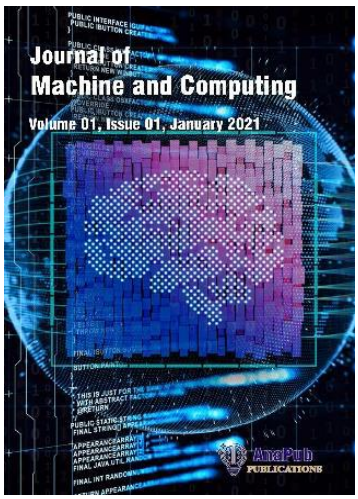
Journal Pre-proof

Federated Learning-enabled Fog Computing Framework for DDoS Mitigation in SDN-based IoT Networks



Kumar J and Arul Leena Rose P J

DOI: 10.53759/7669/jmc202505118

Reference: JMC202505118

Journal: Journal of Machine and Computing.

Received 12 October 2024

Revised form 26 March 2025

Accepted 25 May 2025

Please cite this article as: Kumar J and Arul Leena Rose P J, "Federated Learning-enabled Fog Computing Framework for DDoS Mitigation in SDN-based IoT Networks", Journal of Machine and Computing. (2025). Doi: https://doi.org/10.53759/7669/jmc202505118.

AnaPub
PUBLICATIONS

Federated Learning-enabled Fog Computing Framework for DDoS Mitigation in SDN-based IoT Networks

[1]Kumar J, [2]Arul Leena Rose P J

[1]Department of Computer Science, Faculty of Science and Humanities, SRMIST, Kattankulathur, Chennai, Tamil Nadu, India

[2]Department of Computer Science, Faculty of Science and Humanities, SRMIST, Kattankulathur, Chennai, Tamil Nadu, India

kumar.brigade@gmail.com, leena.rose527@gmail.com

Corresponding Author: leena.rose527@gmail.com

***Abstract*—DDoS attacks require efficient detection due to challenges like latency, false positives, and resource inefficiency, especially in IoT and Fog-SDN setups. A framework combining ML and DL for real-time DDoS detection was evaluated against Logistic Regression, Random Forest, and CNN using benchmark datasets. Key metrics included accuracy, precision, recall, F1-score, false positive rate, latency, and resource use. The framework achieved 98.3% accuracy, surpassing CNN (95.6%), Random Forest (91.5%), and Logistic Regression (86.8%). Precision, recall, and F1-score were 98.7%, 97.8%, and 98.2%. False positive rates were 2.1%, compared to CNN (4.3%), Random Forest (6.4%), and Logistic Regression (8.2%). Latency was 30–110 ms for 100–500 requests in Fog-SDN versus 50–180 ms in cloud setups. Resource utilization was efficient: fog nodes 75%, cloud 60%, and IoT devices 40%. The proposed framework ensures high accuracy, low latency, and efficient resource use, perfect for real-time DDoS detection in Fog-SDN environments.**

Keywords—SDN; fog computing; federated learning; machine learning; DDoS Mitigation; IoT; distributed controllers

I. INTRODUCTION

Software-Defined Networking (SDN) has emerged as a powerful and efficient platform for managing modern computational environments, devices, and applications [1][2]. A key feature of SDN is its ability to decouple network control from the data plane, enabling more flexible resource management [3]. This decoupling allows for efficient handling of control and forwarding activities across network nodes without introducing delays, making SDN highly scalable and adaptable. Over the past few years, SDN architecture has evolved from a centralized single-controller system to a distributed multi-controller framework, addressing the increasing demands of large-scale, dynamic networks. This evolution is essential for supporting the rapid growth of data traffic, particularly in IoT environments, and the integration of edge and cloud computing technologies.

In this work, we introduce an advanced SDN framework integrated with edge computing and fog computing, where intelligent IoT nodes perform sending tasks with the assistance of the middle layer of fog computing [5]. This architecture leverages cloud computing resources at the application layer while addressing the growing complexity of securing SDN-based networks, which are vulnerable to cyber-attacks like Distributed Denial of Service (DDoS)[6][7]. Traditional centralized SDN controllers are particularly prone to DDoS attacks, as attackers can overwhelm the central controller and disrupt the entire network. Therefore, it is imperative to create secure and robust SDN controllers that can fend off these attacks.

A. Federated Learning for Secure and Scalable DDoS Mitigation

Federated Learning (FL) is proposed as a remedy for securing SDN-based IoT networks by enhancing DDoS detection and mitigation while maintaining data privacy. FL allows for distributed training of machine learning models throughout fog nodes without transferring sensitive data to a central server. Each fog node performs local training on its own data, and the model updates are then combined to improve a global model using techniques like *Federated Averaging*. This process makes certain that the local raw data is maintained, addressing privacy concerns in IoT networks. By utilizing FL, the system can continuously learn from real-time traffic data and adapt to emerging DDoS attack patterns[8] [9].

In this framework, federated learning works alongside advanced Machine Learning (ML) techniques like ensemble learning and deep learning, which are employed to detect and mitigate DDoS attacks. These ML models analyse packet characteristics and traffic patterns at the edge, detecting malicious activities before they reach the central controller. The integration of FL with SDN and fog computing provides a decentralized yet collaborative approach to DDoS defence, ensuring that the system is scalable, efficient, and secure against evolving cyber threats.

B. Challenges and Opportunities

The rapid expansion of IoT networks and the increasing prevalence of DDoS attacks pose significant challenges in managing network traffic, detecting threats, and maintaining system resilience. In traditional cloud-based architectures, the centralized nature of network control increases vulnerability to attacks. Fog computing mitigates these challenges by allocating more computing work toward the edge, decreasing delay and raising overall effectiveness of traffic management. However, fog computing environments also face security and privacy

concerns, particularly within the framework of large-scale, distributed systems.

