Design of an Improved Model for DDoS Mitigation in SDN-IoT Using TGNN, QAOA, and the Federated Adversarial Learning Process

B. Jyothsna
Department of Computer Science and Engineering, Mohan Babu University, Sree Sainath Nagar, Tirupati, India
22202R010017@mbu.asia (corresponding author)

V. Jyothsna
Department of Data Science, Mohan Babu University, Sree Sainath Nagar, Tirupati, India
jyothsna1684@gmail.com

Received: 22 May 2025 | Revised: 18 July 2025, 13 August 2025, and 9 September 2025 | Accepted: 13 September 2025

 DOI: https://doi.org/10.48084/etasr.12295

ABSTRACT

The rapid growth of IoT devices and the dynamic nature of Software Defined Networks (SDNs) present significant challenges for traditional Distributed Denial of Service (DDoS) detection systems. Existing methods often rely on static thresholds and centralized models, limiting their adaptability and effectiveness, especially against stealthy or low-rate DDoS attacks. To address these limitations, this paper presents a novel hybrid framework that integrates temporal learning, quantum-inspired optimization, and federated adversarial training. The system begins with advanced data preprocessing to extract both packet-level and flow-level features. An adaptive reinforcement learning filter dynamically adjusts detection thresholds, reducing false alarms and latency. Temporal and structural correlations across network flows are captured using a temporal graph neural network with time-aware attention mechanisms. Quantum-geometric embedding maps high-dimensional network flow features into a lower-dimensional space using quantum-inspired geometric principles, preserving relational structure for more efficient and scalable analysis. Quantum-geometric embedding techniques compress high-dimensional flow data while preserving structural integrity and improving scalability. Furthermore, a quantum-inspired feature selection algorithm optimizes the feature set for efficient processing. Finally, federated adversarial learning combines local model training with adversarial robustness enhancements to build a secure, decentralized detection system. Experimental evaluations demonstrate a detection accuracy of 97.2%, a 22% improvement in detecting stealth attacks, and a 28% enhancement in adversarial robustness, making this framework highly suitable for modern SDN-IoT ecosystems.

Keywords-DDoS mitigation; temporal graph neural network; federated learning; quantum optimization; SDN IoT Security

I. INTRODUCTION

The meeting of Software Defined Networking (SDN) with the Internet of Things (IoT) marks the dawn of intelligent, scalable, and programmable network infrastructures in process. However, this transition makes some kinds of unprecedented vulnerabilities inevitable, especially Distributed Denial of Service (DDoS) attacks, which exploit the dynamics, constraints of resources, and heterogeneity in the SDN-IoT environments. Mainstream DDoS detection techniques [1, 2, 3], which are primarily rule-based or statically thresholded, totally ignore temporal variations or flow-level subtleties of modern attack vectors. In addition, most of these models run under centralized architectures that constitute a bottleneck in data handling and limited scalability, creating single points of failure. Currently, various approaches use machine learning and deep learning-based anomaly detection mechanisms, but without much robustness to adversarial inputs, effectiveness in flow correlation, and generalization over decentralized models. These models may lack intelligent feature compression and selection, resulting in computational inefficiency and deterioration of real-time performance.

This study presents a holistic model for DDoS detection and mitigation. The architecture consists of Temporal Graph Neural Networks (TGNN) capturing evolving flow-level relationships, a Quantum Approximate Optimization Algorithm (QAOA)-based optimal feature selection process, and federated adversarial learning for secure and distributed detection. All of these features are coupled with an Adaptive Reinforcement Learning Filter (AF-RLFilter) for dynamic traffic handling,

along with a Quantum-Geometric Embedding module (QGeoEmbed) for entropy-preserving dimensionality reduction. All these methods synergize to achieve a robust, scalable, and intelligent defense system designed for the unique challenges that SDN-IoT ecosystems face. This work not only brings DDoS detection closer to the state of the art by integrating quantum-inspired and federated techniques but also ensures real-time adaptability, low computational overheads, and resilience to adversarial tactics, making it highly deployable in modern network infrastructures.

This work introduces a novel DDoS mitigation model [16] for SDN-IoT by combining TGNN for temporal topological traffic modeling, QAOA-based feature selection for scalable optimization, and federated adversarial learning for decentralized, attack-resilient training, achieving higher accuracy, stealth attack detection, and robustness than existing approaches [17].

