International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec – 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Cloud-Integrated Federated Learning Approach for Secure and Private Intrusion Detection in SDN Environment

Prof. Selvarani S*[1], Chethan G*[2], Jeevan B M*[3],Shalom Ruffus*[4],Chethan R*[5]

[1]*Assistant professor, Information Science and Engineering, R R Institute of Technology*
[2]*Student, Information Science and Engineering, R R Institute of Technology*
[3]*Student, Information Science and Engineering, R R Institute of Technology*
[4]*Student, Information Science and Engineering, R R Institute of Technology*
[5]*Student, Information Science and Engineering, R R Institute of Technology*

Abstract - Software Defined Networking (SDN) has significantly improved network flexibility by separating the control plane from the data plane and enabling centralized network management. However, this centralized architecture also introduces serious security challenges, making SDN controllers attractive targets for cyberattacks. Traditional intrusion detection systems (IDS) are often ineffective in SDN environments due to their reliance on centralized data collection and static detection mechanisms, which raise privacy and scalability concerns in cloud-based and multi-tenant networks.

Key Words: Software Defined Networking, Federated Learning, Intrusion Detection System, Cloud Security, Explainable AI.

1. INTRODUCTION

Software Defined Networking (SDN) has transformed modern network management by decoupling the control plane from the data plane and enabling centralized, programmable control. This architectural shift allows network administrators to efficiently manage traffic flows, implement dynamic policies, and deploy new services with minimal effort. SDN is widely adopted in cloud data centers and large-scale enterprise networks due to its flexibility and scalability.

Despite these advantages, SDN introduces new security vulnerabilities. The centralized SDN controller becomes a high-value target for attackers, exposing the network to threats such as controller hijacking, flow-rule manipulation, and distributed denial-of-service (DDoS) attacks. Traditional intrusion detection systems, which were designed for static and distributed networks, struggle to adapt to the dynamic and programmable nature of SDN. Moreover, centralized IDS approaches require collecting raw traffic data from multiple domains, leading to increased communication overhead and serious privacy concerns.

2. METHODOLOGY AND SYSTEM DESIGN

2.1 Problem Statement and Motivation

Software Defined Networking introduces centralized control and programmability, which simplifies network management but also exposes new security vulnerabilities. The SDN controller acts as a single point of control, making it an attractive target for attacks such as Distributed Denial of Service (DDoS), flow-rule manipulation, probing, and controller hijacking. Traditional intrusion detection systems rely heavily on centralized data collection and static rule-based detection, which are not suitable for the highly dynamic and distributed nature of SDN environments.

In cloud and multi-tenant networks, centralized IDS solutions also raise serious privacy concerns, as raw traffic data from multiple organizations must be transferred to a central server. This leads to increased communication overhead, regulatory challenges, and potential data leakage. Moreover, signature-based IDS approaches fail to detect zero-day and evolving attacks effectively. These limitations highlight the need for a scalable, adaptive, and privacy-preserving intrusion detection mechanism for SDN.

2.2 Federated Learning–Based Intrusion Detection Approach

Federated Learning (FL) is a distributed machine learning paradigm that enables multiple participants to collaboratively train a global model without sharing raw data. In the proposed system, federated learning is applied to intrusion detection in SDN to preserve privacy while leveraging diverse traffic patterns from multiple domains.

Each SDN domain acts as a federated client and locally trains an intrusion detection model using its own flow-level traffic features. Instead of transferring sensitive traffic data, only the trained model parameters or gradients are sent to a cloud-based aggregation server. The cloud server performs federated aggregation, such as Federated Averaging (FedAvg), to compute a global model. This global model is then redistributed to all participating SDN domains for further training and inference.

2.3 System Architecture

The proposed cloud-integrated federated intrusion detection system is organized into four logical layers: the SDN Client Layer, Cloud Federated Learning Layer, Application and Visualization Layer, and Persistence Layer.

At the SDN Client Layer, each SDN domain collects traffic flow statistics from switches or controllers. These features are preprocessed using a common scaler and used to train a local intrusion detection model. The trained local model weights are periodically shared with the cloud aggregation server.