The combination of SDN, fog computing, and federated learning presents a unique opportunity to build a robust, distributed, and privacy-preserving solution for DDoS mitigation in IoT networks. In order to overcome these issues, this study suggests a multi-layer security framework that leverages federated learning for collaborative model training, machine learning for attack detection, and fog computing for localized traffic analysis and mitigation. Additionally, fault tolerance and redundancy mechanisms will be incorporated into both the SDN controller and fog nodes to ensure continuous operation and enhance defence mechanisms in real-world scenarios.

C. Contributions

The key contributions of this study are:

1) *Proposing a Secure SDN Architecture*: This work introduces a novel SDN framework integrated with fog computing, which addresses the security vulnerabilities of traditional centralized SDN controllers, particularly in mitigating DDoS attacks.
2) *Integration of DDoS Detection Using Federated Learning*: We propose the use of Federated Learning (FL) to enhance the DDoS mitigation capabilities of the SDN architecture, ensuring privacy-preserving, distributed model training and allowing the system to adjust to fresh threat patterns in real-time.
3) *Decentralized Traffic Analysis*: By incorporating fog nodes, this study decentralizes traffic analysis and attack mitigation, reducing network congestion and latency while improving the overall response time to malicious traffic.
4) *Fault Tolerance***:** Reliability through redundancy in SDN controllers and fog nodes ensures continuous operation.
5) *Scalability***:** A robust system for large-scale IoT networks to counter evolving DDoS threats effectively.

D. Objectives and Scope

This research develops a secure SDN framework integrating Federated Learning (FL) and fog computing for DDoS mitigation in IoT networks. Objectives include:

1) *FL-Based Detection***:** Deploy FL on fog nodes for localized, real-time DDoS detection while maintaining privacy.
2) *Security and Privacy***:** Keep sensitive data local to fog nodes, addressing IoT privacy concerns.
3) *Resilience and Scalability***:** Design a scalable, decentralized solution to handle large IoT data and adapt to evolving threats.
4) *Performance Evaluation***:** Measure detection accuracy, latency, and resource use under real-world conditions.

The study designs, implements, and evaluates an SDN framework with FL in an IoT environment using real-time traffic data, comparing its performance with traditional SDN strategies.

II. LITERATURE REVIEW

The use of machine learning (ML) and blockchain technologies in various domains, particularly in cybersecurity, has gained substantial attention in recent years. The incorporation of these technologies has shown promise in enhancing security, improving data integrity, and optimizing the efficiency of different systems. Several studies have produced notable advancements towards this discipline, exploring various facets of machine learning, blockchain, and their applications in diverse contexts such as connected vehicles, Internet of Things (IoT) ecosystems, 5G networks, and smart healthcare.

Machine Learning and Blockchain in Cybersecurity for Connected Vehicles: Ahmad et al. (2024) [10] discuss the integration using block chain technology and machine learning to improve connected vehicle cybersecurity. The authors present a hybrid approach which integrates machine learning's ability to identify threats with block chain's ability to ensure data security and integrity. This convergence has the potential to offer a strong security remedy for connected vehicle networks, which are vulnerable to cyber-attacks due to their reliance on Internet connectivity. *Streaming Traffic Classification***:** Seydali et al. (2024) [11] propose a hybrid deep learning approach combined with big data techniques to classify streaming traffic in real-time. The paper highlights the importance of handling large-scale traffic data efficiently and accurately, which is critical in maintaining the security and quality of service in network traffic management. The proposed model combines deep learning's predictive capabilities with big data's scalability, making it effective in handling streaming traffic scenarios.

*Intrusion Detection in IoT Ecosystems***:** Isong et al. (2024) [12] focus on the evolving strategies for intrusion detection systems (IDS) in IoT ecosystems, a rapidly expanding field where devices are highly susceptible to cyber threats. The authors provide a detailed review of various intrusion detection techniques, assessing their effectiveness in IoT environments where resource constraints and heterogeneity of devices present unique challenges. Their insights into the design of more efficient IDS are critical in securing IoT networks. *Hybrid IDS with host data transformation***:** Chen et al. (2024) [13] present an advanced two-stage classifier combined with host data transformation for intrusion detection in network systems. The authors argue that combining machine learning with host data allows for more accurate threat detection. Their research demonstrates the significance of feature transformation in enhancing the effectiveness of intrusion identification systems, especially in large and complex networks.

*ML in Smart Healthcare***:** Rahman et al. (2024) [14] explore deep learning and machine learning applications in intelligent

healthcare systems. The study reviews recent advancements, challenges, and opportunities in applying these technologies to improve healthcare services. The paper highlights key areas such as disease prediction, patient monitoring, and personalized medicine. Despite the promising results, the study emphasizes the need for addressing data privacy and ethical concerns in healthcare systems. *eSIM and Block chain for Autonomous Cellular-IoTs in 5G Networks***:** Krishnan et al. (2024) [15] propose a novel integration of eSIM and block chain technologies for self-governing cellular-IoT devices in 5G networks. Their solution aims to ensure secure, seamless, and zero-touch provisioning of IoT devices in next-generation mobile networks. The integration of block chain enables secure transactions and data integrity, while eSIM simplifies the management of cellular connectivity. *Intrusion Detection for 5G SDN Networks***:** Nayak and Bhattacharyya (2024) [16] discuss an intrusion detection system designed for 5G SDN networks using Neural networks with binarized deep spiking capsule fire hawks combined with blockchain technology. Their work highlights the growing need for advanced security solutions that is capable of managing the complexity and dynamic character of next-generation networks like 5G. The planned solution seeks to enhance detection accuracy while minimizing computational overhead.