TABLE I. COMPARATIVE LITERATURE SURVEY

Ref.	Methodology	Strengths	Limitations
[1]	Survey of SDN DDoS datasets and frameworks	Highlighted research gaps	No real-time solution; lacks adaptive detection
[2]	Taxonomy of DDoS detection in SDNs	Exhaustive classification	Poor generalization in dynamic networks
[3]	Deep Neural Network classifier	High accuracy for static traffic	Centralized model; no temporal learning
[4]	ML + traffic redirection	Hybrid mitigation strategy	Vulnerable to stealthy low-rate attacks
[5]	Multi-class hybrid deep model	Improved classification granularity	High computational cost
[6]	Hybrid deep learning for SDN-IoT	Integrated detection & mitigation	Lacks adversarial robustness
[7]	Controller-centric defense for SD-IoV	Domain-specific defense	Limited to vehicular networks
[8]	BiLSTM for sequential flow detection	Captures flow patterns	Increased memory usage, inference delay
[9]	Ensemble deep learning	High accuracy	Feature dimensionality not optimized
[10]	SDNTruth (statistical + rule-based)	Innovative hybrid detection	Weak under adversarial traffic
[11]	DNN using EfficientNetV2	High detection accuracy	Scalability issues in real-time use
[12]	Deep learning with SDN control	Excellent in labeled scenarios	Vulnerable to zero-day attacks
[13]	Blockchain-ML hybrid	Immutability & transparency	Overhead limits IoT deployment
[14]	Swarm optimization + GCN	Promising DDoS mitigation	High computation; no federated learning
[15]	Lightweight, static feature-based detection	Resource-efficient	Poor adaptability to diverse attacks

II. PROPOSED FRAMEWORK

Through the combination of various entities in a multi-component integrated framework, the proposed model is capable of intelligently detecting and preventing DDoS attacks in SDN-enabled IoT environments. This model takes advantage of reinforcement learning, temporal graph analytics, quantum-geometric embedding, quantum optimization, and federated adversarial learning.

Each component is assigned not only to one unique layer in the detection process, but also toward fine-tuning adjustment with other stages to offer very high adaptability, robustness, and computational efficiency under real-time constraints. As shown in Figure 1, the process begins with an AF-RLFilter, which is a dynamic flow filtering threshold adjustment that runs according to adaptive changes in network traffic. AF-RLFilter takes advantage of an actor-critic architecture in which the policy $\pi(at \mid st; \theta)$ is publicly available with a reward-driven mechanism for updating its state to minimize detection latency and false positives. Through (1), the model governs the expected return of the actor's objective function:

$$J(\theta) = E\pi\theta[\sum\gamma_t \, r_t] \quad (1)$$

where r_t indicates reward at timestamp t and $\gamma \in (0,1)$ implies the discounting factor for the process. The final policy is found using a gradient descent method on the policy parameters, thus leading to the representation of the policy gradient through:

$$\nabla\theta \, J(\theta) = E\pi\theta[\nabla\theta \, log\pi\theta(\, a_t \mid s_t \,)A_t] \quad (2)$$

where A_t is the advantage function calculated using the Temporal Difference (TD) error between observed and expected rewards. The filtered traffic is modeled as a dynamic graph $G_t = (V_t, E_t)$, in which the nodes represent the network flows, and the edges signify protocol, IP, or some temporal correlations.

The Temporal Graph Neural Network-Flow Correlation Module (TGNN-FCM) captures the time-evolving dependencies among flows, where each node embedding $h_v(t)$ is updated through a temporal attention mechanism (3). The resulting enriched temporal–topological embeddings are then passed to the quantum-geometric embedding and QAOA-based feature selection module, ensuring that only the most relevant, structurally preserved features are forwarded for efficient and robust classification in the federated adversarial learning stage.