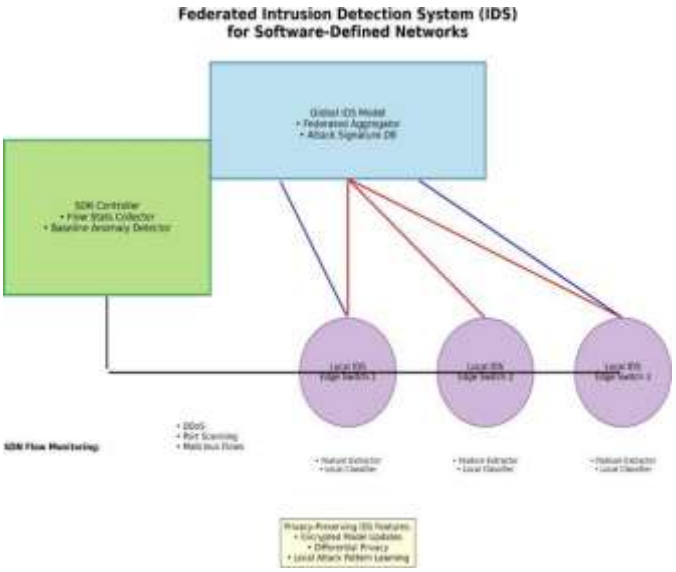

Fig - 1: System Architecture

The Cloud Federated Learning Layer is responsible for coordinating the federated learning process. It aggregates model updates received from multiple SDN domains and generates a global intrusion detection model. This layer also hosts the explainability module, which computes SHAP values for model predictions to provide interpretability.

2.4 Intrusion Detection Workflow and Explainability

Once the global model is trained, it is deployed for intrusion detection across participating SDN domains. Incoming traffic features are classified into normal or attack categories such as DDoS, probing, brute-force, or application-layer attacks. Along with the predicted label, the system generates a confidence score indicating the reliability of the prediction.

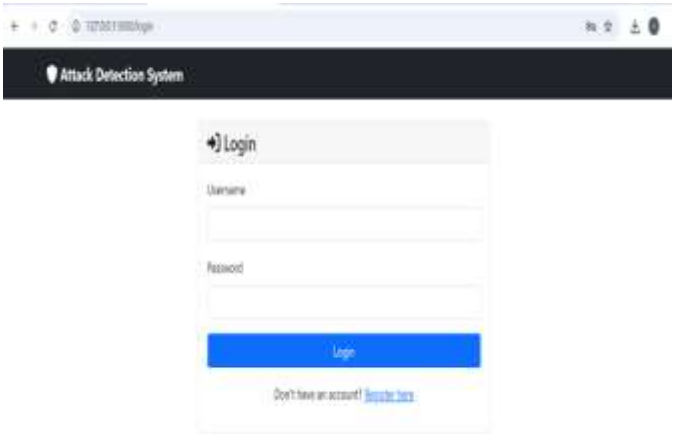

Fig - 2: Login Page

To improve transparency and trust, the system integrates Explainable Artificial Intelligence (XAI) using SHAP (SHapley Additive exPlanations). SHAP analyzes the contribution of each input feature to the final prediction and visually highlights the most influential factors. This enables security analysts to understand why a particular traffic flow was classified as malicious and supports informed decision-making for network mitigation actions.

2.5 Performance Evaluation Setup

The proposed system was evaluated using standard intrusion detection datasets commonly used in SDN research. Key performance metrics such as accuracy, precision, recall, and F1-score were used to assess the effectiveness of the federated model. Experimental results demonstrate that the federated learning-based IDS achieves high detection accuracy while maintaining low inference latency suitable for near real-time deployment.