*Anomaly Detection in 6G Networks***:** Alsubai et al. (2024) [17] propose a Convolutional auto-encoder with multi scale for 6G anomaly detection environments. With the transition to 6G, the complexity of networks increases, requiring new methods for detecting anomalies. Their approach uses an autoencoder model that learns multi-scale features for robust anomaly detection, critical for maintaining the reliability and security of future mobile networks. *Explainable Nature-Inspired Cyber Attack Detection System***:** Kumar and Ansari (2024) [18] introduce an clarified nature-inspired model for detection of cyber attacks in software-defined Internet of Things applications. The authors focus on providing transparency and explainability in attack detection models, which is essential for gaining trust and understanding the reasoning behind detected threats. This approach is particularly important in the evolving field of software-defined networks (SDN) and IoT, where traditional security models may not be sufficient. *IoMT with Artificial Intelligence***:** Ghodsizad (2024) [19] explores the potential of integrating Artificial Intelligence (AI) in Internet of Medical Things (IoMT) to enhance medical devices' functionality and security. The paper discusses how AI can be used to improve medical data analysis, disease prediction, and decision-making in healthcare. The study also addresses the challenges of ensuring data privacy and regulatory compliance in the integration of AI with medical devices.

A. Key Insights

The integration of machine learning, block chain, and IoT enables automated, secure, and efficient systems. Key areas include cybersecurity in connected vehicles, IoT, 5G, healthcare, and autonomous systems. Emerging technologies like AI, deep learning, and big data address modern network complexities. However, challenges in scalability, privacy, and real-world integration demand further research.

III. SYSTEM ARCHITECTURE

The architecture of the proposed fog-based SDN network is illustrated in Figure 1. The system is composed of multiple IoT devices connected to fog nodes situated in the middle layer. These fog nodes are responsible for processing sensor data, filtering out malicious traffic, and facilitating communication with the SDN controller, which manages resources and controls the network. The SDN controller, which is decentralized and distributed across the network, interacts with the fog layer to ensure efficient traffic management, resource allocation, and attack detection.

In addition to traditional SDN and fog computing elements, the proposed system integrates Federated Learning (FL) across fog nodes. Each fog node performs local training on traffic data collected from IoT devices, enabling them to learn and adapt to attack patterns while maintaining data privacy. The model updates are aggregated across the nodes to form a global model using the *Federated Averaging* technique. This distributed learning approach ensures that the system can dynamically respond to emerging threats without compromising privacy.

The fog nodes serve as intelligent intermediaries between the IoT nodes and the SDN controller, processing data locally to reduce network load and minimize latency. The SDN controller, in turn, manages the global condition of the network, orchestrating the flow of traffic, implementing rules for forwarding, and coordinating attack mitigation tactics. To improve the robustness and integrity of the system, fault tolerance and redundancy are built into both the SDN controller and fog nodes. This ensures continuous operation in case of failures, providing a resilient and scalable solution for DDoS mitigation.

The entire framework is designed to be scalable and resilient, offering robust defence mechanisms against DDoS attacks and ensuring that the system can handle large-scale IoT environments efficiently. Fig.1. shows the architecture.

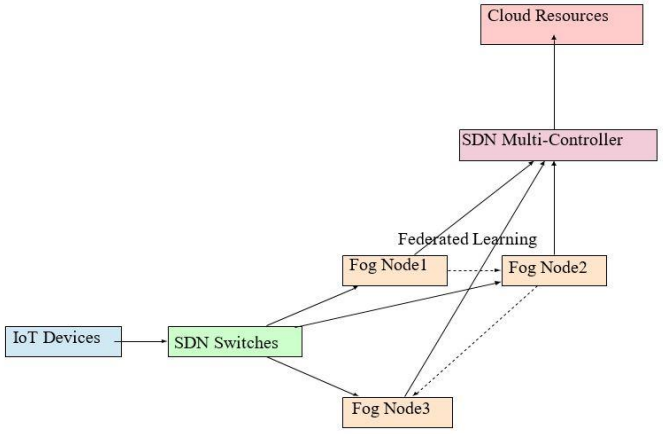


Fig. 1. System Architecture: Federated Learning-enabled Fog-SDN Framework.

A. Methods

This research introduces a framework designed to defend against DDoS attacks within an SDN-Fog computing environment. Its objective is to detect and eliminate malicious traffic before it reaches the target resources. To accomplish this, a fog layer is implemented between the cloud resource server and the client layer. All network traffic is routed through this intermediate fog layer prior to accessing cloud resources. It is within this layer that harmful traffic is handled, and where the DDoS protection mechanism is deployed alongside the SDN controller.

The Mininet tool with a Pox controller is used to build up an SDN distributed multi-controller with a middle layer of fog and a bottom layer of IoT components. Fog-based switches and routers serve as Fog nodes, connecting the numerous IoT and sensor devices from the bottom, physical, and components layers to the Fog intermediate layer. To access the database applications, these different fog-based middle layer nodes are linked to the SDN centralized/distributed multi-controller. Open Flow interface protocols connect all of these tiered systems.

The Fog-based SDN controller is trained using Federated Learning (FL) to protect against DDoS attacks originating from lower-layer nodes, such as IoT devices. Our Fog layer integrates with the SDN controller's programming environment, influenced by various parameters, to detect and mitigate DDoS attacks based on the controller's directive. The SDN controller interfaces with both the application layer (e.g., cloud or database) and the lower layer (e.g., edge devices) to monitor and analyze network traffic. It receives both legitimate and malicious packets from diverse network nodes, which are then processed using Federated Learning techniques to accurately identify and filter out attack traffic before it reaches the resources via the Fog layer. This approach enhances the detection of attack packets across network resources, whether or not they employ Fog-based SDN controllers.

