DDOS Detection In Software Defined Network Using Federated Learning

J.Mohamed Rashid [1], Dr.S.Peer Mohamed Ziyath[2]
[1, 2] Dept of Computer Application
[1, 2] B.S.Abdur Rahman Crescent Institute of Science and Technology, Chennai-73,Tamil nadu, India

Abstract- *Distributed Denial of Service attacks have become a great concern for security in Software Defined Networking(SDN), as they mostly overload centralized security mechanisms. In this work, a Federated Learning-Based Intrusion Detection System(FL-IDS) using Convolutional Neural Networks(CNN) and Long Short TermMemory(LSTM) networks is proposed. Clients train CNN-LSTM models locally on network traffic, preserving data privacy. The federated server aggregates these models securely, using differential privacy techniques. The trained global model is then deployed in SDN switches to analyze real-time traffic, with packets classified according to specific attributes: size, protocol type, and time intervals. Once an attack is detected, the system policy on the SDN switch is updated so that threats will be mitigated dynamically. By decentralizing intrusion detection, this approach increases accuracy while protecting sensitive data.*

Keywords- DDoS attacks, Software-Defined Networking (SDN), Federated Learning, Intrusion Detection System (IDS), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM)..

I. INTRODUCTION

Software-Defined Networking(SDN) centralized and programmed network administration has therefore opened doors to security vulnerabilities. This has especially included, among others, potential DDoS attacks, which pool amounts of traffic editors in an attempt to overwhelm network resources critical to the operation of the services being rendered within the organizational space. Conventional Intrusion Detection Systems (IDS) discover DDoS attacks with blind eyes and cannot retaliate, since they rely on data processing in a centralized way. This makes it much less effective against downstream and evolving attacks since we will perform this in a decentralized way that encompasses both security and scalability. Therefore, the work proposes a Federated Learning-Based Intrusion Detection System (FL-IDS) for the detection and mitigation of DDoS attacks in SDN environments. Unlike traditional models, this model allows various network nodes to locally train CNN and LSTM models on their traffic without exposing raw data. As it uses decentralized federated learning in its essence, it assures privacy, scalability, and real-time detection.

The system is expected to monitor the network traffic over time, during which it would gather key features to pick out the characteristics typical of that traffic, such as size of packets, type of protocol used, time intervals, and normal or malicious nature of network traffic. An attack would trigger the automatic update of the SDN controller through the dynamic changing of its security policies to block any malicious originating source.

II. LITERATURE SURVEY

[1] Srikar and Rao (2023) investigate the detection of DDoS attacks in SDN using optimized machine learning methods. Their study highlights the risks of single-controller SDN environments, which are susceptible to single-point failures and data compromise. They propose an optimized machine learning framework to enhance attack detection accuracy.They highlight the high risk factor associated with sensitive data and emphasize the vulnerability of a single controller, which can lead to data compromise and single-point failure.

[2] Rahim (2024) examines open-source SDN controllers, analyzing their current state, challenges, and potential solutions for future network providers. The study identifies a lack of robust mechanisms for detecting and mitigating cyberattacks, emphasizing the need for enhanced security measures in SDN.

[3] Chang (2024) explores the use of Federated Learning with DBSCAN for DDoS attack detection in SDN. While the approach offers improved privacy and scalability, the study highlights challenges such as high computational costs and sensitivity to parameter selection, which impact real-time detection efficiency.

[4] Nanda, Mishra, and Das (2022) present a privacy-preserving federated learning model for cybersecurity in IoT-enabled SDN environments. Their approach ensures secure model training while preserving data privacy, addressing

critical security concerns in distributed learning-based intrusion detection systems.

III. METHODOLOGY

1. **Requirement Analysis:**

- Identifies the need for an efficient DDoS detection mechanism in SDN.
- Defines functional requirements such as real-time attack detection, federated learning, and automated mitigation.Establishes non-functional requirements, including scalability, privacy, and computational efficiency.
- Analyzes existing security models and their limitations.

2. Design Phase:

- Defines the overall architecture of the SDN-based detection system.
- Designs a federated learning framework for distributed model training.
- Structures the CNN-LSTM-based model for traffic classification.
- Plans secure aggregation techniques for privacy-preserving learning.
- Outlines network simulation, data preprocessing, and visualization components.

3. Implementation Phase:

- Develops the SDN simulation with hosts, switches, and network traffic generation.
- Implements the CNN-LSTM model for attack detection.
- Integrates federated learning to train models on distributed data.
- Implements attack mitigation mechanisms for real-time threat response`.
- Develops logging and visualization tools for monitoring traffic and security status.

4. Testing Phase:

- Train and test the federated model using network traffic datasets to evaluate accuracy.
- Performs unit testing for individual components like packet forwarding and detection.Conducts integration testing to ensure

5. Deployment:

- Integrate the trained model into SDN controllers for real-time DDoS detection.
- Deploys the trained global model in a real or simulated SDN environment.
- Configures the federated learning setup across multiple distributed nodes.