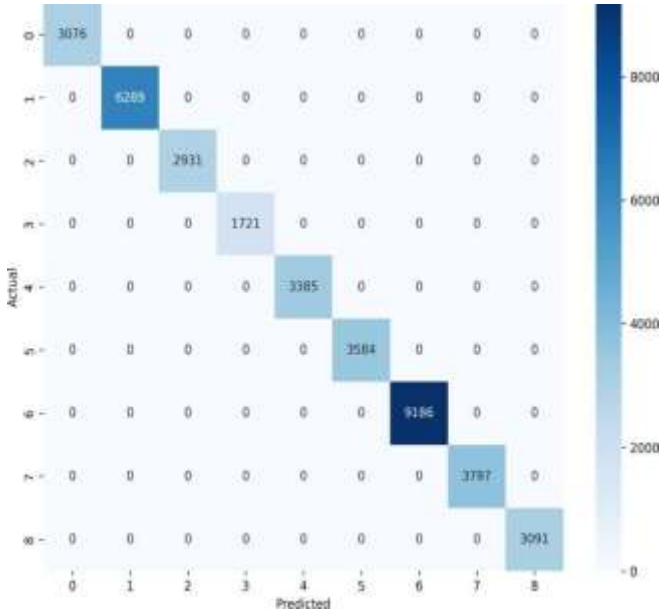

Fig - 3: Confusion Matrix

Batch prediction experiments confirmed the system's scalability, as large volumes of traffic data were processed efficiently without performance degradation. Furthermore, federated training ensured that raw traffic data never left local SDN domains, validating the privacy-preserving nature of the system. The inclusion of SHAP-based explanations added significant value by enhancing interpretability without compromising performance.

3. RESULTS AND DISCUSSION

The proposed federated intrusion detection system was evaluated using benchmark SDN intrusion datasets. Experimental results show that the federated global model achieves high detection accuracy across multiple attack categories while maintaining low inference latency suitable for real-time deployment. Batch prediction experiments demonstrate that the system can efficiently handle large volumes of traffic data without performance degradation.