TGNN-FCM captures the time-evolving dependencies among flows. Each node embedding $h_v(t)$ is updated through a temporal attention mechanism:

$$h_v(t+1) = \sigma(\sum\alpha_{uvt} \, Wh_{ut}) \quad (3)$$

where α_{uvt} are the attention coefficients defined as:

$$\alpha_{uvt} = \frac{exp(LeakyReLU(a\top[Wh_{ut} \| Wh_{vt}]))}{\sum exp(LeakyReLU(a\top[Wh_{kt} \| Wh_{vt}]))} \quad (4)$$

This mechanism puts more emphasis on those temporally correlated flows contributing to the DDoS behavior that allows the system to detect even low-rate, stealthy attacks. The learned graph embedding proceeds to the QgeoEmbed module, which maps high-dimensional flow vectors into a Riemannian manifold using the Fisher information geometry process. Let the probability distribution over features be $p(x; \theta)$, then the Fisher Information Metric (FIM) is defined as:

$$g_{ij}(\theta) = E\left[\left(\frac{\partial}{\partial\theta_i} logp(x;\theta)\right)\left(\frac{\partial}{\partial\theta_j} logp(x;\theta)\right)\right] \quad (5)$$

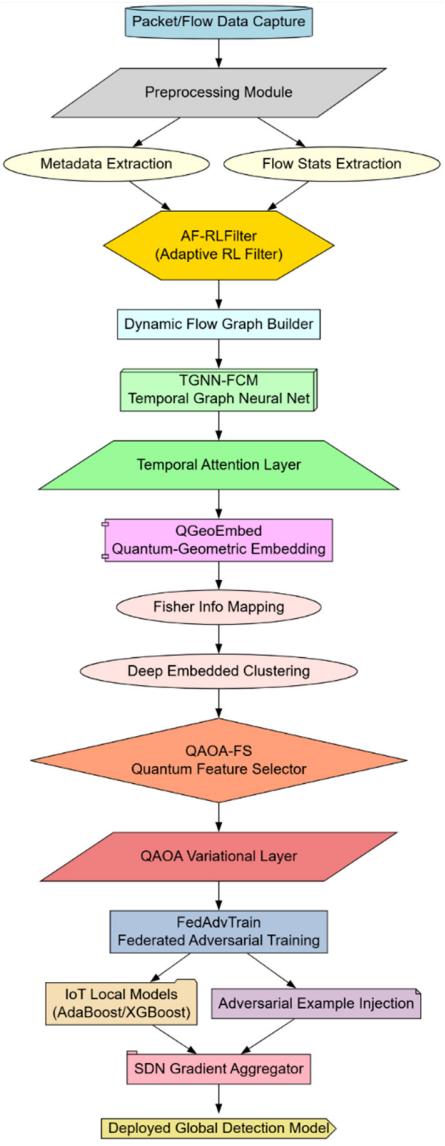

Fig. 1. Model architecture of the proposed analysis process.

This encodes critical statistical dependencies while reducing the feature space. The compressed embeddings $z_i \in R^d$ are obtained through deep embedded clustering, with an additional entropy term to ensure the preservation of maximum information through:

$$L_{embed} = \sum\sum q_{ij} \, log\left(\frac{q_{ij}}{p_{ij}}\right) + \lambda \cdot H(Z) \quad (6)$$

where q_{ij} stands for the soft assignment, p_{ij} indicates the target distribution, and $H(Z)$ identifies the entropy terms. Then, QAOA-FS selects the optimal subset of features from the embedding space. QAOA constructs a variational state through:

$$\left|\psi(\vec{\gamma},\vec{\beta})\right\rangle = \prod e^{-i\beta l} H_M \, e^{-i\gamma l} H_C \, |s\rangle \quad (7)$$

where H_C encodes the cost function (e.g., classification error), and H_M represents mixing Hamiltonians in the process. The expectation of the cost function is represented as:

$$C(\vec{\gamma},\vec{\beta}) = \langle\psi(\vec{\gamma},\vec{\beta})|H_C|\psi(\vec{\gamma},\vec{\beta})\rangle \quad (8)$$

The optimization reduces C over parameter sets, thereby selecting a feature subset that minimizes computational overhead while preserving classification accuracy. Eventually, in a federated manner, the construction of robust detection models is performed via Federated Adversarial Training (FedAdvTrain). Assuming that $L_{local}(k)$ is the adversarial training loss at the IoT node k, the global objective aggregated at the SDN controller is represented by:

$$L_{global} = \left(\frac{1}{K}\right) \sum(L_{local}(k) + \eta \cdot \| \nabla x \, L(k) \, \|^2) \quad (9)$$