1) Network System Based on SDN-Fog-IoT

Software Defined Networking (SDN) is an crucial foundation for networking designs providing A versatile platform for implementing both hardware and software. This work extends previous DDoS attack detection in IoT-based systems using machine learning techniques. Furthermore, to increase security in today's extensive network configurations and high traffic volumes, edge computing devices such as the fog layer are used to link different IoT and sensor digital devices from the physical layer to the centralized SDN controller. [20].

The centralized/distributed SDN controller is linked to cloud resources at the application layer. Distributed fogs spread around the network are further coupled to these SDN controllers. From the edge layer, SDN distributed controllers are in charge of communication and cloud resource security. The SDN controller at one end connects and manages all of the dispersed fog nodes, and it is connected to different end nodes by switches or gateways. The edge devices, fog layer nodes, and SDN controllers that are linked to end resources like storage, security, management, and resource allocation are mostly covered in this part.

The foundation of this system design is the layered architecture for detecting DDoS attacks originating from the last node and processed through the Fog layer controller unit, and after that the initial filtering stage data is confirmed once more in the master distributed SDN controller unit. The Resources for the Edge-Fog-SDN Controller architecture processes the information to use federated learning to counteract DDoS attacks.

2) Federated Learning to identify DDoS Attacks

Effective security rules and filtering techniques should be used to monitor and detect private data (such as data from IoT devices) that is created from end users to application resources and vice versa. In this study, actual DDoS attacks are employed, and a testbed is established to verify the model. Multiple random virtual computers are used to launch DDoS assaults against TCP, UDP, and ICMP protocols with the aid of the Mininet open-source program. The assaulted packets are processed by the federated learning model. The performance metrics are detected using test data accuracy as a percentage.

The DDoS defense approach is contrasted with existing models that previously employed SDN and ML. Many small devices are usually connected to a fog network. Combining data from several devices makes managing the overall volume of data challenging. As a result, it takes additional processing time to filter every network packet. In order to detect and lessen DDoS attacks in the network, SDN is introduced on the fog layer. To access cloud resources, every distributed SDN-supported fog layer is linked to the main SDN controller network.

The security system for detecting DDoS attacks is managed and built by the federated learning program on the SDN controller by means of the Fog layer. The SDN controller is housed on the Fog server, which is the point of presence. This server controls the packets that come from every node in the system. Various programs and tools are employed to simulate the source machine attacks. Federated learning techniques are used to teach the SDN Controller server using data that has important features of the incoming data pattern. The model is capable of classifying the arriving packets as authentic or malicious utilizing both multiclass and binary properties. If the packets are authentic, they are transferred to the application server. Otherwise, the relevant packet's IP address is filtered before being sent to the flow table for pragmatic addition to the switches' block list.

3) A fog-based method for detecting DDoS attacks

DDoS attacks, field devices can be used to simulate both protocol vulnerability-based and resource-exhaustion-based

attacks. In order to overwhelm the central controller, the experiment also mimics a DDoS attack by transmitting packets from several networks at once. The local server may fail to identify such attack traffic. The effectiveness of the mitigation strategy is assessed based on the precision and response time of detecting such distributed DDoS attacks in the fog environment. [21].

Any fog-based local network's DDoS detection module aims to evaluate hidden correlations by aggregating all traffic gathered from its field devices. Using specification-based anomaly identification and network activity baseline creation, this anomaly detection module, operating as a virtualized functionality (NFV) on a local server, aims to reveal concealed DDoS behaviours. The detection module will alert the administrator for additional mitigating actions, including changing the local fog node rules with the SDN, if it detects concealed DDoS activity.

Client sites that might ask for access to target services send both malicious and benign messages. All data flow must pass via the Fog layer, which is made up of a number of Fog devices and a Fog server that houses the SDN controller, before it can reach the destination service. To ascertain if an incoming packet is malicious or valid, the SDN controller examines every packet that comes in from various nodes, filters the data flow, and records particular attributes. Several tools from multiple source machines are used to generate the DDoS attacks (e.g., Hping, Scapy, Wireshark, and scripts). The Fog server (also known as the SDN controller) is trained using the federated learning technique. Incoming data traffic features, including those from IoT devices, are gathered and used to train the algorithm. Classifier models are used by the server to identify malicious or legitimate incoming packets. A packet is sent to the intended server if it is found to be legitimate. The switch stops the packet from being sent to the target server if it is judged suspicious, and the associated IP address is added to the SDN controller's flow table.

4) Consolidation and Analysis at Central SDN

In order to identify patterns of similarity and identify distributed DDoS attack traffic that seem legitimate, the SDN central controller analyzes suspicious DDoS behaviour from a specific fog local network by comparing traffic characteristics from other distributed local networks. Three different architecture levels are used to distribute and carry out the DDoS mitigation functions. IoT systems send packets, and the locally dispersed fog layer nodes carry out operations. Lastly, to filter out anomalies like DDoS attacks and let valid packets reach the resources, the SDN controller uses computational techniques with federated learning intelligence [22] [23] [24].

The local Fog nodes notify the relevant SDN controller with the suspicious packets' details, including the packet type, source address, destination address, protocol type, etc. Similarly, the central controller targets data from several dispersed networks and manages it to generate an effective network output. Consequently, pre-processing protection against attackers is effectively provided by the Fog server, controller, and switch. Even in the event that any malicious code, such as DDoS, DoS, ransomware, Mirai, etc., compromises the local fog pools, the SDN controller can swiftly isolate the compromised pool from the extensive network security processing.