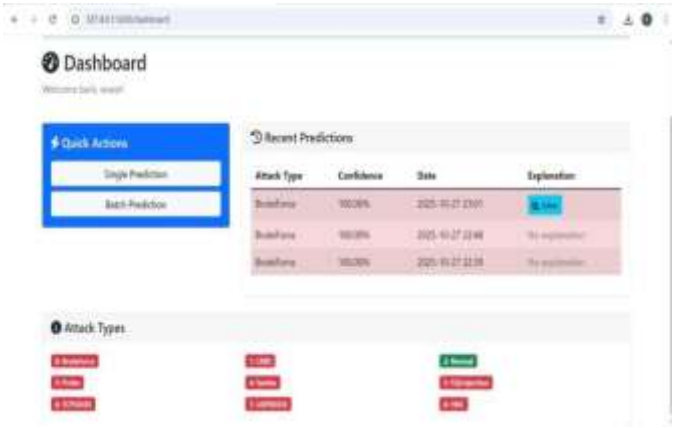

Fig - 4: Dashboard

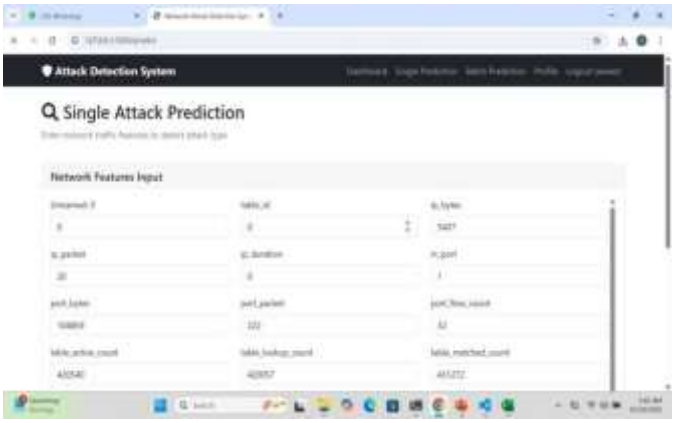

Fig - 5: Prediction Page

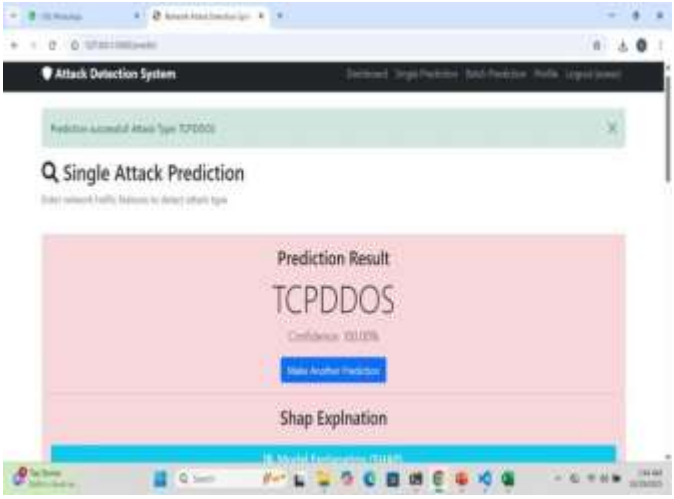

Fig - 6: Result Page

The integration of SHAP-based explainable AI provides valuable insights into model decisions by highlighting the most influential features contributing to each prediction. This improves the interpretability of the system and helps security analysts understand and trust the detection outcomes. Additionally, federated learning ensures that sensitive network traffic data never leaves local SDN domains, effectively addressing privacy and regulatory concerns. Overall, the results confirm that the proposed approach offers a balanced combination of accuracy, privacy, scalability, and transparency.

4. CONCLUSIONS

This project presents a cloud-integrated federated learning approach for secure and privacy-preserving intrusion detection in Software Defined Networking environments. By decentralizing model training and leveraging collaborative learning, the proposed system overcomes the limitations of traditional centralized IDS solutions. The integration of explainable AI further enhances transparency and usability, enabling informed security decisions. The experimental results demonstrate the effectiveness of the system in detecting intrusions while preserving data privacy. This approach provides a strong foundation for future research and deployment of intelligent, privacy-aware security solutions in modern SDN and cloud infrastructures.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the Department of Information Science and Engineering, RR Institute of Technology, for providing the necessary support and resources to carry out this project successfully.

REFERENCES

[1] M. Raza, M. A. Khan, and M. A. Jan, “Federated learning for privacy preserving intrusion detection in software defined networks,” *IEEE Access*, vol. 12, pp. 1–15, 2024.

[2] A. A. Abd Al-Ameer and W. S. Bhaya, “Enhanced intrusion detection in software-defined networks through federated learning and deep learning,” *Journal of Network and Systems Management*, vol. 31, pp. 1– 17, 2023.

[3] A. A. Abd Al-Ameer and W. S. Bhaya, “Intelligent intrusion detection based on multi-model federated learning for software defined network,” *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 2, pp. 88–101, 2023.

[4] V. S. Naresh and D. Ayyappa, “Enhancing security in software defined networks: Privacy-preserving intrusion detection with homomorphic encryption,” *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 1, pp. 245–255, 2025.

[5] J. Wang et al., “NIDS-FGPA: A federated learning network intrusion detection algorithm based on secure aggregation of gradient similarity models,” *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 12789–12805, 2024.

[6] B. Olanrewaju-George and B. Pranggono, “Federated learning-based intrusion detection system for Internet of Things using unsupervised and supervised deep learning models,” *Computers and Security*, vol. 139, p. 103423, 2024.

[7] R. Agarwal, S. Gill, and S. Chauhan, “Federated learning for intrusion detection system: Concepts, challenges and future directions,” *Journal of Cloud Computing*, vol. 11, pp. 1–22, 2022.

[8] A. Alsamiri and R. Alsaqour, “Federated learning for intrusion detection systems in Internet of Vehicles: A general taxonomy, applications and future directions,” *IEEE Access*, vol. 11, pp. 56390–56410, 2023.

[9] P. Belenguer, Y. Li, and J. Kim, “A review of federated learning applications in intrusion detection systems,” *Future Internet*, vol. 17, pp. 1–28, 2025.