3.1 Structure of the suggested work

The System Architecture describes the key components, including SDN controllers, federated clients, and the global server, while also explaining how local training occurs at the client level before models are securely aggregated at the server. The Methodology is categorized into three key phases: Requirement Analysis & Design, where the system requirements and architecture are identified; Implementation & Testing, involving the development of SDN simulation, model training, and evaluation; and Deployment, where the trained model is integrated into SDN controllers for real-time traffic analysis.

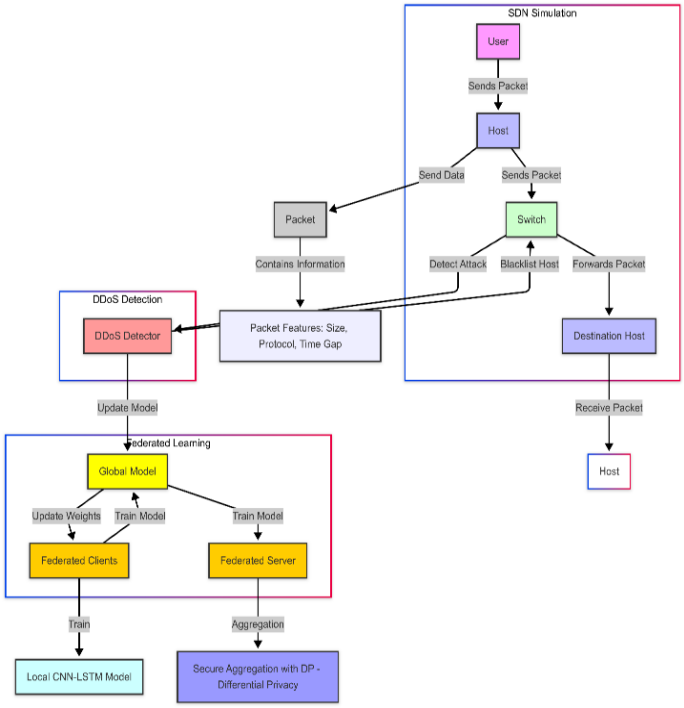


Fig. 1. The suggested work's organization

IV. SOFTWARE IMPLEMENTATION

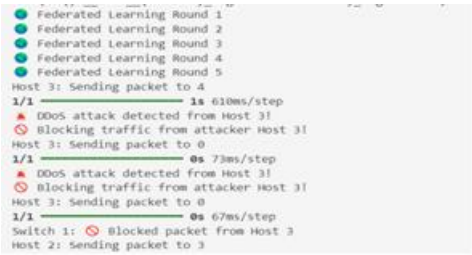
The software implementation of the project involves multiple components, including **network simulation, machine learning model development, federated learning integration, and real-time attack detection**. The key aspects of the software implementation are:

Development Environment & Tools

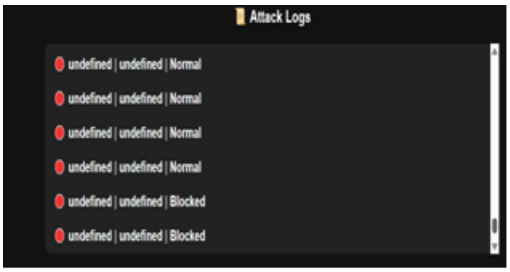
- **Programming Language:** Python (for machine learning and SDN simulation)
- **Deep Learning Frameworks:** TensorFlow/Keras for CNN-LSTM-based DDoS detection
- **Data Processing:** NumPy, Pandas for handling network traffic datasets
- **Visualization:** Matplotlib for real-time attack monitoring
- **Logging & Monitoring:** Python logging module for security event tracking

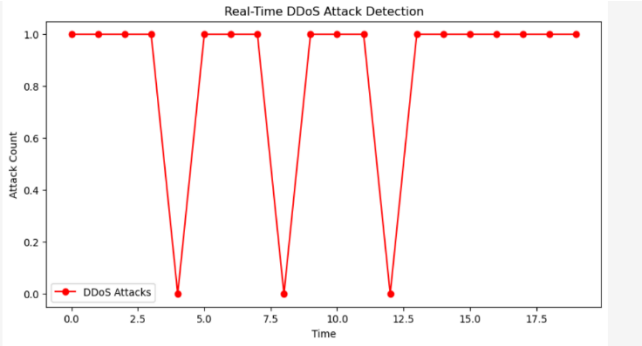
V. RESULT AND DISCUSSIONS

This project demonstrates the practicality of centralized CNN-LSTM-based federated learning as an effective technique for DDoS attack detection in SDN. The trained model obtained high accuracy in distinguishing between normal and attack traffic through CNN layers for spatial feature extraction and LSTM layers that analyze traffic in sequences. This federated learning allowed collaborative training of local models by many client computers, working together without compromising data privacy; secure aggregation guarantees that no single client data was revealed.and the visualization module further accounted for attack trend monitoring and dynamic viewing, sui-table for presentation to network administrators as an overview of threat activity.