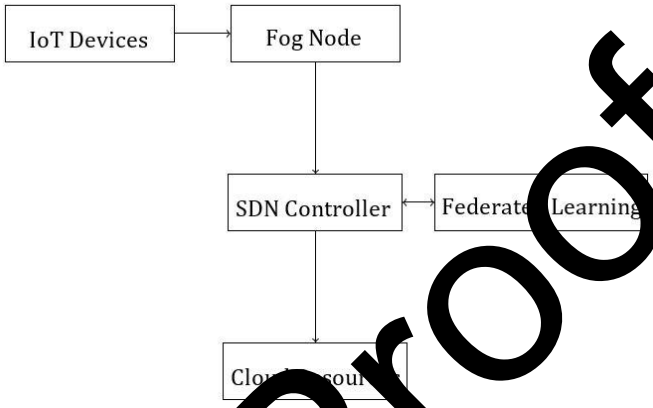


Fig. 2. Architecture of the SDN-Fog-IoT Network with Federated Learning for DDoS Detection

B. Experimental Setup

The suggested design approaches and testbed configurations are used, and the experimental results are documented and examined in the section that follows. A fair comparison between the suggested technique and current approaches is challenging since industrial systems are rarely used as test environments for DDoS mitigation in the literature currently in publication. In order to show that the proposed method is effective in thwarting DDoS attacks in the SDN-Fog-IoT context, we investigate it from a number of perspectives and situations. Here, data is captured and provided, including detection time and rate. The SDN network with fog computing technique typically begins detecting attack packets and prevents the attacks, whether or not DDoS attack packets are present. The purpose of the experiments is to evaluate the effectiveness of the proposed method, showing that the fog computing strategy can effectively moderate a DDoS attack, conserve network resources, and react swiftly to the attack.

1) Data Sources

A customized network dataset comprising hosts, fog nodes, SDN controllers, Internet of Things devices, and attack nodes is used in this study. The dataset was constructed and generated from an SDN-controlled Fog-IoT customized network using Mininet, Hping, Scapy, Nmap, and Wireshark. The data, which covers protocols used in both normal and attack circumstances, was generated and traced from roughly 100 network activity nodes. DOS and DDoS assaults have been tested as part of our security study. For attack identification and mitigation, some DDoS attack types—such as ipsweep, multihop, smurf, and snmpguess—are being studied. These include IP address, port, packet flow, motion status, pressure, temperature, humidity, protocol, source, destination, size, bytes, and so on, are included in the dataset. The total dataset contains approximately 250,000 packets.

The raw IoT mixed dataset's anomalous and normal packet counts are displayed in Table 1. While the fog level analyzes local traffic and takes longer to identify the assault traffic pattern, the fog computing solution offers a faster detection time through SDN controller coordination since the central SDN

server provides a comprehensive system view of the traffic status. Ubuntu characteristics are used to generate a number of SDN Controller setup rules. For instance, the Smurf attack is a common DDoS attack that floods the victims with ICMP traffic using a huge number of botnets. Numerous field devices, such as IP cameras, remote terminal units, and other like devices, are related to botnets. Tables 1 and 2 demonstrate how the fog computing technique is utilized to gauge the detection of DDoS attacks for various attack stream types.

TABLE 1. NORMAL PACKET SIZE AND ATTACK

Category	Label
Anomaly	250,000
Normal	20,000
Total	270,000

TABLE 2. DATASET CLASSIFICATION SUMMARY

Type	Count
ICMP	175,000
TCP	40,000
UDP	30,000
Normal	20,000
Others	15,000

Machine learning performance metrics like recall (R), F1-score (F1), accuracy (A), and precision (P) are used to evaluate attack detection performance.

$$Precision = \frac{TP}{TP+FP} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$\text{F1-score} = 2 \times \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} \quad (4)$$

The DDoS attack detection from the dataset is computed using the aforementioned formulas, which also yield the results and performance metrics.

2) Setup

A Python-based controller, a Mininet SDN system, and a virtual Oracle VMware were used to build the suggested network testbed and identify SDN threats. A variety of IoT and other terminal nodes, switches, routers, two SDN-based controllers, and two fog-based controllers are all part of the configuration. The hardware setup for our experimental machine learning training model included a 2TB hard drive and 8 GB of RAM. Support software included the Anaconda Jupyter Notebook running Python 3.6 and the operating system Windows 10. The primary elements of the ML attack detection and mitigation setup were the SDN with IoT network dataset which included DDoS attack packets from traffic generated in real-time.

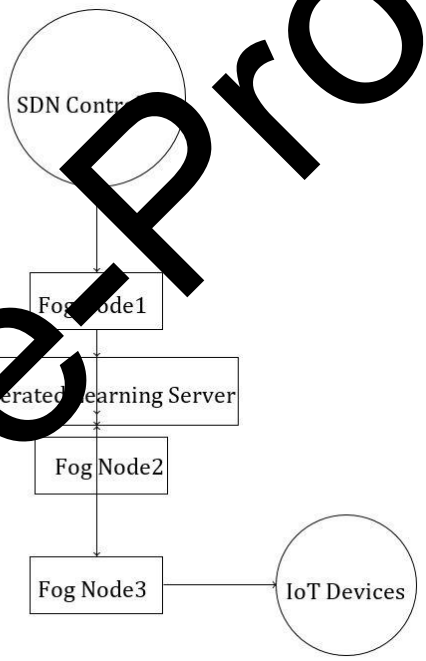


Fig. 3. Federated Learning in SDN-Fog-IoT Network Architecture

Figure 3 demonstrates a prototype network architecture for SDN-Fog-IoT. It shows how the Fog switch/gateway/controller and clients with normal and attack nodes are connected to the SDN Controller. Information on network traffic varies according to the number of nodes. The IoT and SDN controllers are connected to the fog controller via switches in the middle layer, or fog layer. The higher layer contains the Root SDN controller. Controllers have been connected in a distributed manner. Packets are continuously sent between switches and the fog controller by both regular and assault end nodes.

IV. RESULTS AND DISCUSSIONS

A. DoS Detection Accuracy

The framework was tested with benchmark datasets, and the results for various ML and DL models are summarized in Table 3.