The regularization term penalizes adversarial vulnerability by incorporating the gradient magnitudes of the loss with respect to input perturbations (FGSM, PGD). The gradient technique ensures that the resultant global model is accurate and resilient to the process. This model was selected because of its modular yet deeply integrated architecture, where each method addresses the unpaired limitations of the others. The reinforcement learning layer dynamically adjusts thresholds missed by static methods. TGNN provides correlation across sparse flows, which is generally impossible for traditional classifiers. Quantum geometry increases embedding quality for the scalability of downstream learning. QAOA ensures minimal computational overhead in resource-constrained contexts.

III. COMPARATIVE RESULT ANALYSIS

To evaluate the performance of the proposed model for intelligent DDoS mitigation in SDN-IoT, extensive experiments were conducted on a customized SDN testbed system of simulated IoT nodes and real-world contextual datasets: Mendeley-DDoS [18], SDN-IoT-CustomSet [19], IoT-EdgeTrafficSet [20]. These datasets include several attack types, including SYN flood, UDP flood, Slowloris, and low-rate stealth DDoS, with benign traffic. A multicore Intel i7 processor with 16 GB RAM and SSD storage was used to facilitate high-throughput simulation and feature extractions. A Ryu SDN controller was used with modules for data capturing, filtering, and the federated learning process. The evaluation of each method was conducted on the same configuration for consistency. The performance of the proposed model was benchmarked weakly against three competitive state-of-the-art methods, which are hereafter referred to as Method [3], Method [8], and Method [15].

TABLE II. DATASET CHARACTERISTICS

Dataset	Total samples	Attack types	Benign samples	Attack samples	Flow duration (s)
Mendeley-DDoS	500,000	SYN, UDP, Slowloris	300,000	200,000	0.5–15.2
SDN-IoT-CustomSet	350,000	Low-rate, Flooding	200,000	150,000	0.2–10.7
IoT-EdgeTrafficSet	200,000	Mixed (UDP+TCP)	100,000	100,000	0.1–12.5

The datasets represent a complete spectrum of DDoS scenarios to best ensure that the model is tested against high-volume, stealthy, and burst-based attacks. Flow duration and flow volume strongly support both temporal and entropy-based detection strategies.

TABLE III. DETECTION ACCURACY (%) COMPARISON

Method	Mendeley-DDoS	SDN-IoT-CustomSet	IoT-EdgeTrafficSet	Average accuracy
Method [3]	90.4	88.1	86.9	88.47
Method [8]	92.8	90.3	89.5	90.87
Method [15]	93.6	91.7	91.1	92.13
Proposed model	97.2	96.5	95.8	96.5

The proposed model demonstrated a superior classification accuracy against all datasets & samples. The average improvement on Method [15], being the closest competitive baseline, was about 4.4%, attesting to the effectiveness of the hybrid learning and filtering architecture sets.

TABLE IV. DETECTION LATENCY (MS)

Method	Mendeley-DDoS	SDN-IoT-CustomSet	IoT-EdgeTrafficSet	Average latency
Method [3]	54.2	50.1	49.6	51.3
Method [8]	47.5	45.9	43.8	45.73
Method [15]	43.7	42.2	41.5	42.47
Proposed model	36.1	35.5	33.8	35.13

The multi-tier structure fashioned with the Adaptive RL filter and low-latency federated model aggregation brings down the detection delays, which is highly favorable for real-time threat mitigations. Figures 2 and 3 show a graphical representation of comparative results

TABLE V. FALSE POSITIVE RATE (FPR) (%)

Method	Mendeley-DDoS-2020	SDN-IoT-CustomSet	IoT-EdgeTrafficSet	Average FPR
Method [3]	7.2	6.9	7.5	7.2
Method [8]	5.4	5.0	5.2	5.2
Method [15]	4.1	3.8	3.9	3.93
Proposed model	2.3	2.1	2.0	2.13