Attack log





Graph attck Timeline

VI. EXISTINGAND PROPOSED TECHNIQUE

6.1 Existing techniques

Traditional DDoS detection and mitigation systems rely on centralized architectures, whereby a single Intrusion Detection System (IDS) or firewall analyzes network traffic in order to identify and block potential threats. These systems generally use signature-based or anomaly-based detection methods to classify malicious activities.

A signature-based process seems to rely on signature templates and attack patterns that are predefined and stored in a database. Incoming traffic could quickly be flagged as an attack if it matches an existing signature. This works great until it comes to zero-day or newly variant attacks, for which no valid predefined signature exists.

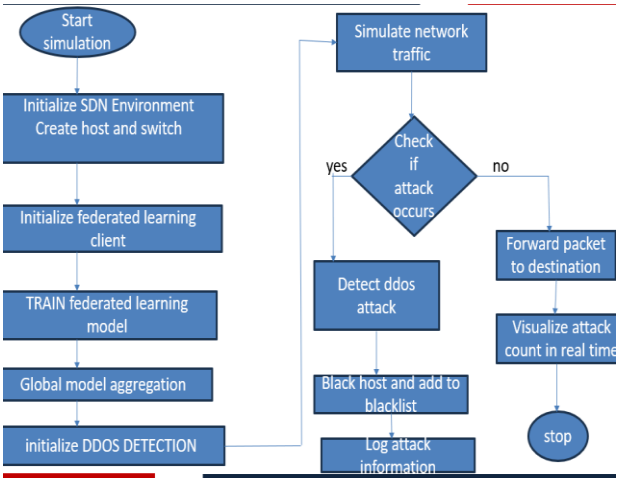
6.2 Proposed Technique

This system proposes a federated learning technique to detect Distributed Denial-of-Service (DDoS) attacks in a Software-Defined Networking (SDN) environment. Traditional intrusion detection techniques largely depend upon centralized paradigms which fail to address challenges regarding scalability, data privacy, and real-time traffic processing. This proposed system solves the above-mentioned challenges by introducing a decentralized learning framework, with multiple SDN switches acting as federated clients, wherein each switch will train its local Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) model with the respective network traffic data. The local models are then secure and contain aggregated training data on the main federated server for delivering the model to the controllers.

A global model is updated as one by securing aggregation; its deployment within SDN controllers makes packet classification possible in real time. The system extracts key features from network traffic: packet size, the type of

protocol, and time between packet arrivals to identify the class of traffic attacks: normal or malicious.

The SDN controller dynamically updates the switch's blacklist so that recursive enacting attacks are prevented from extending the damage for the mission-critical network infrastructure.



VII. CONCLUSION

This project proposes an artificial intelligence-aided federated learning-based detection system for distributed denial-of-service (DDoS) attacks on software-defined networks (SDN), using models of CNNs and LSTMs for real-time attack detection. The federated learning-based model on this system is able to learn/discover solutions from various clients without centralized.The CNN-LSTM models helped to effectively identify DDoS attacks through the spatial and temporal features of the network traffic that were extracted by the model, hence improving the model detection performance.

Federated learning involves training an ML model in such a way that the clients accumulate knowledge based on local traffic data and uses secure updates to aggregate hence improving the global model. In differential privacy-enabled secure aggregation, individual client data remains protected while gaining sufficient strength for model-laden training.

VIII. FUTURE SCOPE

Advancement of privacy and security within federated learning remains another important topic for this line of work. Approaches such as homomorphic encryption and SMPC for privacy-preserving training could be applied for mitigating the risk of downstream model poisoning attacks.

REFERENCES

[1] Sonda srikar , srinivisa Rao, Detection of DDoS attacks in SDN using Optimized Machine Learning Method.IJISAE 2023
[2] Johari rahim,Open-Source Software Defined Networking Controllers: State-of-the-Art, Challenges and Solutions for Future Network Provider.1EEE1 2024
[3] Yao chung chang, A Federated Learning Approach Using DBSCAN for DDoS Attack Detection MDPI 2024
[4] S. Nanda, P. K. Mishra, and S. K. Das, "Privacy-Preserving Federated Learning for Cybersecurity in IoT-Enabled SDN," Future Generation Computer Systems, vol. 130, pp. 91-102, (2022).
[5] Y. Zhang, G. Zhang, R. Gu, and J. Li, "A Hybrid Deep Learning Model for DDoS Attack Detection in SDN," 2020 IEEE International Conference on Communications **(ICC)**, Dublin, Ireland, pp. 1-6, (2020).
[6] H. M. Song, A. J. Alazab, and J. Wang, "A Federated Learning-Based Approach for Anomaly Detection in Software-Defined Networks," Journal of Network and Computer Applications, vol. 186, p. 103054, (2021).
[7] K. A. Al-Masri, F. Iqbal, A. Al-Nemrat, and A. A. Abu Hameed, "A Machine Learning-Based Approach for DDoS Attack Detection in SDN," IEEE Access, vol.\. 122495-122505, (2021)
[8] Doshi, B. D. Tran, and M. Kim, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," IEEE Transactions onConsumer Electronics, vol. 63, no. 4, pp. 426-434, (2017).