of Jendouba, Tunisia, in 2024, in which she focused on deep learning and cybersecurity. Her graduate research was centered around using neural networks for real-time intrusion detection systems, defense against adversarial attacks, and privacy-preserving learning.