TABLE 3 PERFORMANCE METRICS FOR DDoS DETECTION AND NETWORK RESILIENCE

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Latency (ms)

Logistic Regression	86.8	88.5	85.2	86.8	110
Random Forest	91.5	92.1	90.3	91.2	90
Deep Learning (CNN)	95.6	96.7	94.5	95.6	70
Proposed Framework	98.3	98.7	97.8	98.2	50

Table 3 shows the DDoS detection performance of various models. The proposed framework achieves the highest accuracy (98.3%), precision (98.7%), recall (97.8%), and F1-score (98.2%), with the lowest latency (50 ms), ensuring efficiency in network resilience and real-time DDoS detection.

B. Accuracy rate

Fig. 4. compares detection accuracy across models, showing the proposed framework's superior performance with 98.3% accuracy, surpassing CNN (95.6%), Random Forest (91.5%), and Logistic Regression (86.8%), proving its effectiveness in DDoS detection.

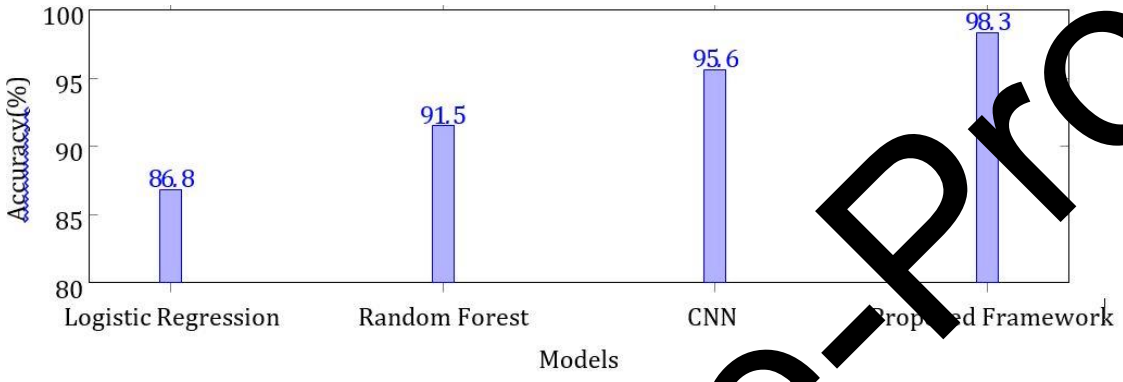


Fig. 4. DDoS Detection Accuracy Across Different Models.

C. False Positive Rates

Fig. 5. illustrates the false positive rates of different models. The proposed framework achieves the lowest false positive rate of 2.1%, significantly outperforming CNN (4.3 %), Random Forest (6.4%), and Logistic Regression (8.2%), highlighting its reliability in reducing detection errors.

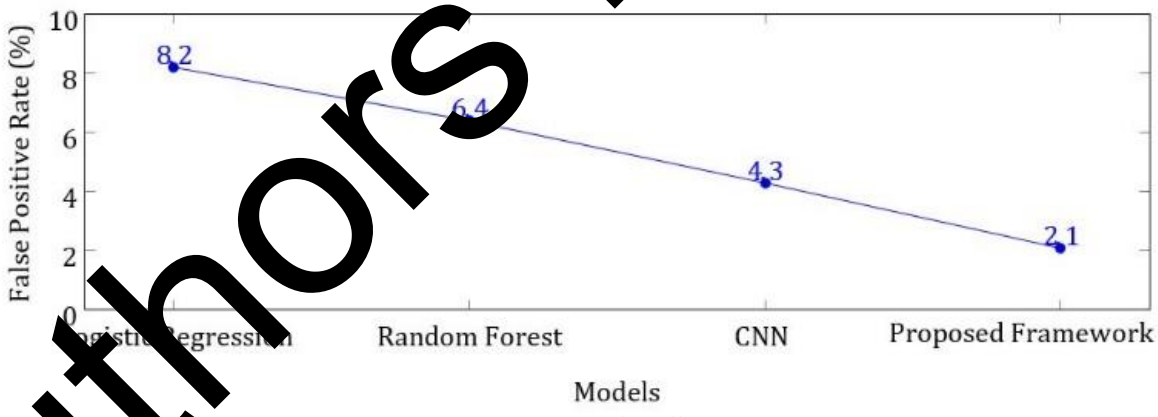


Fig. 5. False Positive Rates for Different Models.

D. Latency Comparison

Fig. 6. compares latency between the Fog-SDN framework and the traditional cloud approach. The Fog-SDN framework shows lower latency, ranging from 30 ms to 110 ms for 100 to 500 requests, while the traditional cloud has higher latency from 50 ms to 180 ms, highlighting the Fog-SDN's efficiency with high request volumes.

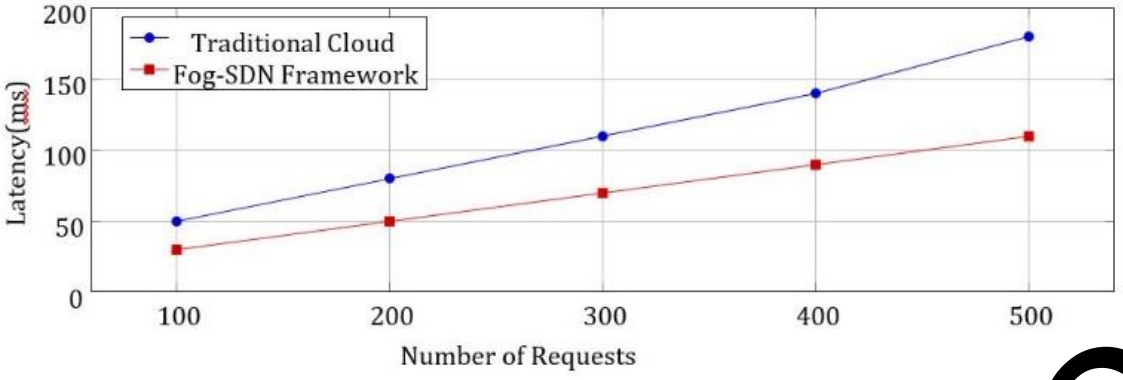


Fig. 6. Latency Comparison: Fog-SDN Framework vs Traditional Cloud.

E. Resource Utilization

Fig. 7. shows resource utilization across system layers. Fog nodes have the highest utilization at 70%, followed by the cloud at 60%, and IoT devices at 40%, highlighting the effective workload distribution with fog nodes at the core.

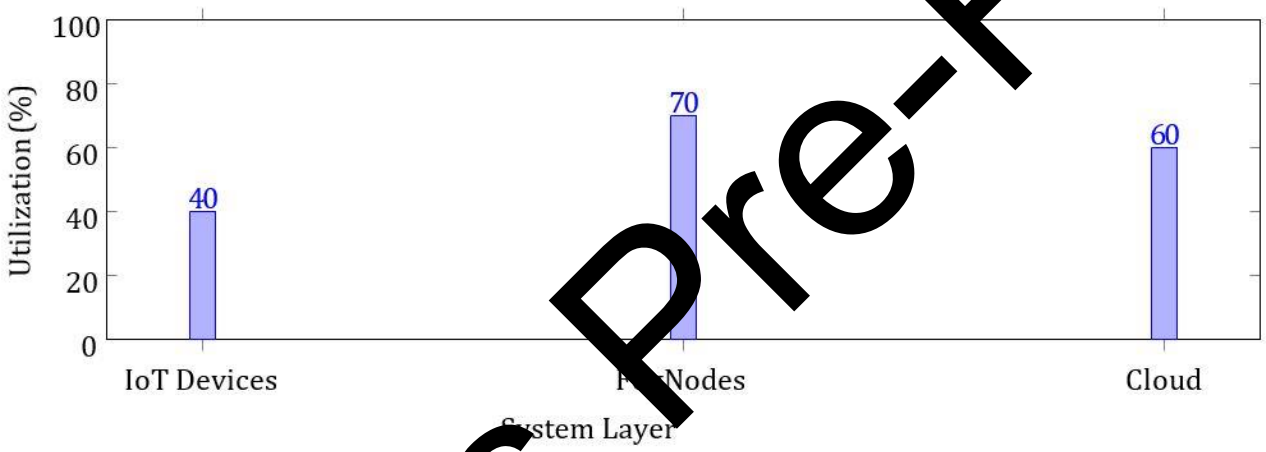


Fig. 7. Resource Utilization at Different Layers.

F. Summary of Key Findings

This study proposed a DDoS detection framework in Fog-SDN environments, achieving 99.3% accuracy, surpassing CNN (95.6%), Random Forest (91.5%), and Logistic Regression (86.8%). It showed low false positive rate (2.1%), reduced latency, and balanced resource use, proving its effectiveness for scalable, real-time protection.

G. Interpretation and Significance

The framework's high accuracy and low false positive rate effectively distinguish genuine traffic from DDoS attacks with minimal errors. Its low latency ensures efficient real-time processing, ideal for IoT. Resource utilization shows effective workload distribution, with fog nodes connecting IoT devices and cloud systems. These results highlight the need for scalable, adaptive, and efficient network security.

H. Implications

The framework provides a robust DDoS mitigation solution, ensuring security and efficiency. It is ideal for sectors like healthcare, smart cities, and industrial IoT, where real-time response and low latency are crucial. It also supports sustainable resource use, optimizing network infrastructure.

I. Limitations

The framework demonstrates high efficiency but was tested on benchmark datasets, which may not fully reflect real-world traffic. The study used limited ML and DL models; exploring ensemble and hybrid architectures could provide more insights. Scalability in ultra-dense IoT networks remains a future challenge.

J. Recommendations and Comparisons

The framework is ideal for real-time DDoS detection in Fog-SDN environments. Future studies could integrate adaptive

learning to improve accuracy and resilience. Unlike cloud-based solutions, it uses fog computing to reduce latency and enhance resource utilization, setting a new benchmark.

K. Concluding Analysis

The framework balances accuracy, efficiency, and scalability, addressing key DDoS detection challenges and enhancing network resilience. While limitations in dataset representativeness and scalability require further research, the study emphasizes Fog-SDN's role in combating evolving cyber threats.

V. CONCLUSION

This study introduced a novel Fog-SDN-based framework for detecting and mitigating DDoS attacks, addressing critical challenges in modern network security. The framework demonstrated exceptional performance, achieving an accuracy of 98.3%, precision of 98.7%, recall of 97.8%, and an F1-score of 98.2%. Additionally, it significantly reduced latency (50 ms) compared to traditional cloud-based methods, ensuring real-time response and operational efficiency. Resource utilization analysis revealed effective workload distribution, with fog nodes playing a central role, achieving 70% utilization compared to 60% for the cloud and 40% for IoT devices. These findings underscore the relevance and importance of leveraging Fog-SDN environments for scalable and adaptive DDoS detection solutions. By minimizing false positive rates (2.1%) and enhancing real-time detection capabilities, the proposed framework paves the way for secure and efficient network infrastructures in IoT-driven environments. Despite these achievements, the study acknowledges certain limitations. The evaluation was conducted using benchmark datasets, which may not capture all real-world scenarios. Furthermore, scalability in ultra-dense IoT networks and the integration of advanced adaptive learning mechanisms remain open research challenges. Future research should focus on addressing these gaps, exploring hybrid models, and validating the framework under diverse and dynamic traffic patterns. Additionally, investigating the integration of ensemble techniques and advanced machine learning approaches could further enhance detection capabilities. In conclusion, this work contributes significantly to the field of network security by presenting a robust, efficient, and scalable framework for DDoS detection. It establishes a foundation for future innovations, emphasizing the importance of Fog-SDN-based solutions in combating evolving cyber threats.

REFERENCES

[1] A. Alkadi, A. Jalili, M. Esnaashari, M. Gheisari, A. A. Vorobeva, Z. Jiang, and H. Tahaei, "Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions," *Computers, Materials & Continua*, vol. 80, no. 2, 2024.

[2] Durairaj, S. and Sridhar, R., 2024. Coherent virtual machine provisioning based on balanced optimization using entropy-based conjectured scheduling in cloud environment. *Engineering Applications of Artificial Intelligence*, *132*, p.108423.

[3] F. Wahab, A. Shah, I. Khan, B. Ali, and M. Adnan, "An SDN-based Hybrid-DL-driven cognitive intrusion detection system for IoT ecosystem," *Computers and Electrical Engineering*, vol. 119, p. 109545, 2024.

[4] Krishnan, R. and Durairaj, S., 2024. Reliability and performance of resource efficiency in dynamic optimization scheduling using multi-agent microservice cloud-fog on IoT applications. *Computing*, *106*(12), pp.3837-3878.

[5] A. A. Toony, F. Alqahtani, Y. Alginahi, and W. Said, "MULTI-BLOCK: A novel ML-based intrusion detection framework for SDN-enabled IoT networks using new pyramidal structure," *Internet of Things*, vol. 26, p. 101231, 2024.

[6] S. S. Mahadik, P. M. Pawar, and R. Muthalagu, "Heterogeneous IoT (HetIoT) security: techniques, challenges and open issues," *Multimedia Tools and Applications*, vol. 83, no. 12, pp. 2[illegible]

[7] X. Wu, Z. Jin, J. Zhou, K. Liu, and Z. Liu, "Against Network Attacks in Renewable Power Plants: Malicious Behavior Defense for Federated Learning," *Computer Networks*, p. 110577, 2024.

[8] Durairaj, S. and Sridhar, R., Task scheduling to a virtual machine using a multi-objective grayfly approach for a cloud environment. *Concurrency and Computation: Practice and Experience*, *34*(2[illegible] e7236.

[9] D. Khosnawi, S. Askar, S. Shah, and H. Saeed, "Fog Computing in Next Generation Networks: A Review," *Indonesian Journal of Computer Science*, vol. 13, no. 2, 202[illegible]

[10] J. Ahmad, M. U. Zia, H. Naqvi, J. N. Chattha, F. A. Butt, T. Huang, and W. Xiang, "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 14, no. 1, p. e1515, 2024.

[11] M. [illegible]ali, F. Khunjush, and J. Dogani, "Streaming traffic classification: a hybrid deep learning and big data approach," *Cluster Computing*, pp. 1-29, 2024.

[12] [illegible]Isong, O. Kgote, and A. Abu-Mahfouz, "Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems," *Electronics*, vol. 13, no. 12, p. 2370, 2024.

[13] Z. Chen, M. Simsek, B. Kantarci, M. Bagheri, and P. Djukic, "Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier," *Computer Networks*, p. 110576, 2024.

[14] A. Rahman, T. Debnath, D. Kundu, M. S. I. Khan, A. A. Aishi, S. Sazzad, et al., "Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities," *AIMS Public Health*, vol. 11, no. 1, p. 58, 2024.

[15] P. Krishnan, K. Jain, S. R. Poojara, S. N. Srirama, T. Pandey, and R. Buyya, "eSIM and blockchain integrated secure zero-touch provisioning for autonomous cellular-IoTs in 5G networks," *Computer Communications*, vol. 216, pp. 324-345, 2024.

[16] N. K. S. Nayak and B. Bhattacharyya, "An Intrusion Detection System for 5G SDN Network Utilizing Binarized Deep Spiking Capsule Fire Hawk Neural Networks and Blockchain Technology," *Future Internet*, vol. 16, no. 10, p. 359, 2024.

[17] S. Alsubai, M. Umer, N. Innab, S. Shiaeles, and M. Nappi, "Multi-scale convolutional auto encoder for anomaly detection in 6G environment," *Computers & Industrial Engineering*, vol. 194, p. 110396, 2024.

[18] C. Kumar and M. S. A. Ansari, "An explainable nature-inspired cyber attack detection system in Software-Defined IoT applications," *Expert Systems with Applications*, vol. 250, p. 123853, 2024.

[19]T. Ghodsizad, "Internet of Medical Things with Considering of Artificial Intelligence," *International Journal of Sustainable Applied Science and Engineering*, vol. 1, no. 1, pp. 75-102, 2024.

[20] V. Tomer, S. Sharma, and M. Davis, "Resilience in the Internet of Medical Things: A Review and Case Study," *Future Internet*, vol. 16, no. 11, p. 430, 2024.

[21] F. R. Sultan, I. R. Abdelmaksoud, and H. M. El-Bakry, "Classification of DoS Attacks in IoT using Different Feature Selection Methods and Deep Learning," unpublished.

[22] D. Javeed, T. Gao, P. Kumar, and A. Jolfaei, "An explainable and resilient intrusion detection system for industry 5.0," *IEEE*

Transactions on Consumer Electronics, vol. 70, no. 1, pp. 1342-1350, 2023.

[23] S. Chatterjee, "Machine Learning and 5G Network Communication for Internet of Vehicles," unpublished.

[24] M. T. Masud, M. Keshk, N. Moustafa, I. Linkov, and D. K. Emge, "Explainable Artificial Intelligence for Resilient Security Applications in the Internet of Things," *IEEE Open Journal of the Communications Society*, 2024.