UDC 004.9 **doi:** https://doi.org/10.20998/2522-9052.2025.4.14

Mohammad-Reza Feizi-Derakhshi[1,2], Watheq Ghanim Mutasher AL-Talebei[1]

[1] Department of Computer Engineering, University of Tabriz, Tabriz, Iran
[2] Uruk University, Baghdad, Iraq

DCGAN DATA BALANCING TO IMPROVE ACCURACY OF HYBRID CNN-LSTM INTRUSION DETECTION FRAMEWORK IN SDN ENVIRONMENT

Abstract. Maintaining robust network security in Software-Defined Networking (SDN) systems has become increasingly challenging due to sophisticated cyber-attacks and the centralized nature of SDN. **This paper** introduces a novel intrusion detection system based on a hybrid deep learning model that combines Convolutional Neural Networks (CNN) for spatial feature extraction and Long Short-Term Memory (LSTM) networks for temporal dependency extraction. **The approach** is applied to the large InSDN dataset, having labeled traffic for normal activity as well as various classes of attacks, to train multi-class as well as binary classifiers. Synthetic samples are generated based on Deep Convolutional Generative Adversarial Networks (DCGAN) in order to effectively tackle the issues due to class imbalance and thereby enhance the detection rate for minority classes of attacks. **Experimental tests** carried out in a simulated SDN network with Mininet and Hping3 have outstanding performance, with the binary model achieving 99.81% accuracy and the optimal multi-class model achieving 99.4% accuracy. **Such promising results** demonstrate the capability of the proposed framework to offer an efficient and scalable real-time intrusion detection solution for the modern SDN infrastructures.

Keywords: Software-Defined Networking; Attacks; CNN; LSTM; DCGAN; Mininet.

Introduction

In today's more globalized world, the convergence of the Internet of Things (IoT) and Software-Defined Networking (SDN) is much promising for enhancing Quality of Service (QoS) and traffic bottlenecks. Using the help of advanced machine learning methodologies, such networks can predict traffic behavior intelligently, dynamically adjust network configurations, and allocate resources in real-time to meet varying demands. Nevertheless, convergence of the two technologies is not an issue-free exercise. SDN and IoT platforms must overcome essential challenges such as security vulnerabilities, power consumption limitations, and the ever-present need to maximize performance. Furthermore, adaptive technologies such as dynamic network slicing for dividing a physical network into multiple logical networks to meet specific service requirements, multi-objective optimization, and edge computing that facilitates data processing closer to the data source are important factors in maximizing resource usage and system response time [1–4]

Real-time vulnerability detection in SDN networks becomes an increasing issue due to the centralized control model as well as ongoing, dynamic cyber threats. The literature has witnessed numerous models being suggested for handling this problem. For instance, hybrid Deep Autoencoder and Random Forest (DAERF) models have been proposed to improve SDN intrusion detection based on adaptive multi-layer approaches—such as active monitoring and identification via entropy levels—that minimize degradations in controller performance [5, 6]. Also, deep learning techniques, i.e., Convolutional Neural Networks (CNNs), have been demonstrated to be capable of learning high-level features automatically from structured traffic data to identify malicious activities like phishing and malware attacks with great accuracy even despite the issues that come with data preprocessing and computational complexity [7]. In addition, new studies using ensemble machine learning algorithms have exhibited significant progress in real-time vulnerability detection in SDN networks with good performance and robustness for adaptive security monitoring [8].Present improvements in SDN security include ensemble and hybrid models to detect threats in real time, while load-balancing and clustering metrics help network topologies distribute workloads and use less energy, Similarly, adversarial balancing techniques—like those in IC-BGAN—could further optimize SDN threat detection by ensuring model stability and fairness when handling imbalanced attack traffic [9, 10].

Their integration in Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) networks produces a robust hybrid model that can detect both spatial and temporal relationships within sequential data such as network traffic. CNN-LSTM architectures were demonstrated to yield promising performance in reducing false alarms and maximizing detection rates by being capable of learning complex patterns of known and unknown threats efficiently, thereby proving to be very apt for intrusion detection in real-time environments in SDN atmospheres [11, 12]. Further, tools like Mininet are typically employed to emulate SDN setups, offering a customizable testbed made up of controllers, switches, and hosts, which is important in gauging the performance of such detection models across different network scenarios [13, 14].

Although there are positive findings on the performance of emerging intrusion detection systems (IDS) in SDN networks, some significant issues plague their efficiency at scale. Most current methods give an efficient process for extracting features, which will not identify a large portion of behavioral indicators of varied attacks and thus reduce the system's capability in precise identification of composite threats. Besides, scalability remains an issue since such approaches will perform badly in real-world network settings with their high data rate and dynamic nature, leading to low adaptability in real-time systems. Problems such as class imbalance, where benign traffic far exceeds malicious traffic, also

skew the detection process and lead to high false-negative rates. Also, the lack of transparency and explain ability within the decision-making process makes it more difficult for network administrators to understand and rely on the output of such systems, and therefore in further optimization and calibration. There is a significant need for robust and deep hybrid structures to overcome these problems by enhancing feature extraction, scalability, improved class imbalance handling, and explainable decision-making processes, thus helping to provide more efficient and effective IDS solutions for SDN domains [15, 16].

In this work, an efficient and scalable real-time intrusion detection system in SDN environments using a hybrid CNN-LSTM is introduced. Class imbalance is addressed through the use of Deep Convolutional Generative Adversarial Networks (DCGAN) to generate minority-class synthetic samples to enhance classification performance. The introduced system is evaluated and implemented according to the Mininet emulator and proved its effectiveness and applicability for effectively detecting and classifying a wide range of network attacks in real-time.

Finally, this paper makes the following primary contributions: (1) a hybrid CNN-LSTM model architecture for real-time intrusion detection in SDN; (2) use of DCGAN to oversample the minority and majority classes of the dataset; and (3) system deployment and testing on a Mininet-based SDN emulator for demonstration of real-world relevance and effectiveness.

1. Related Work

Deep learning has also emerged as a useful tool to enhance security in Software-Defined Networking (SDN) in the form of building intelligent and scalable real-time intrusion detection systems (IDS) using learning complex patterns from high-dimensional network traffic.

In [15], the authors introduce a CNN-LSTM based hybrid intrusion detection model for detecting spatial and temporal features in SDN traffic. The authors describe the design of the model and its evaluation through a Mininet-based testbed, handling issues such as limited feature extraction and class imbalance in real-time detection while imposing minimal performance overhead.

For instance, the authors of [16] presented a hybrid CNN-based model and a novel regularization technique known as SD-Reg for intrusion detection in SDNs. The model was evaluated using the InSDN dataset in binary and multi-class modes with satisfactory accuracy. However, it was reported to be prone to imbalanced data, particularly minority attack class detection. To address this, [17] presented CNN-LSTM and LSTM-FCN models in industrial IoT environments and evaluated them on TON-IoT, BoT-IoT, and UNSW-NB15 datasets. Notably, the proposed models achieved over 99.9% accuracy on two datasets, reflecting strong performance in attack detection and classification for various IoT platforms. Further, [18] conducted a comprehensive review of machine and deep learning-based solutions for SDN. Their findings identify numerous limitations, such as non-scalability, constrained real-time responsiveness, and poor adaptability to new threats. As such, they highlighted the importance of integrating solutions encompassing dataset quality, model interpretability, and compatibility with SDN controllers. Additionally. recent studies indicate that integrating visual analytics, such as nesting circles, with temporal models might improve the understanding of alerts, and Transformer designs have the capacity to capture intricate assault sequences. Both of these approaches could potentially supplement CNN-LSTM techniques in SDN environments [19].

The authors in [20] employed a CNN-LSTM combined model to detect DDoS attacks from a labeled dataset. Impressive performance was observed by their model achieving 99.9% accuracy at 500 epochs and showing clear separation of benign and malicious traffic with proof presented by a perfect confusion matrix. Jyothsna et al. [21] employed Grey Wolf Optimization (GWO) in combination with a CNN-LSTM model trained on the InSDN dataset in another study. Their approach reached 95.69% accuracy in detecting seven various attack types, which is indicative of significant improvements over conventional ML approaches in SDN settings. Class imbalance is one of the most common issues in IDS design. To overcome this, [22] employed Generative Adversarial Networks (GANs) to generate synthetic minority class samples. Their GAN-based models drastically reduced false positives and improved detection accuracy on benchmarks such as NSL-KDD and UNSW-NB15. In parallel, in the broader ML-SDN research community, [23] proposed hybrid IDS models that incorporated deep learning along with traditional models. Correspondingly, [24] sought to combine LightGBM with feature selection techniques for enhancing attack detection in cloud-based SDN environments.

