HCL: A Hybrid CNN-LSTM Framework for Intrusion Detection in SDN-IoT Networks

Ankit Chouhan, Nashid Shahriar, and JingTao Yao
Department of Computer Science
University of Regina, Regina, SK S4S 0A2, Canada
{ankit.chouhan, nashid.shahriar, jingtao.yao}@uregina.ca

***Abstract*—The seamless integration of Software-Defined Networking within Internet of Things (IoT) infrastructures has introduced novel paradigms for efficient network resource management. Nevertheless, this integration has also exposure to various cyber threats. Addressing these threats necessitates advanced detection mechanisms capable of adapting to the dynamic security needs. This paper introduces a Hybrid CNN LSTM (HCL) deep learning-based framework, which integrates hybrid Convolutional Neural Networks and Long Short-Term Memory networks to enhance intrusion detection in SDN-IoT networks. The performance analysis, conducted using real-world SDN datasets, attests to the framework's efficiency, exhibiting a high detection accuracy and less inference time, ensuring reliable security measures without compromising network performance. The HCL framework demonstrates above 90% accuracy in differentiating between benign and malicious traffic, with a particular focus on detecting DoS, DDoS, port scanning, and fuzzing attacks. Additionally, the framework's scalability aligns seamlessly with varying number of devices, maintaining strong defense across diverse network topologies. These results demonstrate the framework's effectiveness in defending against modern cyber threats in SDN-IoT networks.**

***Index Terms*—SDN, IoT, Deep learning, CNN, LSTM, Security**

I. Introduction

The integration of the Internet of Things (IoT) with Software-Defined Networking (SDN) offers a transformative way to manage and optimize network resources efficiently [1]. SDN offers centralized network resource management, enabling efficient traffic monitoring and management [2]. However, this convergence of IoT and SDN networks introduces significant security challenges. The inherent vulnerabilities of IoT devices, combined with the dynamic nature of SDN, make these networks susceptible to various cyber threats [3]. The number of attacks on IoT devices is increasing, with reports showing over 100 million detected in the first half of 2019. Network security firms have noticed a surge in attack attempts [4]. During the 2020 global pandemic, DDoS attacks spiked, with projections indicating more complex and frequent attacks [5].

In response to these security challenges, intrusion detection systems (IDS) are essential for protecting SDN-based IoT networks [6]. By monitoring network traffic and detecting anomalies, IDS can identify and mitigate attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), port scanning, fuzzing, and OS vulnerabilities [7], [8]. However, traditional IDS often struggle with the rapidly evolving cyber threats, particularly in dynamic SDN-IoT environments [9]. The centralized control of SDN improves anomaly detection by using comprehensive network data and advanced algorithms [10].

Machine learning (ML) has become essential in cybersecurity, especially in intrusion detection and threat analysis [4]. When integrated into Software-Defined Internet of Things environments, ML enhances the detection and mitigation of security challenges. It uses algorithms like SVM, Naive Bayes, and Decision Trees to identify patterns indicative of attacks [11]. Advancing into the subset of ML, Deep Learning (DL) techniques like Convolutional Neural Networks (CNN) and Recurrent Neural Networks, including Long Short-Term Memory (LSTM) networks, have significantly handle complex security issues [12]. DL models focus on data, layer by layer, to learn from patterns. While CNNs useful in image and language processing by capturing spatial relationships, they sometimes fall short in network security because they focus on spatial characteristics rather than temporal ones [2]. For sequential and time-related data, which is in network traffic, LSTM networks are more preferable.

SDN-IoT networks can benefit from federated learning by enabling distributed model training across devices to improve privacy and scalability, though it introduces challenges such as communication overhead, device heterogeneity, and vulnerability to adversarial attacks [13], [14], while existing ML and DL solutions for DDoS detection and mitigation show promise but face limitations like scalability issues [2], [15], evolving attack types [16], multi-class classification challenges [15], and limited evaluation on real testbed SDN-IoT datasets [17]. To address these limitations, we propose a Hybrid CNN LSTM (HCL) framework, which combines CNN and LSTM models in a deep learning approach. The framework is applied to real-world datasets [18] generated from SDN and IoT environments. The HCL framework detects attacks like DoS, DDoS, port scanning, fuzzing, and OS vulnerabilities in SDN-IoT networks. It enhances security and ensures efficient network performance as cyber threats evolve.