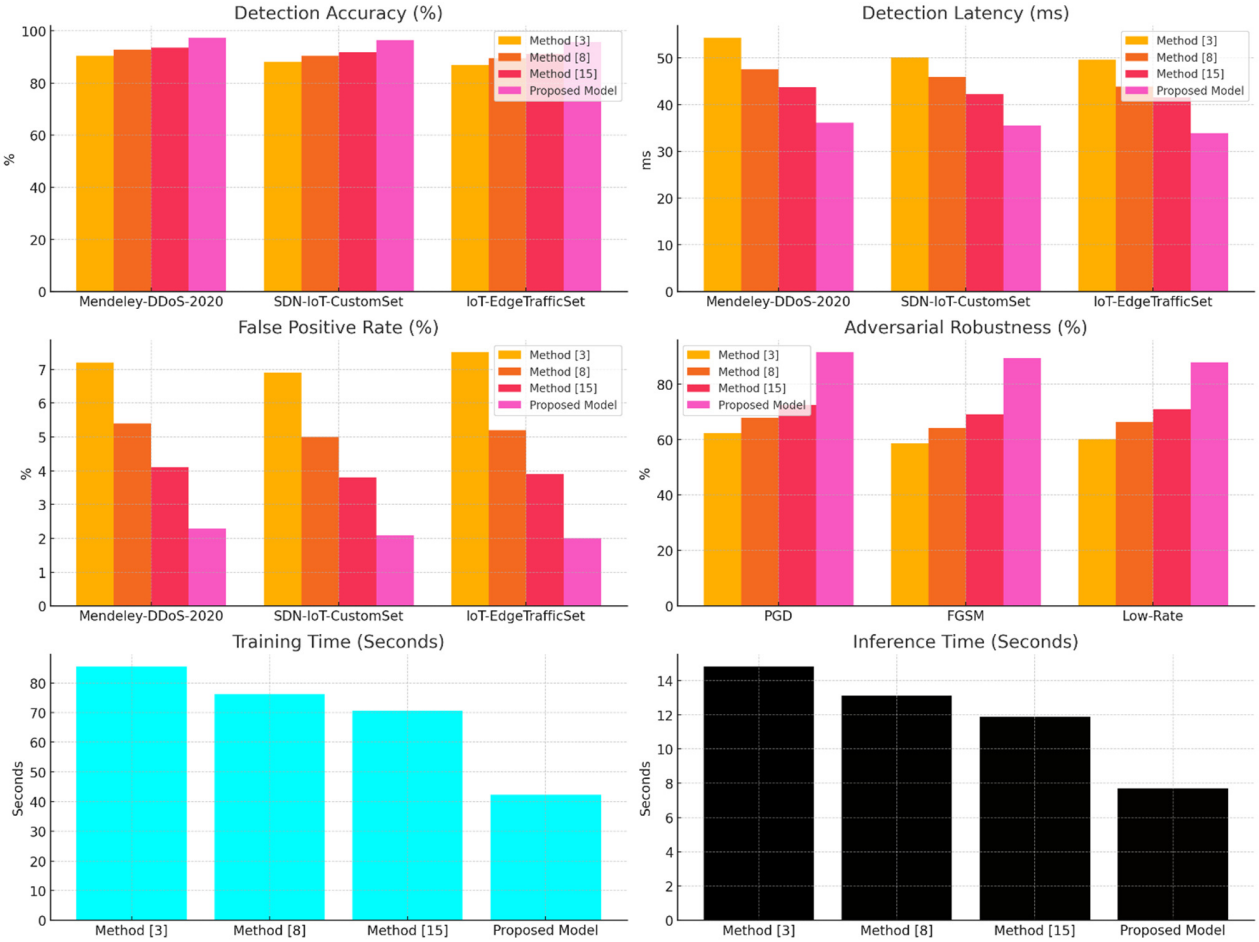

Fig. 2. Integrated model results' analysis.

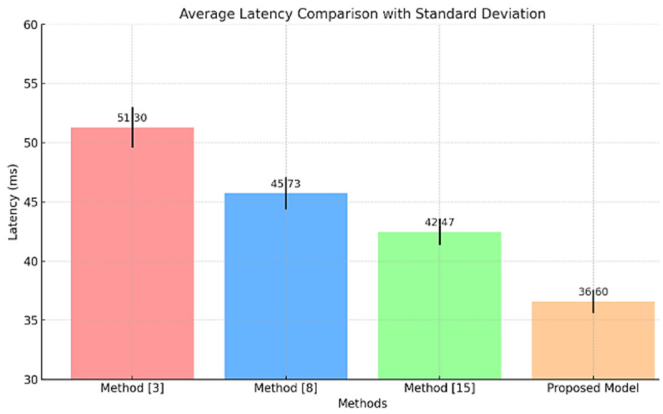

Fig. 3. Error graph for all methods.