Moreover, [25] designed a DDoS detection framework based on Apache Spark with high-speed data processing and utilized Decision Tree classifiers with a high accuracy of 93.6%. This exemplifies the effectiveness of distributed ML techniques on SDN platforms. Similarly, [26] introduced the SRAIOT algorithm—a secure routing protocol based on SDN for IoT networks—incorporating intrusion detection features into the hierarchical control architecture of SDN to improve both threat mitigation and routing efficiency. Additionally, [27] studied deep learning models for intrusion detection in SDNs with a particular emphasis on model explain ability and low-latency detection. Their study demonstrated that hybrid models were always superior to standalone ML or DL models. On top of real-time detection. [28] proposed Deep-IDS, a system designed for IoT nodes from a 64-unit LSTM model which can learn to evolve with evolving threats through online learning. They confirmed better performance than traditional IDS solutions. Similarly, [29] suggested an online ML model, which is an ensemble-based SDN-optimized model, for enhancing DDoS detection and mitigation and found a significant improvement over traditional approaches.

In healthcare IoT, [30] designed an intelligent IDS system by combining Support Vector Machines (SVM)

with deep neural networks (DNN), reporting high detection rates for healthcare-sensitive environments. Furthermore, [31] proposed a novel image-based representation of sequential packet data and used CNNs to identify low-rate DDoS attacks. Their method achieved detection accuracies ranging from 97.7% to 99% on various attack types. In a broader review, [32] gave an overall overview of machine and deep learning methods for anomaly detection in SDNs. They emphasized their attempt to reduce detection errors and enhance adaptability in DDoS-prone networks. From this point, [33] utilized meta-learning on a custom dataset of over one million records, which were generated using Mininet and Wireshark. Their real-time IDS model outperformed traditional classifiers in server-based attack detection.

In another intriguing research, [34] demonstrated that Support Vector Machines (SVM) and Decision Trees (DT) can efficiently classify DDoS traffic in SDN, particularly if trained on custom-crafted datasets simulating real-world attacks. Finally, [35] proposed a hybrid CNN-BiLSTM model to detect anomalous user behavior in social networks. Their approach achieved an F1-score of 0.82 on the VAST 2008 dataset, showing the advantage of the fusion of spatial and temporal features in detecting anomalies in complex data scenarios. As a conclusion, the literature herein irrevocably proves the prospects of hybrid deep learning models—specifically CNN-LSTM—in effective network intrusion detection for SDN scenarios. However, perennial challenges such as class imbalance, real-time scalability, and reliable detection of minority classes remain. The present work attempts to bridge these gaps by combining DCGAN-driven data augmentation and realizing CNN-LSTM models in an SDN emulator environment in real time, thereby improving both detection efficiency and system responsiveness.

2. Dataset

The InSDN dataset is a standard flow-based dataset used to test detection systems for DDoS, DOS, and other attacks in Software Defined Networks (SDN). Multi-layered security measures, encryption, updates, and user awareness are required for proper defense [36]. The intrusion detection systems in Software-Defined Networks (SDN). It includes benign and different types of attacks found in SDN components like DoS, DDoS, Brute force, Web attacks, exploits, probes, and botnets. The dataset contains traffic from applications like HTTPS, HTTP, SSL, DNS, email, FTP, and SSH [37]. The table 1¬ provides the sample of the dataset.

Table 1 – **SDN Dataset**

Name	DDoS	Probe	Normal	DoS	BFA	Web-attack	Botnet	U2R
Account	121942	98129	68424	53616	1405	192	164	17

3. Proposed System

The proposed system provides a comprehensive real-time intrusion detection system for Software-Defined Networking (SDN) based on a hybrid deep learning architecture in the form of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The system operates at two hierarchical levels: binary and multi-class classification.

At the binary level, the system initially separates malicious traffic from benign traffic with the aid of the InSDN dataset. The data set is taken through strict preprocessing measures like feature selection, normalization, and splitting into train, validation, and test sets prior to training. The CNN module extracts spatial features from network packets, and the LSTM module for temporal dependencies so that the model will be able to detect advanced attack patterns along the timeline. The trained binary classifier is stored and employed in an emulated SDN environment. For multi-class classification, four independent models are trained to classify malicious traffic into single attack categories such as DDoS, Probe, and DoS. The models vary based on the number of target classes (five or eight) and class imbalance handling (original or augmented datasets). To reduce data imbalance and enhance classification accuracy, Deep Convolutional Generative Adversarial Networks (DCGAN) are employed to generate synthetic samples for under-sampled attack classes. Performance comparison of the models decides the optimal configuration to deploy. Such models are employed on a virtual SDN testbed simulated using Mininet, where real-time packet emission is carried out using Hping3. Some hosts in the network are given the task of processing real-time traffic, forecasting anomalies, and carrying out dynamic routing. Traffic is routed to a secure path (if for benign data) or dropped in case it is detected as malicious according to the classification. This modular architecture facilitates adaptive, scalable, and low-latency intrusion detection across the SDN network. (Fig. 1) provides a schematic illustration of the system workflow of the suggested system.

3.1. Analysis Dataset

Three main types (CSV) have been merged, which consist of eight classes, seven of which are attacks and one is Normal. The number of attacks was 275465, while a normal was 68424. The dataset consists of 84 columns (83 Features and 1 Label). For the binary classification model, a label transformation was applied whereby all attack classes were encoded under a unified label (“1”), and normal traffic was labeled as (“0”), thereby converting the dataset into a binary format: attack vs. non-attack. This transformation was implemented during the preprocessing phase and is illustrated in Fig. 2, which shows the overall distribution of attack types after merging.

In Fig. 2, the overall distribution of network traffic is indicated after combining all classes of attacks into a single "attack" class while maintaining a separate "normal" class. This visual representation clearly indicates the large disparity between normal traffic and the aggregated attack samples.

According to research in classification of imbalanced data in [37, 38], can say that a class is Minority or Majority based on the percentage of the number of samples in each class compared to the total sample.