II. Related Work

Various ML [4] and DL models have been proposed for detecting cyber attacks in SDN-IoT networks. DL [12], [15] models offers key advantages in cyber defense, helping researchers better understand emerging threats. The field of

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

attack detection and prevention remains important due to the potential damage attackers can cause [19], with recent studies focusing on ML and DL techniques to identify network attacks in SDN-IoT environments.

DL-based detection in SDN-IoT networks has emerged as a powerful approach to improving security. Elsayed et al. [15] proposed a secured automatic two-level IDS using an enhanced LSTM network to protect IoT and SDN networks. The system distinguished between benign and malicious traffic and categorized attacks, showing good accuracy on the ToN-IoT and InSDN datasets. However, the authors noted challenges with supervised learning at scale and LSTM's limitations in terms of training time and complexity, suggesting further research to improve efficiency and scalability. Chaganti et al. [2] proposed an LSTM-based IDS for IoT-SDN networks, achieving 97.1% accuracy on two datasets. The system outperformed traditional models and used t-SNE for feature visualization but faced challenges in real-world deployment due to high computational demands and data requirements.

Towhid and Shahriar [20] proposed a method for early intrusion detection in SDN using machine learning techniques. The author used flow-based features and shows that Random Forest performs better than LSTM in real-time detection scenarios with limited packet data. The challenges include performance reduction with fewer packets, class imbalance, managing computational requirements. Alashhab et al. [16] proposed a DL-based LSTM model to detect low-rate DDoS attacks in SDN-enabled IoT networks, addressing the difficulty of identifying these covert attacks. Tested on the Edge IIoTset dataset, the model achieved high accuracy normal traffic. However, the paper noted challenges in scaling the detection system for real-world applications.

The existing work highlights the potential of DL techniques to address the complex challenges of SDN-IoT network security, though challenges remain, such as high computational demands, multiclass classification difficulties, and scalability issues. Despite progress in detecting cyber attacks, continuous advancements are necessary due to evolving threats. To address these limitations, this paper introduces an HCL framework that integrates a HCL to detect various cyber attacks in SDN-IoT networks.

III. The HCL Framework

The HCL framework for SDN-IoT attack detection includes an IoT device layer with devices like heart monitors and vehicles, sending data to a Gateway Module. This module forwards data to the SDN Controller, which manages policies and contains an IDS using CNN for feature extraction and LSTM for traffic analysis. The HCL framework performs two key operations: network traffic preprocessing and model learning, as detailed in the following subsection.

In the first operation of the HCL framework, network traffic undergoes several preprocessing steps. Data is initially collected from IoT devices, followed by label encoding to convert categorical labels into numeric form. Benign traffic is encoded as 0, while DoS, DDoS, port scanning, OS, and service detection, and fuzzing are encoded as 1, 2, 3, 4, and 5, respectively, making them suitable for ML/DL algorithms. After preprocessing, a total of 21 features have been selected for model training. The features include flow metrics such as duration, average, standard deviation, minimum, and maximum durations, along with packet and byte counts for source-to-destination and destination-to-source flows. Additional features capture traffic volume per IP, packets per protocol and port, and inbound connections per source and destination IP.

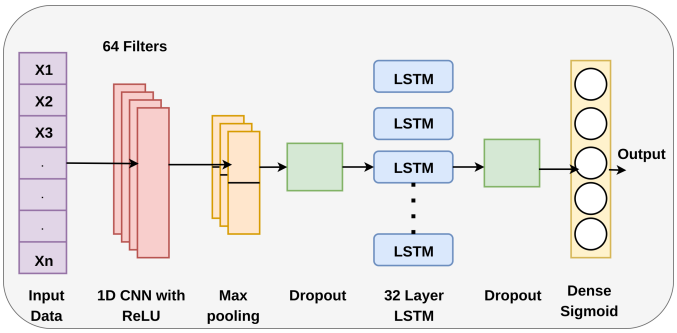


Fig. 1: The HCL Architecture

Algorithm 1 The HCL Framework

Input: Network Traffic Data $\mathbf{X} = \{x_1, x_2, ..., x_n\}$
Output: Intrusion Detection Probability y
Parameters: CNN Weights $\mathbf{W}$, States $\mathbf{H}, \mathbf{C}$, Output $\mathbf{W}_o$
procedure PREPROCESSDATA($\mathbf{X}$)
    Encode categorical labels using LabelEncoder
    Normalize features using StandardScaler
    Split data into $\mathbf{X}_{train}, \mathbf{X}_{test}, \mathbf{X}_{val}$
    Balance $\mathbf{X}_{train}$ using SMOTE
end procedure
procedure CNNLAYER($\mathbf{X}$)
    $\mathbf{F} \leftarrow \text{ReLU}(\mathbf{W} * \mathbf{X})$ ▷ 1D CNN with ReLU
    $\mathbf{P} \leftarrow \text{MaxPooling}(\mathbf{F})$ ▷ Max Pooling
    $\mathbf{D} \leftarrow \text{Dropout}(\mathbf{P}, p)$ ▷ Dropout
end procedure
procedure LSTMLAYER($\mathbf{D}$)
    Initialize $\mathbf{H}_0, \mathbf{C}_0$
    for each timestep t in $\mathbf{D}$ **do**
        $\mathbf{H}_t, \mathbf{C}_t \leftarrow \text{LSTM}(\mathbf{D}_t, \mathbf{H}_{t-1}, \mathbf{C}_{t-1})$
    end for
end procedure
procedure DENSELAYER($\mathbf{H}_T$)
    $y \leftarrow \sigma(\mathbf{W}_o^T \mathbf{H}_T + b_o)$ ▷ Sigmoid for binary
end procedure
Call PREPROCESSDATA($\mathbf{X}$)
$\mathbf{D} \leftarrow$ Call CNNLAYER($\mathbf{X}$)
$\mathbf{H}_T \leftarrow$ Call LSTMLAYER($\mathbf{D}$)
$y \leftarrow$ Call DENSELAYER($\mathbf{H}_T$)
return y

Algorithm 1 outlines all the operations from network traffic preprocessing to model learning within the HCL framework illustrates in Fig 1, designed to detect various cyber attacks.

IV. Experimental Results and Evaluation

A. Experimental Dataset

To evaluate the HCL framework, the SDN network dataset [18] is used, with a testbed set up in Mininet to simulate an IoT environment managed by an ONOS controller. The testbed features IoT devices mimicking smart home technologies and includes attacks such as DoS, DDoS using hping3, port scanning, OS fingerprinting with nmap, and fuzzing attacks. Two scenarios are tested: one with five IoT devices and another with ten, where devices dynamically connect and disconnect to mimic real-world IoT variability. The dataset contains 210,000 records of both benign and malicious traffic, including 24,834 records for benign traffic and a similar number of records for each class of attack. This distribution offers a robust framework for testing SDN-based IoT networks. The dataset is divided into an 80-20 ratio, with 80% of the data used for training and 20% reserved for testing. A custom application tags flows based on port connections, organizing the data into CSV files with separate files for different attack types. While it mirrors the Bot-IoT dataset's features, it only includes attributes extractable from SDN flow entries. During DoS and DDoS attacks, only 100 flow records are kept per cycle due to IP spoofing, while no cap is enforced for port scanning and OS fingerprinting due to packet uniqueness. A concise set of 21 key features, is selected for model training. The rationale for this selection is based on excluding features that may lead to overfitting, such as IP address, port numbers and protocols.

B. Evaluation Metrics

In assessing the performance of the proposed framework within the SDN-enabled IoT environment, we measure accuracy, precision, recall, and the F1 score. Additionally, inference time is a essential metric, representing the model's efficiency and responsiveness in a real-time setting. Our experiments are designed to evaluate not only binary classification scenarios, distinguishing between normal and malicious traffic, but also multiclass classification, identifying various types of attacks. We utilize a one-vs-rest strategy to handle the multiclass classification problem, ensuring that each class is compared against all others to improve detection accuracy. This approach is applied to both scenarios with 5 and 10 IoT devices, to validate the model's efficacy across different network scales and complexity.

To ensure precise intrusion detection in the IoT network, the hybrid model in HCL framework is implemented in Python using Keras and scikit-learn on a 2.3-GHz Quad-Core Intel Core i7 with 16 GB RAM. The model features setup, outlined in Table I, supports both binary and multiclass classification, distinguishing between normal activities and cyber threats across varying IoT scenarios.

C. Evaluation Results

We assess the efficiency of our HCL framework's hybrid CNN-LSTM model, examining its capabilities in both binary and multiclass classification. This section presents our evaluation outcomes, comparing the performance of the hybrid model against standalone CNN and LSTM [16] architectures.

TABLE I: Simulation Parameters

Parameter	Value
Model Type	Sequential
CNN Layer (Conv1D)	64 filters, kernel size 3, activation 'relu', padding 'same'
Pooling(MaxPooling1D)	Pool size 2
Regularization(Dropout)	0.25 after MaxPooling1D
LSTM Layer	32 units, with state returned across batches
Normalization	Applied after LSTM
Regularization	0.3 after LSTM
Optimizer	Adam with learning rate 0.001
Loss Function	Categorical Crossentropy
Metrics	Accuracy
Epochs	50 (maximum, subject to early stopping)
Batch Size	256

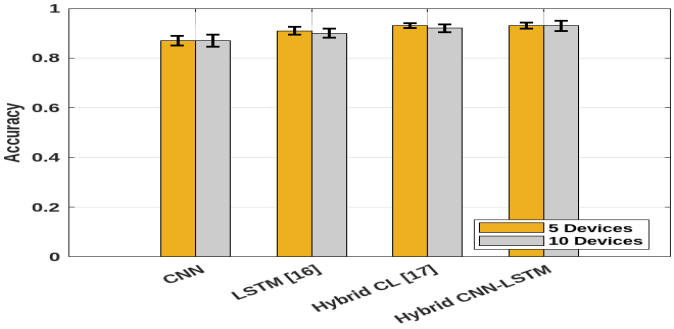


Fig. 2: Average Accuracy by Varying Number of Devices in Binary Classification.

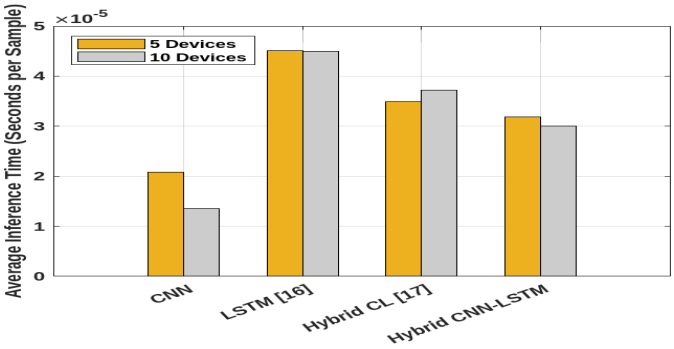


Fig. 3: Average Inference Time by Varying Number of Devices in Binary Classification.

1) Binary Classification: Fig. 2 shows the average accuracy of four models: HCL, standalone CNN, standalone LSTM [16], and hybrid CL [17], for binary classification with 5 and 10 IoT devices. The HCL, hybrid CL, and CNN models achieve identical accuracy of 0.93, indicating robust performance. The LSTM and hybrid CL models also show competitive accuracy, though the latter experiences increased inference time as devices scale. The average inference time is shown in Fig 3. The LSTM has higher inference time, while the hybrid CL model's time increases with 10 devices. The CNN model is fastest, achieving 0.85 seconds for 10 devices,

benefiting from efficient batch processing. Overall, the CNN provides the quickest inferences, while the HCL offers higher accuracy, balancing speed and performance.

2) Multiclass Classification: Fig. 4 shows the average accuracy of models for multiclass classification, with error bars showing the standard deviation across 20 runs. The HCL achieves the highest accuracy (0.93 for 5 devices, 0.92 for 10 devices), followed by the hybrid CL [17], CNN (0.83 and 0.82), and LSTM [16] (0.87 and 0.86). Fig. 5 illustrates average inference times. The CNN is the fastest (1.09s for 5 devices, 1.1s for 10), followed by the HCL (1.39s and 1.38s). The LSTM [16] is the slowest (5.32s and 5.1s). The HCL offers the best balance of accuracy and speed, while the CNN excels in speed but with lower accuracy.

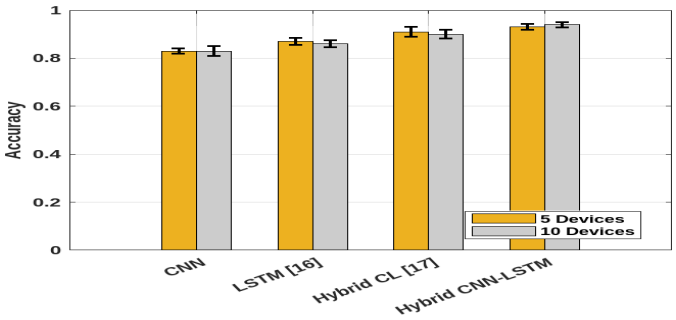


Fig. 4: Average Accuracy by Varying Number of Devices in Multiclass Classification.

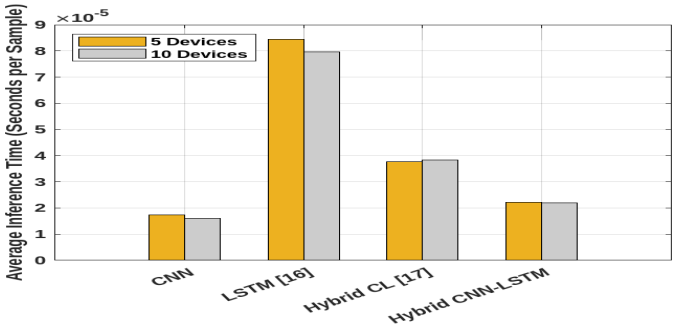


Fig. 5: Average Inference Time by Varying Number of Devices in Multiclass Classification.

Table II shows the other performance metrics such as precision, recall and F1-score for each class in multiclassification scenario. The HCL model consistently performs well across all classes for both scenarios with 5 and 10 devices. For 5 devices, it shows strong recall especially in class 5 with perfect recall, while maintaining high precision across classes. For 10 devices, there is a slight drop in precision for benign class but overall the model maintains performance. The CNN model shows a significant drop in precision for benign class for both scenarios but notably so for 10 devices, where precision drops to 0.94. The LSTM [16] model has a similar performance pattern to the hybrid model, with a slight drop in precision when moving from 5 to 10 devices. The HCL model also performs well, with strong precision and recall in most classes. However, it experiences a slight drop in precision in the 10-device scenario.

Fig 6 shows the training and validation accuracy of 10 devices as well as Receiver Operating Curve (RoC) to measure the performance of our HCL model for multiclass classification of 5 and 10 devices. Multiple ROC curves are plotted, each representing a different class in a multiclass classification setting. The AUC for each class is close to 1.00, with the lowest being 0.95 for benign Class and the highest being 1.00 for DoS attack. The training accuracy shows how well the model is learning the training dataset, while the validation accuracy shows how well the model generalizes to data it has not seen before. The curves start to increasing, which indicates that the model is reaching its peak performance on the current data. In the case of 10 devices, consistency in AUC suggests the model's performance is robust to the change from 5 to 10 devices. Again, high AUC values are observed (0.94 to 1.00), with multiple classes achieving near-perfect scores. Performance is consistent with the 5-device setting, showing that increasing the number of devices does not degrade the model's discriminative ability. Further, validation accuracy closely tracks training accuracy, indicating the model's effectiveness across different data splits.

D. Discussion

The HCL framework shows promising results, with high precision and recall indicating strong accuracy in classifying traffic as benign or malicious.

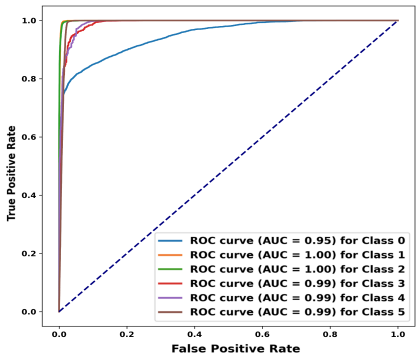
- The model shows high precision, recall, and class differentiation, reflected in high AUC values for Precision-Recall and ROC curves.
- The consistency of performance metrics between the 5-device and 10-device settings suggests that scaling the number of devices does not have a negative impact on model performance.
- Training and validation accuracy trends imply the model learns well without overfitting, maintaining a good balance between fitting the training data and generalizing to unseen data. This is consistent across both device settings.

V. Conclusion

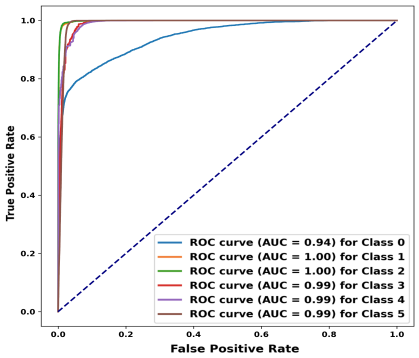
In IoT networks, where devices are constantly communicating, integrating SDN brings efficient network management. It also opens doors to new cyber threats, especially for interconnected IoT devices. This paper explores a deep learning framework combining CNN and LSTM networks to strengthen cybersecurity in SDN-IoT systems. This hybrid CNN-LSTM model detects various cyber attacks and identifies benign and attack network traffic. It achieves more than 90% accuracy in detecting various cyber attacks, proving its effectiveness as an intrusion detection system. In practical scenarios involving 5 to 10 IoT devices, our model consistently maintained high accuracy, precision, recall, and F1 scores. This indicates not only the model's effectiveness in attack detection but also its resilience and reliability when scaled across varying network sizes. Such adaptability is crucial for SDN-IoT networks that

TABLE II: Multiclass Metrics Across Models and Devices

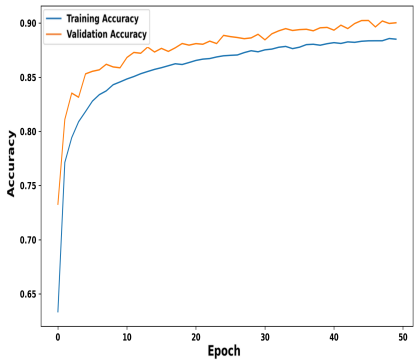
Class	No of Devices	Hybrid CNN-LSTM			CNN			LSTM [16]			HybridCL [17]		
		Precision	Recall	F1 Score	Precision	Recall	F1 Score	Precision	Recall	F1 Score	Precision	Recall	F1 Score
Benign (0)	5	0.92	0.88	0.90	0.93	0.61	0.74	0.92	0.71	0.80	0.92	0.71	0.80
	10	0.90	0.91	0.90	0.94	0.63	0.75	0.91	0.68	0.78	0.93	0.74	0.83
DoS (1)	5	0.96	0.98	0.97	0.95	0.98	0.96	0.96	0.99	0.97	0.96	0.99	0.97
	10	0.94	0.98	0.96	0.95	0.98	0.96	0.95	0.98	0.96	0.98	0.98	0.97
DDoS (2)	5	0.95	0.98	0.96	0.94	0.97	0.95	0.96	0.98	0.97	0.96	0.98	0.97
	10	0.97	0.95	0.96	0.93	0.98	0.95	0.96	0.96	0.97	0.97	0.97	0.97
Port Scanning (3)	5	0.88	0.90	0.89	0.86	0.82	0.84	0.89	0.90	0.89	0.89	0.90	0.89
	10	0.89	0.93	0.91	0.85	0.80	0.82	0.87	0.87	0.87	0.91	0.76	0.83
OS Fingerprinting (4)	5	0.89	0.89	0.89	0.79	0.86	0.82	0.88	0.91	0.89	0.88	0.91	0.89
	10	0.90	0.88	0.89	0.76	0.88	0.82	0.86	0.89	0.87	0.78	0.91	0.84
Fuzzing (5)	5	0.90	1.00	0.95	0.80	0.98	0.88	0.87	0.99	0.93	0.87	0.99	0.93
	10	0.87	0.98	0.92	0.84	0.98	0.90	0.84	0.99	0.91	0.83	0.99	0.91



(a) ROC curve for 5 devices



(b) ROC curve for 10 devices



(c) Training and validation accuracy-10 devices

Fig. 6: Comparison of the HCL model's multiclass classification performance metrics for 5 and 10 IoT devices

are inherently dynamic and expanding. Future work includes implementing the framework in real SDN-IoT networks and optimizing the model for faster performance.

ACKNOWLEDGMENT

The research was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

[1] H. A. Hassan, E. E. Hemdan, W. El-Shafai *et al.*, "Intrusion detection systems for the internet of thing: a survey study," *Wireless Personal Communications*, 2753-2778, 2023.

[2] R. Chaganti, W. Suliman, V. Ravi *et al.*, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," *Information*, 41, 2023.

[3] D. Yeom, N. Niknami, and J. Wu, "Evaluating performance of intrusion detection systems under different configurations in SDN," in *Proceedings of the Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, 418–423, 2023.

[4] J. Bhayo, S. A. Shah, S. Hameed *et al.*, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Engineering Applications of Artificial Intelligence*.

[5] M. Saiyed and I. Al Anbagi, "Entropy and divergence-based DDoS attack detection system in IoT networks," in *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications*. IEEE, 224–230, 2023.

[6] J. Ashraf, N. Moustafa, A. D. Bukhshi *et al.*, "Intrusion detection system for SDN-enabled IoT networks using machine learning techniques," in *2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), IEEE*, 46–52, 2021.

[7] S. Javanmardi, M. Shojafar, R. Mohammadi *et al.*, "An SDN perspective IoT-Fog security: A survey," *Computer Networks*, 109732, 2023.

[8] M. Aslam, D. Ye, A. Tariq *et al.*, "Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT," *Sensors*, 2697, 2022.

[9] D. Javeed, T. Gao, M. S. Saeed *et al.*, "A softwarized intrusion detection system for IoT-enabled smart healthcare system," *ACM Transactions on Internet Technology*, 2023.

[10] A. Wani, R. S, and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," *CAAI Transactions on Intelligence Technology*, 281-290, 2021.

[11] M. Bagaa, T. Taleb, J. B. Bernabe *et al.*, "A machine learning security framework for IoT systems," *IEEE Access*, 114066-114077, 2020.

[12] V. Ravi, R. Chaganti *et al.*, "Deep learning feature fusion approach for an intrusion detection system in SDN-based IoT networks," *IEEE Internet of Things Magazine*, 24-29, 2022.

[13] A. Chouhan and J. T. Yao, "Privacy-preserving federated learning: Insights and perspectives," in *Book of Abstracts, International Joint Conference on Rough Sets (IJCRS'24)*, 6–9, 2024.

[14] J. T. Yao and A. Sharma, "Continual federated learning for dynamic data environments," in *2024 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, 10690191, 2024.

[15] R. A. Elsayed, R. A. Hamada, M. I. Abdalla *et al.*, "Securing IoT and SDN systems using deep-learning based automatic intrusion detection," *Ain Shams Engineering Journal*, 102211, 2023.

[16] A. A. Alashhab, M. S. M. Zahid, A. Muneer *et al.*, "Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks," *International Journal of Advanced Computer Science and Applications*, 2022.

[17] H. C. Altunay and Z. Albayrak, "A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks," *Engineering Science and Technology, an International Journal*, 101322, 2023.

[18] A. K. Sarica and P. Angin, "A novel SDN dataset for intrusion detection in IoT networks," in *2020 16th International Conference on Network and Service Management (CNSM), IEEE*, 1–5, 2020.

[19] T. Jafarian, A. Ghaffari, A. Seyfollahi *et al.*, "Detecting and mitigating security anomalies in software-defined networking using gradient-boosted trees and floodlight controller characteristics," *Computer Standards & Interfaces*, 103871, 2024.

[20] M. S. Towhid and N. Shahriar, "Early detection of intrusion in SDN," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 1-6, 2023.