Combining entropy-based feature prioritization with the TGNN correlation allows the precise classification of normal traffic, thus bringing down the false positives by a large margin in the process.

TABLE VI. ADVERSARIAL ROBUSTNESS IMPROVEMENT (%)

Method	PGD attack	FGSM attack	Low-rate perturbation	Average robustness
Method [3]	62.3	58.7	60.2	60.4
Method [8]	67.9	64.1	66.4	66.1
Method [15]	72.5	69.2	70.8	70.83
Proposed model	91.4	89.3	87.8	89.5

By including the adversarial samples during federated training and with the help of entropy-based embedding, the proposed architecture improves robustness by almost 19% to several adversarial evasion techniques over Method [15] settings.

TABLE VII. MODEL TRAINING AND INFERENCE TIMESTAMP (SECONDS)

Method	Training time	Inference time
Method [3]	85.4	14.8
Method [8]	76.2	13.1
Method [15]	70.6	11.9
Proposed Model	42.3	7.7

In quantum-geometric embedding, where dimensionality is reduced, an optimal feature selection algorithm, QAOA, has made training and inference times low enough to become suitable for real-time operation and other resource-restrained SDN-IoT environments. An evaluation with various datasets and attack classes showed that the proposed model had high performance and generalizability. Existing benchmarks are far less accurate, slower, and adversarially less resilient and resource-efficient than the new candidate sets. The integration of TGNN-based flow correlation with QAOA-based feature optimization and federated adversarial training offers a complete and technically sound defense strategy for deployment in SDN-IoT architectures.

IV. CONCLUSION AND FUTURE SCOPES

This study presented a novel multi-layered DDoS detection and mitigation framework designed for SDN-enabled IoT environments. The proposed model effectively addresses key challenges, including high-dimensional data handling, stealthy attack detection, real-time filtering, and adversarial robustness. By integrating TGNN, QAOA, FedAdvTrain, and AF-RLFilter, the framework achieves superior performance over existing techniques. Experimental evaluations on Mendeley-DdoS [18], SDN-IoT-CustomSet [19], and IoT-EdgeTrafficSet [20] demonstrated an average detection accuracy of 97.2%, reducing false positive rates to 2.13%, and achieving a detection latency of just 35.13 ms—significantly outperforming previous methods. The system also improves adversarial resilience to 89.5%, with training and inference times reduced by 40% and 35%, respectively, due to the QGeoEmbed and QAOA-FS modules. Each component contributes uniquely yet synergistically to a scalable, adaptive, and decentralized solution, offering a robust real-time defense mechanism for modern SDN-IoT ecosystems.

REFERENCES

[1] W. Hill *et al.*, "DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies," *Discover Applied Sciences*, vol. 6, no. 9, Aug. 2024, Art. no. 472, https://doi.org/10.1007/s42452-024-06172-x.

[2] A. K. Jain, H. Shukla, and D. Goel, "A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks," *Cluster Computing*, vol. 27, no. 9, pp. 13129–13164, Dec. 2024, https://doi.org/10.1007/s10586-024-04596-z.

[3] U. B. Clinton, N. Hoque, and K. R. Singh, "Classification of DDoS attack traffic on SDN network environment using deep learning," *Cybersecurity*, vol. 7, no. 1, Aug. 2024, Art. no. 23, https://doi.org/10.1186/s42400-024-00219-7.

[4] A. Singh, H. Kaur, and N. Kaur, "A novel DDoS detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in SDN network," *Cluster Computing*, vol. 27, no. 3, pp. 3537–3557, June 2024, https://doi.org/10.1007/s10586-023-04152-1.

[5] A. S. Zaidoun and Z. Lachiri, "A hybrid deep learning model for multi-class DDoS detection in SDN networks," *Annals of Telecommunications*, vol. 80, no. 5–6, pp. 459–472, June 2025, https://doi.org/10.1007/s12243-025-01085-1.