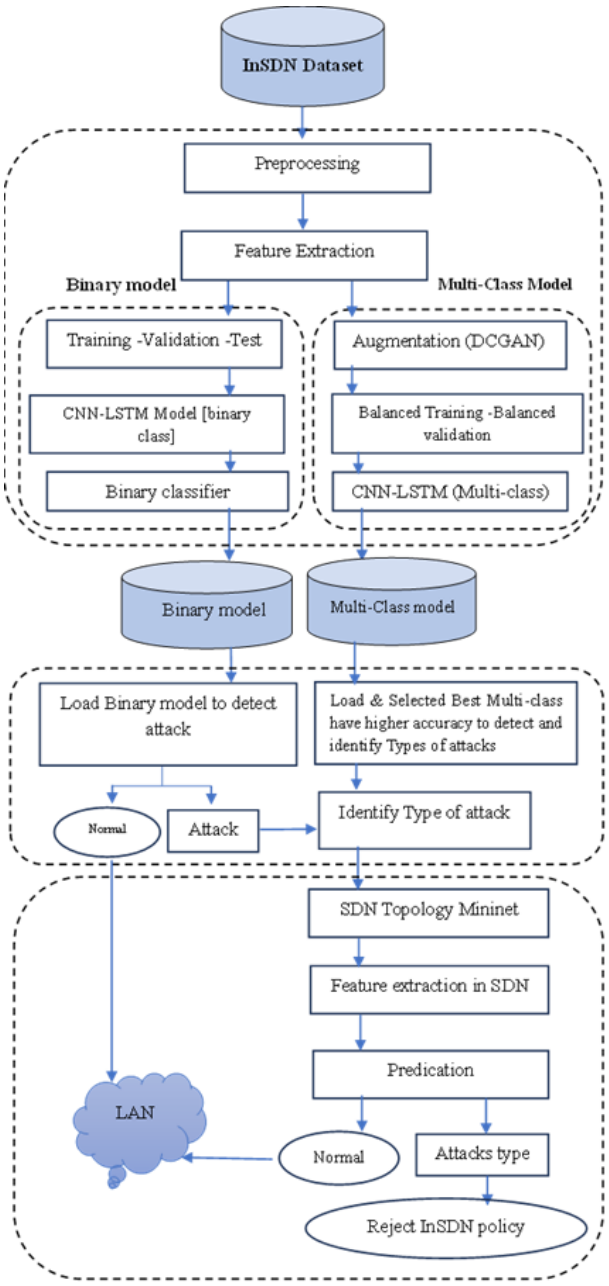

Fig. 1. System Flowchart of the Proposed IDS Framework

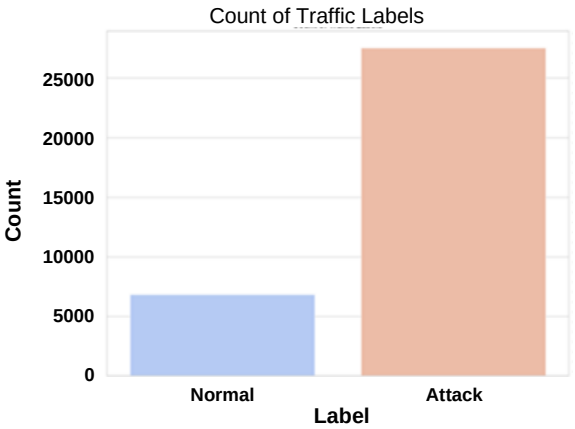

Fig. 2. Merge Attacks with Normal

If the class percentage is less than 15% (or a specific percentage considered a threshold in the study), it is considered a Minority Class. If the class percentage is greater than or equal to 15%, it is considered a Majority Class. For example, as shown in Table 2, classes such as DDoS (35.46%), Probe (28.53%), Normal (19.90%), and DoS (15.59%) exceed the 15% threshold and are thus classified as Majority Classes, whereas classes like BFA (0.41%), Web-Attack (0.056%), BOTNET (0.048%), and U2R (0.0049%) are classified as Minority Classes.

It is noted for this InSDN dataset that the separation rate between Minority and Majority was that samples greater than 15 percent as illustrated in Table 2 and (Fig. 3), were considered Majority and less were considered Minority.

Table 2 – *Percentage and types of attacks and normal from all samples*

Class	Account	Count Ratio	Percentage	Class Type
DDoS	121942	121942/343,889	35.46%	Majority
Probe	98129	98129/343,889	28.53%	Majority
Normal	68424	68424/343,889	19.90%	Majority
DoS	53616	53616/343,889	15.59%	Majority
BFA	1405	1405/343,889	0.41%	Minority
Web-Attack	192	192/343,889	0.056%	Minority
BOTNET	164	164/343,889	0.048%	Minority
U2R	17	17/343,889	0.0049%	Minority

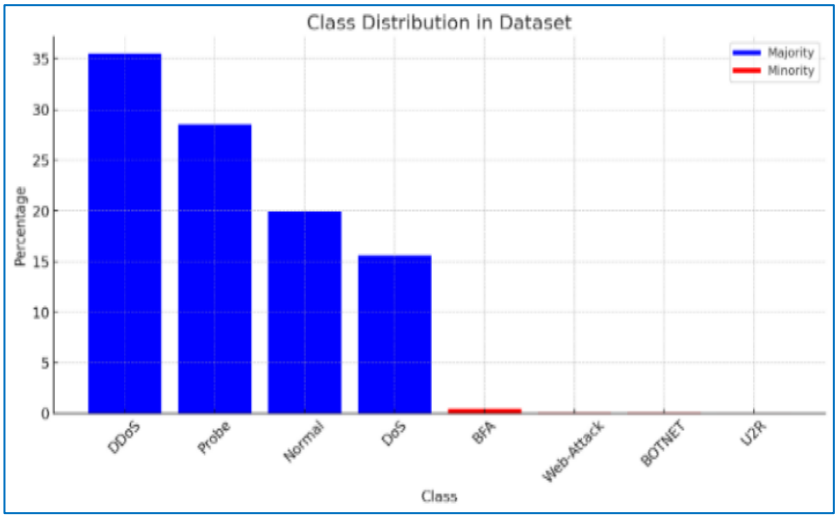

Fig. 3. Class distribution imbalance across categories

Recommendations for handling imbalance, according to this analysis, merging certain attacks is necessary to balance the dataset between majority and minority classes before further processing. Additionally, assigning higher weights to minority classes during model training ensures the model focuses on them, preventing poor performance.

3.2. DCGAN model

Deep Convolutional Generative Adversarial Networks (DCGAN) play a crucial role during generating synthetic samples to balance imbalanced datasets, particularly for minority attack classes like BFA, Web-Attack, U2R, and BOTNET. The DCGAN architecture consists of a generator and multiple discriminators (including dense, Conv1D, and GRU-based models) that compete to improve synthetic data quality. The generator creates realistic synthetic samples from random noise, while the discriminators distinguish between real and generated data. By training adversarially, the DCGAN enhances the minority class representation and classification performance for rare attack types.

3.3. Binary and multi-classes models

These models combine Convolutional Neural Networks (CNNs) to extract spatial features with Long Short-Term Memory (LSTM) networks to capture temporal dependencies in binary and multi-class classification.

The binary model's mechanism combines all attack types into a single class known as the "abnormal" class which enables the model to classify the traffic into normal and attack traffic as illustrate in Fig. 2. The data was preprocessed ahead of model training, such as feature extraction, target correlation testing, and normalization. The data is finally split for training and testing, with hyperparameter tuning on top. The details regarding architecture and results of the binary classification model are provided in the following sections. In the multi-class classification approach, four distinct models are implemented and evaluated. The best- performing model is subsequently selected and deployed on an SDN emulator for intrusion detection, as illustrated below.

3.3.1. Model 1: 8 Classes – No Augmentation or Balancing. This model preserves all eight original classes without merging any minority classes, maintaining the original distribution. It utilizes the same architecture and preprocessing as binary class (Model 1), with input dimensions of (240,721, 72, 1) for the training and (34,046, 72, 1) for testing. Although no balancing methods have been implemented, which creates an unbalanced dataset. Regardless of this, the architecture of the CNN-LSTM hybrid network remains the same and continues to classify sequential data.

3.3.2. Model 2: 5 Classes – No Balancing. The second model has 5 classes without balance. This model employs the same preprocessing procedures as the first model, but it merges four minority classes into one to create five classes with dimensions of the input data that are changed to (34,046, 72, 1) for testing and (240,722, 72, 1) for training. The CNN-LSTM architecture, optimized for sequential input data, is employed for multi-class classification. With layers and parameters described in the model overview, the model structure is made to manage five output types. It maintains sequential learning capabilities, data division, and normalization for efficient classification

3.3.3. Model 3: 8 Classes – Balanced with DCGAN. To address class imbalance in the initial 8-class dataset, Model 3 employs a Deep Convolutional Generative Adversarial Network (DCGAN) to synthesize realistic 1D sequences for underrepresented classes. The DCGAN architecture comprises a generator and a discriminator, both leveraging Conv1D, Gated Recurrent Unit (GRU), and fully connected layers for effective adversarial training.

For classification, a hybrid CNN-LSTM model is implemented, consisting of two Conv1D layers (with 256 and 128 filters, respectively) for spatial feature extraction, followed by an LSTM layer (128 units) to capture temporal dependencies. The model concludes with dense classification layers using ReLU activation and SoftMax output. Training is conducted using the Adam optimizer, with performance evaluated through key metrics, including area under the curve (AUC), accuracy, precision, and recall. This approach enhances class balance via data augmentation while simultaneously learning discriminative spatial and temporal patterns.

3.3.4. Model 4: 5 Classes – Balanced with DCGAN. To mitigate class imbalance after consolidating attack categories into five distinct classes, Model 4 employs a DCGAN-based synthetic data augmentation framework to address class imbalance by generating synthetic samples for minority attack classes (BFA, Web-Attack, U2R, BOTNET) . Categorical labels are first transformed into numeric representations via label encoding. The final balanced dataset (X_resample, Y_resample) is constructed by combining original samples with DCGAN-generated synthetic sequences.

The proposed CNN-LSTM architecture comprises two Conv1D layers (256 and 128 filters, respectively) for spatial feature extraction, followed by a 128-unit LSTM layer to model temporal dependencies. The classification module consists of dense layers with ReLU activation and a SoftMax output. To enhance training stability and generalization, the model integrates dropout regularization, batch normalization, and max-pooling layers.

Comparative evaluations demonstrate that Model4 achieves superior performance in multi-class classification scenarios, outperforming alternative approaches in terms of robustness and discriminative capability.

3.4. Implementation (CNN-LSTM models) in SDN emulator topology

To evaluate the proposed intrusion detection system in a test environment, a Software-Defined Networking (SDN) topology is implemented using the Mininet emulator. The topology consists of multiple hosts (e.g., Host 1 to Host 8) that interact by generating and transmitting network traffic. One host (e.g., Host 2) is designated for real-time traffic monitoring and attack prediction. Detection begins with a binary CNN-LSTM

model, which classifies incoming packets as either normal or anomalous. If traffic is identified as malicious, a secondary multi-class CNN-LSTM model determines the specific attack type. This hierarchical architecture enables efficient and accurate threat detection.

Based on the classification result, legitimate traffic is routed to an Accept Area, while malicious traffic is redirected to a Reject Area. These real-time decisions are enforced through SDN controller policies, enhancing network responsiveness and security. The deployment framework and SDN topology are illustrated in Fig. 4 and Fig. 5).

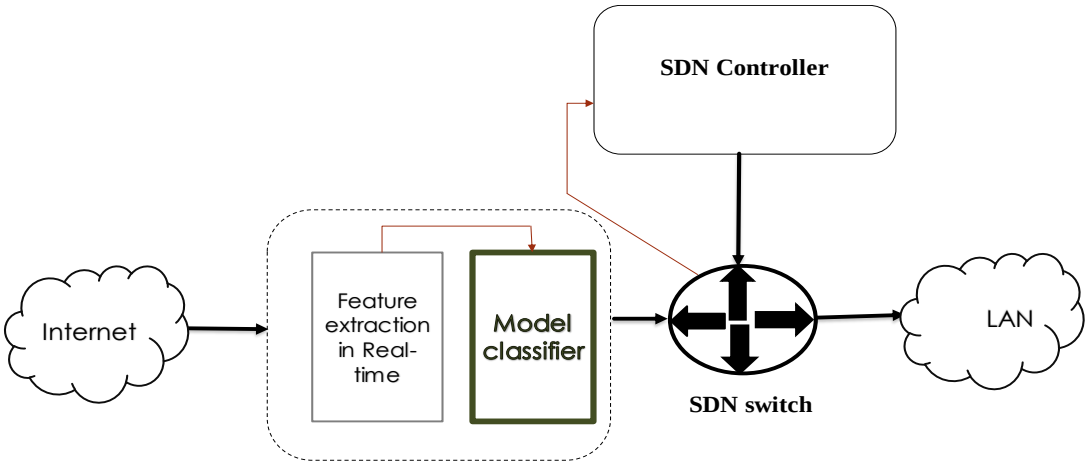

Fig. 4. Implementing Model Classifier Detection attacks on SDN Emulator

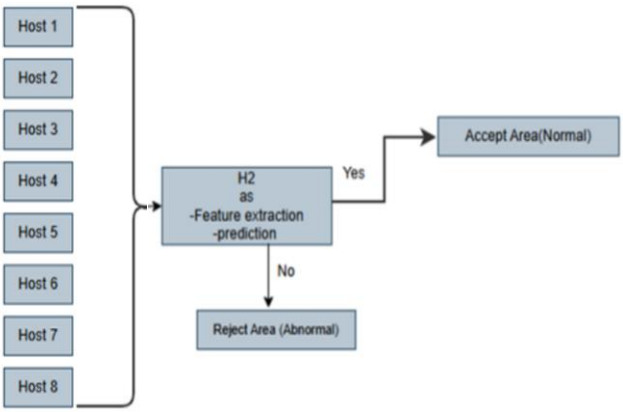

Fig. 5. Mininet Network Topology of proposed system

4. Result

The correlation analysis feature was conducted to identify features with the strongest association to the Label (Fig. 6) illustrates both the highest and lowest correlation values observed. By applying a threshold of (< –0.01), we eliminated 11 statistically insignificant features through the implemented code, thereby optimizing the feature set for binary class model performance.

The extracted features were processed for the binary classification model as illustrated in Fig. 6. As part of preprocessing, normalization was performed using Robust Scaler to constrain the large feature values within a (-1, 1) range, improving numerical stability.

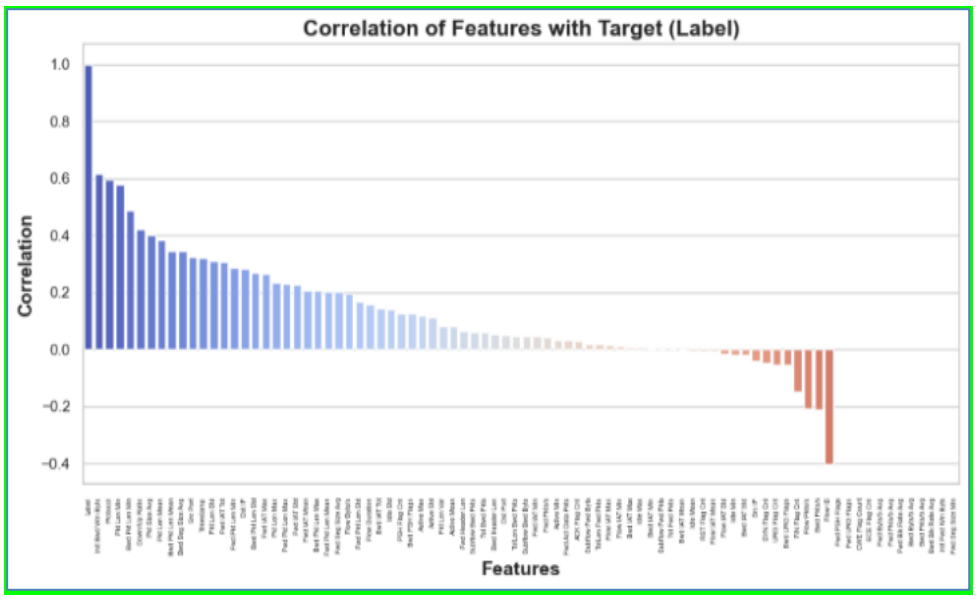

Fig. 6. Correlation of feature with label

To validate this approach, we implemented a dedicated binary classification model with data partitioned into training, validation, and testing sets. Following the application of macro and micro evaluation measures, the model was trained using these processed features. The resulting performance metrics are presented in Table 3.

Table 3 – **Binary model metrics with (Macro, Micro)**

	Metric of system	Macro	Micro
Accuracy	99.813	99.81	99.81
Precision	99.814	99.62	99.81
Recall	99.813	99.80	99.81
F1-Score	99.813	99.71	99.81

The close alignment between micro-average and accuracy metrics indicates that dataset imbalance did not significantly impact the model's attack detection capability.

Discrepancies between these metrics would suggest model deficiencies. (Fig. 7) illustrates the training and validation loss across 10 epochs, demonstrating model convergence.

Furthermore, (Fig. 8) presents the binary classifier's performance metrics, while (Fig. 9) displays the confusion matrix, confirming the model's effectiveness in distinguishing normal from attack traffic with high precision and minimal misclassification errors.

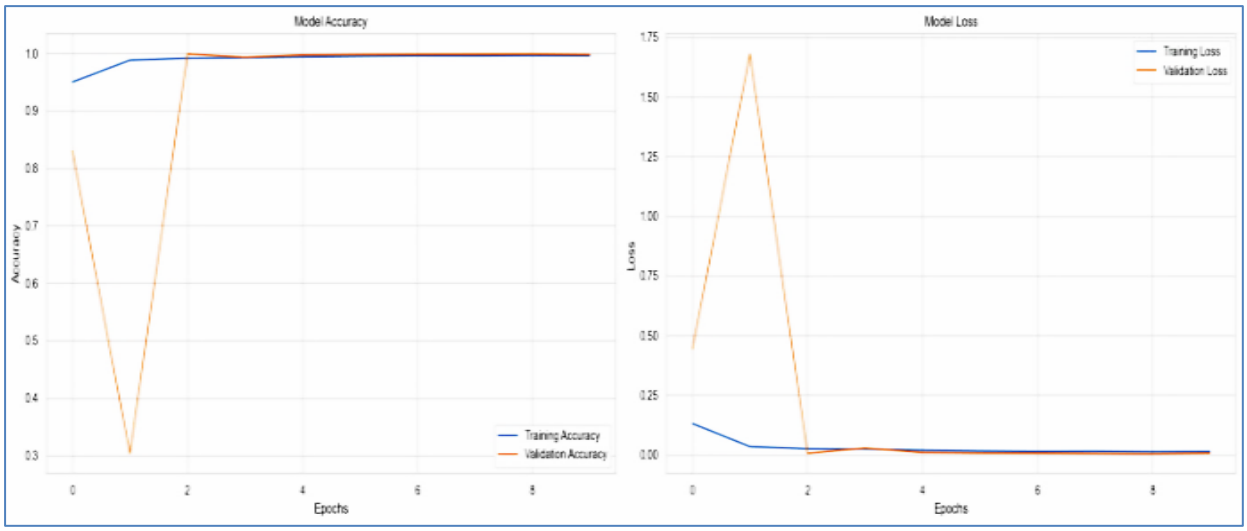

Fig. 7. Train Loss and Validation Loss versus the number of epochs

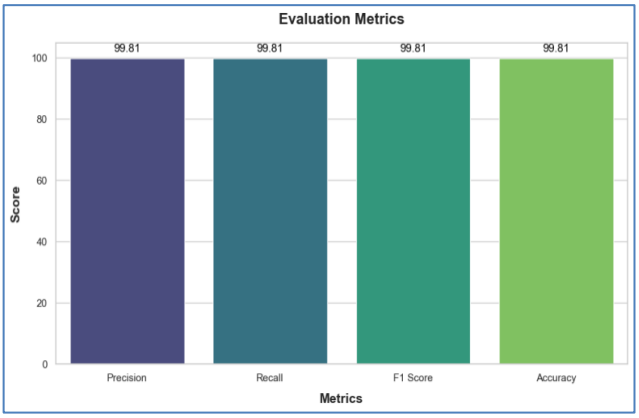

Fig. 8. Model evaluation Metrics

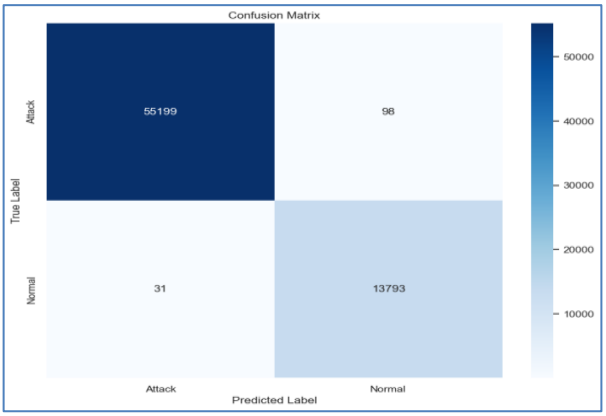

Fig. 9. Confusion Matrix-binary class

In addition, the development of a multi-class classification model for the InSDN dataset encompasses multiple critical stages: data analysis, preprocessing, model selection, training, and comprehensive evaluation. (Fig. 10–12) presents the correlation analysis between the top 10 selected features and target labels, highlighting the most discriminative features employed in model training. This structured approach ensures robust model development and interpretable feature selection.

The implementation of all models in the proposed system yielded varying performance outcomes. By integrating CNN and LSTM architectures across different class configurations, we obtained the results presented in Table 4. The comprehensive evaluation metrics include.

The comparative analysis reveals significant performance variations across models. Model 1 demonstrates moderate accuracy (65.96%) with notable divergence between macro and micro metrics (F1-score: 63.15% macro vs 65.97% micro), indicating class imbalance effects. Model 2 achieves exceptional accuracy (99.68%) yet shows similar metric discrepancies (F1-score: 99.67% vs 99.68% macro), suggesting potential overfitting despite high performance. Model 3 performs poorest (53.45% accuracy) with substantial metric variations (F1-score: 44.55% vs 53.45% macro), rendering it unreliable.

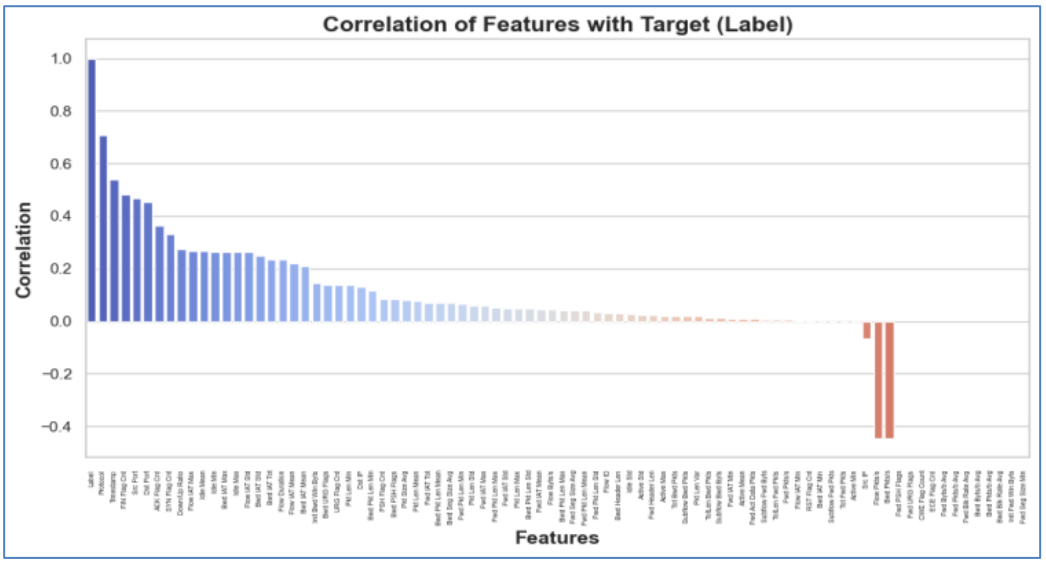

Fig. 10. Correlation of features with label

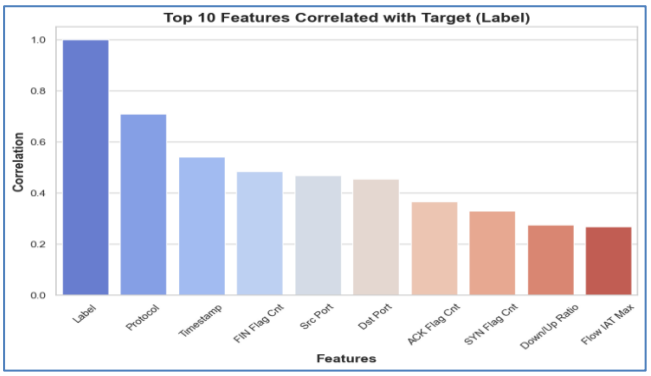

Fig. 11. Ten features correlation with label

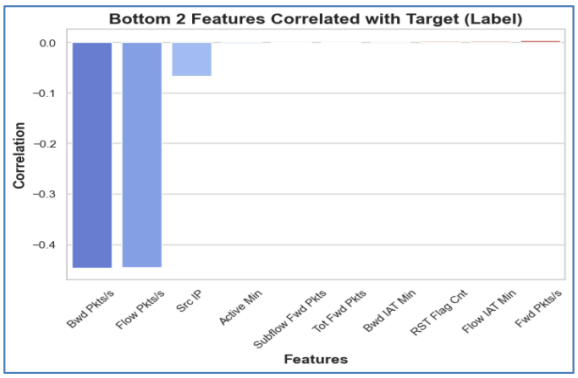

Fig.12. Two features correlation with label

Table 4 – **Comparative Performance Analysis of Proposed Multi class Models**

	Average			Average			Average			Average		
Models	ACC	Macro	Micro	P	Macro	Micro	R	Macro	Micro	F1	Macro	Micro
Model 1	65.96	65.97	65.97	77.96	38.66	65.97	65.96	31.53	65.97	63.15	29.27	65.97
Model 2	99.68	99.68	99.81	99.67	99.2	99.68	99.68	95.35	99.68	99.67	97.05	99.68
Model 3	53.45	53.45	53.45	45.7	37.65	53.45	53.45	39.96	53.45	44.55	35.52	53.45
Model 4	99.45	99.45	99.45	99.45	99.42	99.45	99.45	99.31	99.45	99.44	99.36	99.45

Model 4 emerges as optimal, achieving near-perfect accuracy (99.45%) with minimal metric divergence (F1-score: 99.44% vs 99.45% macro) in Fig. 14.

The DCGAN-augmented balanced dataset enables robust performance across all classes, evidenced by converging macro and micro metrics. The confusion matrix confirms in Fig. 15 the model's efficacy, demonstrating precise classification with minimal errors in Fig. 13. These results establish Model 4 as the most dependable solution for network threat identification.

The employ Model 4 was deploying in an SDN environment, leveraging its superior performance (99.45% accuracy, 99.44% F1-score) as demonstrated in prior evaluations.

The experimental framework implemented a Mininet-emulated topology comprising eight nodes (seven generating diverse attack vectors - including DoS, DDOS and Probe and one normal traffic source), with one node designated for real-time packet analysis using the hybrid detection system.

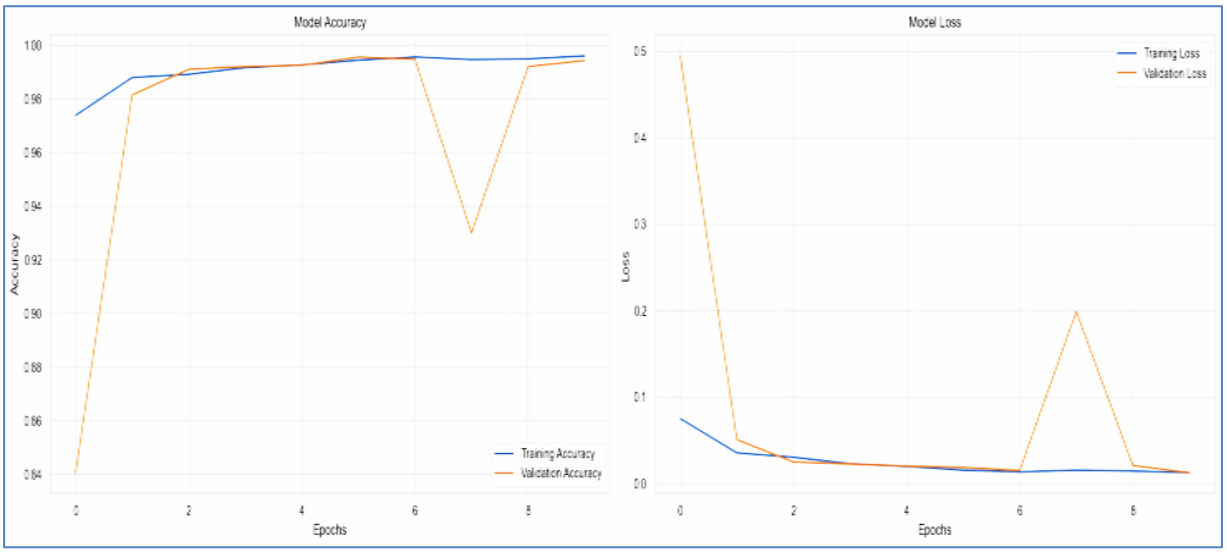

Fig. 13. Train Loss and Validation Loss versus the number of epochs in model 4

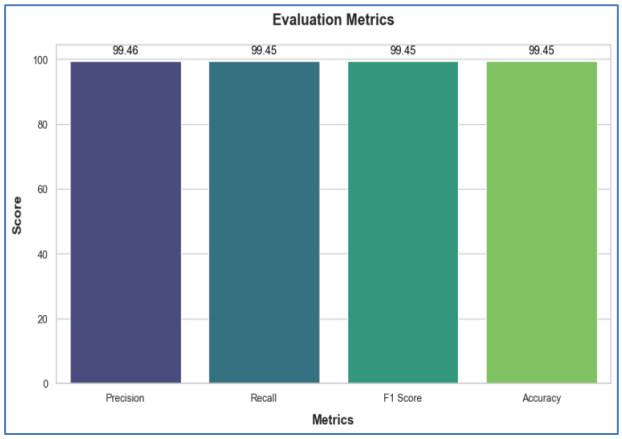

Fig. 14. Evaluation Metrics-model4

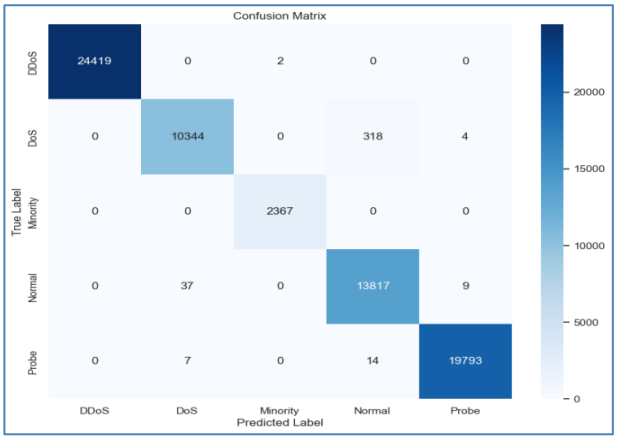

Fig. 15. Confusion Matrix-model4

As evidenced in (Fig. 16 and 17), the model's binary classification layer achieved 99.68% attack detection accuracy, while the multi-class component maintained 99.45% precision in attack-type identification. This dual-stage architecture, combined with SDN's programmable flow control, enabled both high-accuracy threat detection and automatic traffic mitigation.

The SDN controller dynamically enforces security measures based on model predictions, including malicious traffic blocking and suspicious packet rerouting.

Table 5 presents a comprehensive comparison with existing approaches and analyzing key aspects including types of datasets, methodology, performance metrics.

Table 5 – **Comparison proposed systems**

Authors	Algorithm	Dataset	Accuracy	Precision	Recall	F1-Score
J AHANZAIB el at. [13]	Cu (LSTM-CNN)	CICIDS2017	98.6	99.37	99.35	99.35
Mahmoud el at. [14]	CNN-SoftMax (SD-Reg) Binary class	InSDN	97.47%	97.15	94.39	95.65
	Multi class	InSDN	97.37%	92.96	88.54	89.1
Mohammad el at. [15]	CNN-LSTM	Bot-IoT	99.99%	98.50%	99.00%	98.70%
Thura &Nadia [17]	CNN-LSTM	Mendeley datasets	99.9%	-	-	-
Proposed model	CNN-LSTM Binary class	InSDN	99.81	99.81	99.81	99.81
Proposed model	CNN-LSTM Multi class	InSDN	99.4	99.45	99.45	99.44

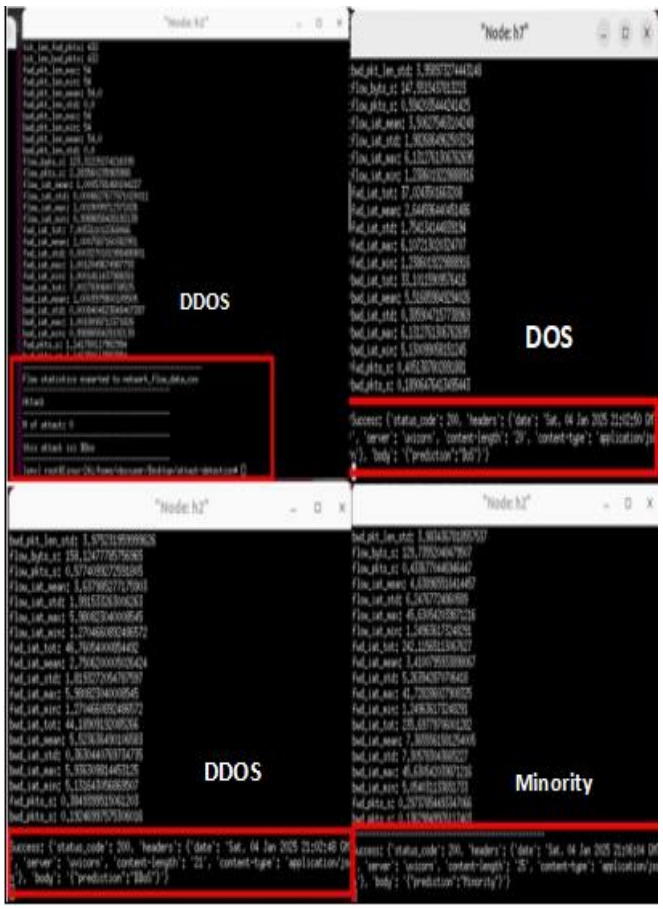

Fig. 16. Shown some attacks generate in SDN emulator

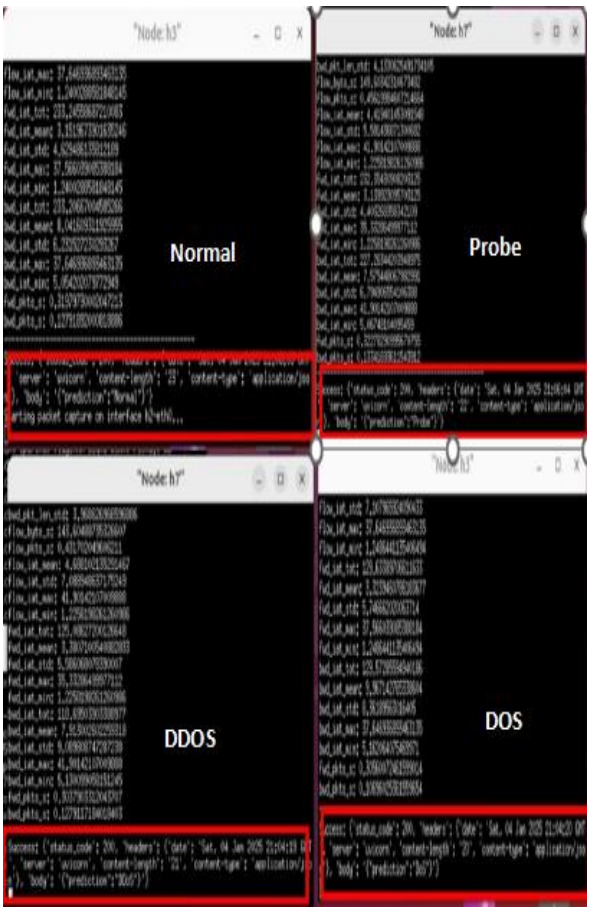

Fig. 17. Attacks generate in SDN emulator

While existing studies have applied deep learning and machine learning to SDN intrusion detection, their accuracy remains insufficient for practical implementation. This study focuses on developing a real-time deep learning approach for vulnerability detection in SDN emulators, aiming to achieve superior performance metrics. The proposed method introduces three keys innovations: A hybrid CNN-LSTM model architecture, a real-time SDN emulator for attack detection and DCGAN-based dataset balancing. The model's performance depends on dataset characteristics (balanced/imbalanced, class composition) and training hyperparameters.

Notably, different datasets exhibit varying behaviors, even when using the same benchmark dataset (InSDN), leading to divergent metrics across studies.

Conclusion and Future work

This paper proposed a real-time intrusion detection system in Software-Defined Networking (SDN) using a hybrid deep learning model of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The system trains binary and multi-class classifiers using the InSDN dataset, and data imbalance is addressed with Deep Convolutional Generative Adversarial Networks (DCGAN). Experimental results demonstrated that the binary classifier achieved a 99.81% accuracy, while the best multi-class model achieved 99.4%, confirming the effectiveness of the combined CNN-LSTM approach using data augmentation.

The system was implemented in a test SDN network with Mininet and Hping3 to test its real-time detection capability. The architecture performed well in detecting various types of attacks with low latency and was able to classify malicious traffic and enforce SDN policies dynamically.

For future work, the system may be made larger to accommodate larger SDN topologies for testing scalability and performance on more real-world network setups. Additionally, implementing the system in real-world situations outside the emulator will provide better insight into its survivability. Future work can also include adding online learning mechanisms and improving the model's ability to learn and adapt to evolving attack patterns in dynamic networks.

References

1. Shafiq, S., Rahman, M. S., Shaon, S. A., Mahmud, I. and Hosen, A. S. M. S. (2024), “A Review on Software-Defined Networking for Internet of Things Inclusive of Distributed Computing, Blockchain, and Mobile Network Technology: Basics, Trends, Challenges, and Future Research Potentials,” *International Journal of Distributed Sensor Networks*, vol. 2024, doi: https://doi.org/10.1155/2024/9006405
2. Khongbuh, W. and Saha, G. (2024), “A Survey for Software-Defined Networking (SDN) Enabled Internet of Things (IoT) Networks”, *Science and Technology Journal*, vol. 12, no. 1, pp. 77–88, doi: https://doi.org/10.22232/stj.2024.12.01.10

3. Domeke, A., Cimoli, B. and Monroy, I. T. (2022), "Integration of network slicing and machine learning into edge networks for low-latency services in 5G and beyond systems", *Applied Sciences*, vol. 12, no. 13, doi: https://doi.org/10.3390/app12136617
4. Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A. and Flinck, H. (2018), "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions", *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, doi: https://doi.org/10.1109/COMST.2018.2815638
5. Acquah, D. K., Sowah, R. A. and Togo, E. T. (2024), "Network Intrusion Detection and Prevention System Using Hybrid Machine Learning Techniques", *Security and Privacy*, vol. 2024, art. id. 5775671, doi: https://doi.org/10.1155/2024/5775671
6. Mhamdi, L. and Isa, M. M. (2024), "Securing SDN: Hybrid autoencoder-random forest for intrusion detection and attack mitigation", *Journal of Network and Computer Applications*, vol. 225, no. 103868, doi: https://doi.org/10.1016/j.jnca.2024.103868
7. Abdallah, M., An Le Khac, N., Jahromi, H. and Delia Jurcut, A. (2021), "A hybrid CNN-LSTM based approach for anomaly detection systems in SDNs", *The 16th International Conference on Availability, Reliability and Security*, doi: https://doi.org/10.1145/3465481.3469190
8. Alanazi, F., Jambi, K., Eassa, F., Khemakhem, M., Basuhail, A. and Alsubhi, K. (2022), "Ensemble deep learning models for mitigating DDoS attack in software-defined network", *Intell. Autom. Soft Comput.*, vol. 33, no. 2, pp. 923–938, doi: https://doi.org/10.32604/iasc.2022.024668
9. Alasadi, H. S., Farzinvash, L., Mortazavi, S. A. and Feizi-Derakhshi, M.-R. (2024), "Enhancing Data Collection in Heterogenous Wireless Sensor Networks: A Novel Tree-Structured Genetic Algorithm Approach", *IEEE Access*, vol. 12, doi: https://doi.org/10.1109/ACCESS.2024.3502458
10. Iraji, M., Tanha, J., Balafar, M.-A. and Feizi Derakhshi, M. R. (2024), "A novel interpolation consistency for bad generative adversarial networks (IC-BGAN)", *Multimedia Tools Appl*, vol. 83, no. 38, pp. 86161–86205, doi: https://doi.org/10.1007/s11042-024-20333-5
11. Ketkar, N. and Moolayil, J. (2021), *Deep learning with python: Learn Best Practices of Deep Learning Models with PyTorch*, Apress Media LLC, 306 p., doi: https://doi.org/10.1007/978-1-4842-5364-9
12. Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M. and Ahmad, R. (2022), "CNN-LSTM: Hybrid deep neural network for network intrusion detection system", *IEEE Access*, vol. 10, pp. 99837–99849, doi: https://doi.org/10.1109/ACCESS.2022.3206425
13. Oyucu, S., Polat, O., Türkoğlu, M., Polat, H., Aksöz, A. and Ağdaş, M. T. (2023), "Ensemble Learning framework for DDoS detection in SDN-based SCADA systems", *Sensors* (Basel, Switzerland), vol. 24, no. 1, doi: https://doi.org/10.3390/s24010155
14. Zulu, L. L., Ogudo, K. A. and Umenne, P. O. (2018), "Simulating software defined networking using mininet to optimize host communication in a realistic programmable network," *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems* (icABCD), pp. 1–6, doi: https://doi.org/10.1109/ICABCD.2018.8465433
15. Malik, J., Akhunzada, A., Bibi, I., Imran, M., Musaddiq, A. and Kim, S. W. (2020), "Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN", *IEEE Access*, vol. 8, pp. 134695–134706, doi: https://doi.org/10.1109/ACCESS.2020.3009849
16. ElSayed, M. S., Le-Khac, N. A., Albahar, M. A. and Jurcut, A. (2021), "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique", *Journal of Network and Computer Applications*, vol. 191, doi: https://doi.org/10.1016/j.jnca.2021.103160
17. Shahin, M., Chen, F. F., Bouzary, H., Hosseinzadeh, A. and Rashidifar, R. (2022), "A Novel Fully Convolutional Neural Network Approach For Detection and Classification of Attacks on Industrial IoT Devices in Smart Manufacturing Systems", doi: https://doi.org/10.21203/rs.3.rs-1739779/v1
18. Ahmed, N., Ngadi, A. b., Sharif, J. M., Hussain, S., Uddin, M., Rathore, M. S., Iqbal, J., Abdelhaq, M., Alsaqour, R., Ullah, S. S. and Zuhra, F. T. (2022), "Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction", *Sensors* (Basel, Switzerland), vol. 22, no. 20, pp. 7896, doi: https://doi.org/10.3390/s22207896
19. Shahryari, M.-S., Farzinvash, L., Mohammad-Khanli, L., Ramezani, M. and Feizi-Derakhshi, M.-R. (2023), "Nesting Circles: An Interactive Visualization Paradigm for Network Intrusion Detection System Alerts", *Secur Commun Netw*, vol. 2023, doi: https://doi.org/10.1155/2023/5513227
20. Khaleel, T. J. and Shiltagh, N. A. (2023), "DDOS ATTACK DETECTION USING HYBRID (CCN AND LSTM) ML MODEL", *Int J Comput Inf*, vol. 11, no. 1, pp. 1–10, doi: https://doi.org/10.25195/ijci.v49i2.446
21. Jyothsna, V., Sandhya, E., Swetha, T., Lokesh Kumar Reddy, P., Jyothsna, B. and Bhasha, P. (2023), "Deep Learning Model for Intrusion Detection in SDN Networks", *2023 1st International Conference on Optimization Techniques for Learning*, ICOTL 2023 - Proceedings, Institute of Electrical and Electronics Engineers Inc., doi: https://doi.org/10.1109/ICOTL59758.2023.10435198
22. Kandhro, I. A., Alanazi, S. M., Fatima, K., Uddin, M., Ali, F., Kehar, A. and Karuppayah, S. (2023), "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures", *IEEE Access*, vol. 11, pp. 9136–9148, doi: https://doi.org/10.1109/ACCESS.2023.3238664
23. Aleem, S. and Ahmed, S. (2023), "Network Security and Communication Unlocking Network Security and QoS: The Fusion of SDN, IoT, and Machine Learning: A Comprehensive Analysis", *Int J Sci Res Netw Secur Commun*, vol. 3, no. 2, pp. 1–15, doi: https://doi.org/10.5281/zenodo.1234567
24. Kaur, G. and Kaur, M. (2023), "Enhanced Security Framework for Modern Network Architectures: Integrating AI-Driven Threat Detection and Prevention Mechanisms", *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 3, pp. 45–58, doi: https://doi.org/10.14569/IJACSA.2023.0140306
25. Samaan, S. S. and Jeiad, H. A. (2023), "Feature-based real-time distributed denial of service detection in SDN using machine learning and Spark", *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2302–2312, doi: https://doi.org/10.11591/eei.v12i4.4711
26. Rui, K., Pan, H. and Shu, S. (2023), "Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques", *Sci Rep*, vol. 13, no. 1, doi: https://doi.org/10.1038/s41598-023-44764-6

27. Maddu, M. and Rao, Y. N. (2024), “Network intrusion detection and mitigation in SDN using deep learning models”, *Int J Inf Secur*, vol. 23, no. 2, pp. 849–862, doi: https://doi.org/10.1007/s10207-023-00771-2
28. Racherla, S., Sripathi, P., Faruqui, N., Alamgir Kabir, M., Whaiduzzaman, M. and Aziz Shah, S. (2024), “Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning”, *IEEE Access*, vol. 12, pp. 63584–63597, doi: https://doi.org/10.1109/ACCESS.2024.3396461
29. Alashhab, A. A., Isyaku, B., Zahid, M. S., Abaselnour, A., Nagmeldin, W. A., Abdelmaboud, A., Abdullah, T. A. A. and Maiwada, U. D. (2024), “Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model”, *IEEE Access*, vol. 12, pp. 51630–51649, doi: https://doi.org/10.1109/ACCESS.2024.3384398
30. Arthi, R., Krishnaveni, S. and Zeadally, S. (2024), “An intelligent SDN-IoT enabled intrusion detection system for healthcare systems using a hybrid deep learning and machine learning approach”, *China Communications*, doi: https://doi.org/10.23919/JCC.ja.2022-0681
31. Ghadermazi, J., Shah, A. and Bastian, N. D. (2024), “Towards Real-time Network Intrusion Detection with Image-based Sequential Packets Representation”, *IEEE Trans Big Data*, doi: https://doi.org/10.1109/TBDATA.2024.3403394
32. Musa, N. S., Mirza, N. M., Rafique, S. H., Abdallah, A. M. and Murugan, T. (2024), “Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks - Current Research Solutions”, *IEEE Access*, vol. 12, pp. 17982–18011, doi: https://doi.org/10.1109/ACCESS.2024.3360868
33. Rustam, F., Raza, A., Qasim, M., Posa, S. K. and Jurcut, A. D. (2024), “A Novel Approach for Real-Time Server-Based Attack Detection Using Meta-Learning”, *IEEE Access*, vol. 12, pp. 39614–39627, doi: https://doi.org/10.1109/ACCESS.2024.3375878
34. Hirsi, A., Audah, L., Salh, A., Alhartomi, M. A. and Ahmed, S. (2024), “Detecting DDoS Threats using Supervised Machine Learning for Traffic Classification in Software Defined Networking”, *IEEE Access*, doi: https://doi.org/10.1109/ACCESS.2024.3486034
35. Ebrahimzadeh, F., Nazari, A., Feizi-derakhshi, M. R. and Mansoorizadeh, M. (2023), “A Hybrid Recurrent Neural Network Approach for Detecting Abnormal User Behavior in Social Networks,” doi: https://doi.org/10.21203/rs.3.rs-3242416/v1
36. Elsayed, M. S., Le-Khac, N. A. and Jurcut, A. D. (2020), “InSDN: A novel SDN intrusion dataset,” *IEEE Access*, vol. 8, pp. 165263–165284, doi: https://doi.org/10.1109/ACCESS.2020.3022633
37. Koziarski, M. (2020), “Radial-Based Under sampling for imbalanced data classification”, *Pattern Recognit*, vol. 102, 107262, doi: https://doi.org/10.1016/j.patcog.2020.107262
38. Christopher, V., Aathman, T., Mahendrakumaran, K., Nawaratne, R., De Silva, D. and Alahakoon, D. (2021), “Minority Resampling Boosted Unsupervised Learning with Hyperdimensional Computing for Threat Detection at the Edge of Internet of Things”, *IEEE Access*, vol. 9, pp. 126646–126657, doi: https://doi.org/10.1109/ACCESS.2021.3111053

.

Received (Надійшла) 23.06.2025
Accepted for publication (Прийнята до друку) 27.08.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Фейзі-Дерахші Мохаммад-Реза – доктор філософії (штучний інтелект), професор штучного інтелекту, лабораторія систем комп'ютерного інтелекту, кафедра комп'ютерної інженерії, університет Тебриза, Тебриз, Іран; Урукський університет, Багдад, Ірак;
Mohammad-Reza Feizi-Derakhshi – Ph.D (artificial intelligence), Full Professor of Artificial Intelligence, Computerized Intelligence Systems Laboratory, Department of Computer Engineering, University of Tabriz, Tabriz, Iran; Uruk University, Baghdad, Iraq;
e-mail: mfeizi@tabrizu.ac.ir; ORCID ID: https://orcid.org/0000-0002-8548-976X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=35748449200.

Муташар Аль-Талебей Ватек Ганім – магістр комп'ютерних наук, аспірант (штучний інтелект), університет Тебриза, Тебриз, Іран;
Watheq Ghanim Mutasher AL-Talebei – M.Sc. in Computer Science, Ph.D. student in Artificial Intelligence, University of Tabriz, Tabriz, Iran;
e-mail: watheq.ghanim@tabrizu.ac.ir; ORCID ID: https://orcid.org/0000-0001-6789-1301;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57453938500.

Балансування даних DCGAN для покращення точності гібридної CNN-LSTM системи виявлення вторгнень у середовищі SDN

Мохаммад-Реза Фейзі-Дерахші, Ватек Ганім Муташар Аль-Талебей

Анотація. Підтримання надійної мережевої безпеки в системах із програмно-визначеними мережами (SDN) стає все більш складним через складні кібератаки та централізовану природу SDN. **Ця робота** представляє нову систему виявлення вторгнень на основі гібридної моделі глибокого навчання, яка поєднує згорткові нейронні мережі (CNN) для виділення просторових ознак та мережі довгої короткочасної пам’яті (LSTM) для виділення часових залежностей. **Підхід застосовано** до великого набору даних InSDN, що містить маркований трафік для звичайної активності та різних класів атак, для навчання як багатокласових, так і бінарних класифікаторів. Синтетичні зразки генеруються на основі глибоких згорткових генеративних змагальних мереж (DCGAN) для ефективного вирішення проблем через дисбаланс класів і, таким чином, підвищення рівня виявлення для менших класів атак. **Експериментальні тести**, проведені в імітованій SDN мережі з Mininet та Hping3, демонструють видатну продуктивність: бінарна модель досягає 99.81% точності, а оптимальна багатокласова модель — 99.4% точності. **Такі перспективні** результати демонструють здатність запропонованої рамки запропонувати ефективне та масштабоване рішення для виявлення вторгнень у реальному часі для сучасних SDN інфраструктур.

Ключові слова: програмно-визначені мережі (SDN); атаки; CNN; LSTM; DCGAN; Mininet.