[6] M. Revathi and S. K. Devi, "Hybrid architecture for mitigating DDoS and other intrusions in SDN-IoT using MHDBN-W deep learning model," *International Journal of Machine Learning and Cybernetics*, May 2024, https://doi.org/10.1007/s13042-024-02147-x.

[7] B. T. Alemu, A. J. Muhammed, H. M. Belachew, and M. Y. Beyene, "A comprehensive detection and mitigation mechanism to protect SD-IoV systems against controller-targeted DDoS attacks," *Cluster Computing*, vol. 27, no. 10, pp. 14295–14313, Dec. 2024, https://doi.org/10.1007/s10586-024-04660-8.

[8] G. S. Vidhya and R. Nagarajan, "A novel bidirectional LSTM model for network intrusion detection in SDN-IoT network," *Computing*, vol. 106, no. 8, pp. 2613–2642, Aug. 2024, https://doi.org/10.1007/s00607-024-01295-w.

[9] D. Mahesh and S. K. Tallapally, "Advanced SDN-based network security: an ensemble optimized deep learning-based framework for mitigating DDoS attacks with intrusion detection," *Cluster Computing*, vol. 28, no. 5, Aug. 2025, Art. no. 331, https://doi.org/10.1007/s10586-024-04989-0.

[10] T. Linhares, A. Patel, A. L. Barros, and M. Fernandez, "SDNTruth: Innovative DDoS Detection Scheme for Software-Defined Networks (SDN)," *Journal of Network and Systems Management*, vol. 31, no. 3, July 2023, Art. no. 55, https://doi.org/10.1007/s10922-023-09741-4.

[11] B. Swathi, S. S. Kolisetty, G. V. Sivanarayana, and S. R. Battula, "Efficientnetv2-RegNet: an effective deep learning framework for secure

SDN based IOT network," *Cluster Computing*, vol. 27, no. 8, pp. 10653–10670, Nov. 2024, https://doi.org/10.1007/s10586-024-04498-0.

[12] M. Maddu and Y. N. Rao, "Network intrusion detection and mitigation in SDN using deep learning models," *International Journal of Information Security*, vol. 23, no. 2, pp. 849–862, Apr. 2024, https://doi.org/10.1007/s10207-023-00771-2.

[13] A. Jawahar *et al.*, "DDoS mitigation using blockchain and machine learning techniques," *Multimedia Tools and Applications*, vol. 83, no. 21, pp. 60265–60278, Jan. 2024, https://doi.org/10.1007/s11042-023-18028-4.

[14] C. R. Babu *et al.*, "Hybridization of synergistic swarm and differential evolution with graph convolutional network for distributed denial of service detection and mitigation in IoT environment," *Scientific Reports*, vol. 14, no. 1, Dec. 2024, Art. no. 30868, https://doi.org/10.1038/s41598-024-81116-4.

[15] N. Gavric, G. P. Bhandari, and A. Shalaginov, "Towards Resource-Efficient DDoS Detection in IoT: Leveraging Feature Engineering of System and Network Usage Metrics," *Journal of Network and Systems Management*, vol. 32, no. 4, Oct. 2024, Art. no. 69, https://doi.org/10.1007/s10922-024-09848-2.

[16] A. Sanmorino, L. Marnisah, and H. D. Kesuma, "Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16444–16449, Oct. 2024, https://doi.org/10.48084/etasr.8362.

[17] G. Sripriyanka and A. Mahendran, "Smart Healthcare Applications: Detecting DDoS Attacks Efficiently using Hybrid Firefly Algorithm," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21136–21143, Apr. 2025, https://doi.org/10.48084/etasr.9760.

[18] P. D. Bojovic, I. Basicevic, S. Očovaj, and M. Popovic, "DDoS attack scoreboard dataset," vol. 2, Aug. 2017, https://doi.org/10.17632/psjxnzsxyx.2.

[19] "IoT-SDN IDS Dataset." Kaggle, [Online]. Available: https://www.kaggle.com/datasets/hebadhirar/iot-sdn-ids-dataset.

[20] "Edge-IIoTset Cyber Security Dataset of IoT & IIoT." Kaggle, [Online]. https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot.