iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2026 **Issue:** Conference **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83169

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com
National Conference on Integrated Approaches to Sustainable Innovation 2026 (IASI 2026)

An Explainable Federated Learning-Based Intrusion Detection and Mitigation Framework for MultiController Software-Defined Networks

Ankita Das[1], Rukshan Khatun[2], Sukriti Santra[3]
Artificial Intelligence and Machine Learning Department, OmDayal Group of Institutions

Abstract: ***Software-Defined Networking (SDN) supports centralized policy enforcement through the separation of control and data planes. Nevertheless, SDN controllers are still susceptible to complex attacks such as Distributed Denial of Service(DDoS), port scanning, and probing attacks. Conventional centralized intrusion detection systems are prone to scalability issues, privacy issues, and single points of failure in multi-controller settings. In this paper, we present an explainable federated learning-based intrusion detection system (IDS) for multi-controller SDN networks. Each controller maintains a multilayer perceptron (MLP) classifier trained on flowlevel data and jointly learns a global model using the Flower framework without exchanging raw data, addressing privacy and communication overhead issues. Explainable Artificial Intelligence (XAI) enables security analysts to develop adaptive mitigation strategies within the SDN control plane. Experimental results on the InSDN dataset show 99% accuracy on prominent attack categories with robustness to non-IID data distributions, providing an efficient, interpretable, and privacy-preserving solution for securing largescale SDN networks.***

Keywords: Software Defined Networking, Intrusion Detection System, Federated Learning, Privacy, Explainable-AI, Network Security

I. INTRODUCTION

SDN has emerged as a revolutionary paradigm in modern network architecture, fundamentally transforming network design and management through the separation of the control and data planes [1]. This architectural innovation provides unprecedented programmability, flexibility, and centralisation, making SDN attractive for large-scale deployments in data centres, cloud networks, and enterprise environments [2]. The centralised controller maintains a global network view and governs distributed switches through standardised protocols such as OpenFlow, enabling sophisticated traffic engineering and dynamic load balancing [3]. However, centralisation creates critical vulnerabilities, making controllers high-value targets for sophisticated cyberattacks. Once compromised, attackers can manipulate network behaviour, exfiltrate sensitive information, or disrupt entire network infrastructures [4]. SDN networks face diverse threats, including DDoS attacks that flood controllers with excessive packet-in requests, saturating resources and rendering networks unresponsive and port scanning attacks that exploit flow installation mechanisms to discover topology and vulnerabilities [5]. Multi-controller architectures address scalability and single-point-offailure risks by distributing control across network segments [6].

Machine learning and deep learning approaches have shown significant promise for intrusion detection in SDN environments, enabling the learning of complex attack patterns and adaptation to evolving threats [7]. Federated learning has emerged as a privacy-preserving machine learning paradigm that enables collaborative model training across distributed nodes without requiring centralization of raw data, offering a compelling solution for multi-controller SDN environments [8]. The black-box nature of deep learning models raises concerns about trustworthiness, interpretability, and operational understanding of detection decisions, as security analysts require transparency into why specific traffic flows are classified as malicious [9].To address these challenges XAI techniques, particularly SHapley Additive exPlanations (SHAP), provide mathematically rigorous frameworks for interpreting machine learning model decisions, transforming opaque classifiers into transparent tools that support human decision-making and enable automated generation of context-aware mitigation strategies[10].

This paper addresses the critical gap in SDN security by proposing a comprehensive explainable federated learning-based intrusion detection and mitigation framework specifically designed for multi-controller SDN architectures.

©IJRASET: All Rights are Reserved

The main contributions of this study are:

1) We propose a federated learning-based intrusion detection framework for multi-controller SDN architectures that enables distributed controllers to collaboratively train MLP classifiers using local flow-level features while learning a global model through the Flower framework without sharing raw traffic data, ensuring privacy preservation and reducing communication overhead.

2) Integration of SHAP-based XAI to provide interpretable insights into model predictions at both global and attack-specific granularities. SHAP explainability has been systematically leveraged to drive adaptive, context-aware mitigation strategies directly within the SDN control plane for dynamic threat responses.

3) Development of an attack-aware mitigation mechanism that translates explainability insights into actionable security policies. The framework automatically generates and deploys mitigation rules based on feature importance analysis, enabling proactive and targeted defense mechanisms tailored to specific attack patterns.

4) Comprehensive experimental evaluation on the InSDN benchmark dataset to assess the framework's effectiveness in multi-class attack detection, robustness under non-IID data distributions, and the impact of federated learning configurations on model convergence and detection performance in realistic multi-controller SDN environments.

The remaining contents of this paper are organized as follows: Section 2 reviews the related work, Section 3 describes in detail the proposed methodology, Section 4 analyzes the experimental results, and Section 5 concludes the research by summarizing the results of the work and potential future research opportunities.

II. LITERATURE REVIEW

In this section, the authors reviewed related work in various relevant areas. The review covers security vulnerability in SDN, IDS in SDN, federated learning and explainable AI based IDS, and mitigation strategies in SDN-based IDS. They have been illustrated in section 2.1 to 2.4.

A. Review of the Related Work on Security Vulnerability in SDN

Badotra et al. examined the security threats of distributed SDN controllers. Their research was primarily on Distributed Denial of Service (DDoS) attacks in which attackers overwhelm the controller with redundant requests[11]. They demonstrated that such attacks are able to saturate controller CPU and memory resulting in network unavailability. Their study, however, was limited to the performance degradation. It lacked an intrusion detection system or mitigation system to prevent the DDoS attack within real time. Kanwal et al. examined the general threat picture of SDN controller structures[12].

They have talked about some of the attacks such as control-plane DDoS attacks, spoofing attacks, malicious flow rule injection, and man-in-the-middle attacks among the SDN elements. The centralized controller is an extensive target, which is clearly depicted with their work. Nevertheless, this was an analytical piece of work that did not put any attack detection or defense response into practice or test. Arevalo-Herrera et al. paid attention to the weaknesses in SDN controllers and OpenFlow communication[13]. They dealt with controller saturation attacks, flow rule manipulation and control-plane exploitation attacks. In their survey, they also examined datasets and detection methods found in the previous literature. They emphasized that the majority of studies involve the use of old datasets and controllers. Nevertheless, their study did not suggest any viable IDS or mitigation model of these attacks. Das et al. suggested a 5G network security framework based on blockchain-enabled SDN[14]. Their work was primarily focused on man-in-the-middle attacks, controller impersonation, and unauthorized access attacks based on smart contract-based authentication. The architecture enhanced interconnection between SDN controllers. Though, it did not deal with traffic-based attacks like DDoS or packet flooding and it did not involve any intrusion detection mechanism.

B. Review of the Related Work on IDS in SDN

Toony et al. suggested an ML-based intrusion detection system of SDN-based IoT networks[15]. Their system was aimed at identifying DDoS attacks, botnet attacks, and coordinated multi-target attacks based on flow-level facilities and multi-target ensemble learning. The framework demonstrated good accuracy in detecting IoT datasets. The model was however demanding centralized data collection and high computational power. It has not covered the question of privacy and implementation in distributed SDN controller systems. Cui et al. proposed a hybrid CNN-BiLSTM with attention-based hybrid CNN-BiLSTM IDS to be applied to SDN [16].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Their analysis was aimed at identifying various types of attacks, such as DDoS, Botnet, Web attacks, and U2R attacks through the InSDN dataset. The model was very precise in classifications. The method however depended on centralized training and failed to address the aspect of privacy protection or scaling in the multi-controller SDN settings. Zainudin et al. suggested a federated learning-inspired IDS based on low complexity in SDN-based industrial cyber-physical systems[17]. Their contribution covered DDoS attacks, probing attacks and spoofing attacks and limited the amount of computational overhead by use of feature selection. Even though the direction enhanced the efficiency and privacy, it primarily targeted the industrial CPS setting and never assessed explainability or attack interpretation at the controller level. Raza et al. have created a federated learning-based IDS of SDN to identify a multi-class attack in a cyberattack, such as DoS, DDoS, brute-force, and infiltration attacks[8]. Their strategy ensured data privacy whereby there was no centralized data dissemination and it performed better than the conventional centralized IDS. But there were no explainable AI methods that were used in the work, and it was hard to see why the traffic was deemed to be malicious by the network operators. Nguyen et al. suggested a FedNIDS, which is a Federated Intrusion Detection System built on packets[18]. The framework dealt with both existing and new attacks such as zero-day attacks and evasion attacks, where they shared models updates over distributed networks. Although FedNIDS was more robust in detection and privacy, it does not specifically integrate with SDN controllers and control-plane attack mitigation, being designed to be applied to a general network. Chetouane et al. proposed a continuous federated learning IDS of SDN edge computing[19].

The model centered on their system which sought to detect DDoS as well as on developing patterns of attacks by continually updating the IDS model whenever new attacks emerge. This enhanced customizability and confidentiality. Nevertheless, the framework lacked explainability of the attack and involved complicated interactions between clients and controllers.

C. Review of the Related Work on Federated Learning and Explainable-AI-based IDS in SDN

Prasad et al. introduced a XAI architecture to present threat detection in multicast systems based on SDN[20]. They employed a hybrid CNN-LSTM model and combined with LIME and SHAP in the explanation of detection results. Their work largely covered DDoS attacks, manipulation of packets and threat of data leakage with multicast traffic. The architecture enhanced the network administrators with transparency. Nevertheless, the paper did not consider the federated learning, privacy preservation, or multicontroller SDN environments, but only multicast situations. Laghari et al. , in their work proposed SIoV-DS is a zero-trust IDS, based on SDN, in Internet of Vehicles (IoV) environments [21]. To explain their work, they used their system based on Variational Autoencoder (VAE) and EX-LSTM and SHAP. The model identified DoS, spoofing, and malware attacks within intra-vehicle, inter-vehicle and infrastructure layers. Although the methodology was highly accurate and explained well, it was specific to the case of the IoV and it did not consider federated training involving multiple SDN controllers. Asiri et al. suggested Federated EXi, a federated learning system with SHAP to identify DDoS attacks in IoT edge networks[22]. They worked on ensuring that both data and federated models were available against performance degradation due to DDoS. The methodology offered descriptive explanations on model behavior under attack conditions. Nonetheless, the framework was tested in the environment of the IoT edges only and was not combined with SDN controllers and control-plane traffic analysis. Fatema et al. have suggested FEDXAIIDS, which is a federated explainable intrusion detector based on ANN and SHAP[23]. Their work covered several network-layer attacks, such as DDoS, DoS, brute-force, and infiltration attacks, and ensured the privacy of data by using federated learning. The most significant features that led to attacks were also determined in the model. Nonetheless, the system was tested with a broad IoT data set and never specifically incorporated SDN-related peculiarities, control-plane attacks, or real-time controller deployment. Tserenkhuu et al. suggested an IDS model of SDN-based IoT networks based on deep learning feature selection using the XAI tool[24]. They dealt with DoS and DDoS, malware, probing, and brute-force attack and applied SHAP and Random Forest feature importance to minimize the number of features. The high detection accuracy was attained in the framework. Nevertheless, the method was based on the centralized model training and failed to apply federated learning and distributed SDN controller security.

D. Review of the Related Work on Attack Mitigation in SDN

Alashhab et al. suggested an online machine learning-based ensemble detecting and mitigating DDoS, low-rate DDoS, and zeroday DDoS attack in SDN[25]. Their system also participates in an online learning mode that is constantly informed by the live traffic to update the detection model. Mitigation follows detection of an attack, which involves installation of flow rules at the controller to reject malicious traffic. The method was very successful in detecting very high accuracy on various SDN datasets. Nevertheless, it primarily discussed DDoS-type attacks and did not look at multi-controller SDN environments and explainability of mitigation

decisions. Dogan et al. is a systematic literature review concerning ML- and DL-based detection and mitigation methods in SDN[26]. Their research examined a huge amount of literature covering DDoS, DoS, spoofing, probing, malware attacks and classified the methods used to mitigate the problems as traffic rate limiting, flow rule updates, and controller reconfiguration. The authors emphasized that the majority of the current mechanisms of mitigation are reactive, and they have difficulties with real-time implementation, scalability, and coordination with various controllers. Nevertheless, the piece of work did not suggest a specific mitigation framework. Ohri et al. suggested a blockchain-based security system to alleviate attacks in the multi-SDN controllers setting [27]. They primarily focused on DoS attacks, spoofing attacks, and authentication attacks through Ethereum smart contracts and Proof-of-Work consensus. The blockchain provided access control and avoided unauthorized interactions with the controllers. As much as the improvement resulted in trust and resilience, it lacked the implementation of traffic level intrusion detection and machine learning based mitigation against large scale attacks like DDoS.

E. Research Gap

Badotra et al. examined the DDoS attacks on distributed SDN controllers and demonstrated the extreme consumption of controller resources but the study did not include real-time intrusion detection and mitigation strategies[11]. Toony et al. introduced an MLbased IDS to SDN-based IoT networks with a high detection rate, but their method failed to follow the principle of scalability and privacy concerns in multi-controller SDN settings [15]. Raza et al. have discussed privacy in the context of federated learningbased SDN IDS but their framework lacked explainable AI, which is why the decisions made by the detection are challenging to interpret by the network operators [8]. Prasad et al. incorporated explainability in SHAP into SDN intrusion detection enhancing transparency, albeit in centralized and single-controller deployment with no federated learning [20]. The framework offered by Alashhab et al. was an online ML-based SDN-based DDoS detection and mitigation system, but it targeted only DDoS attacks and was not concerned with multi-controller coordination and explainable decision-making of mitigation [21]. These gaps suggest that there is no singular solution that can help with privacy-saving federated learning, explainable intrusion detection, and adaptive mitigation in the context of multi-controller SDN.

F. Problem Domain

The research gap analysis and literature review shows the inefficiency of an effective system to store and synchronize the federated learning model parameters, intrusion detection decision, and SHAP-generated explainability across distributed controllers in multi-controller SDN settings. Current solutions lack the ability to save essential security artifacts like local and global model weights, attack classification records and explainability data when controllers fail or switch domains. Consequently, intrusion detection functions tend to need retraining due to controller disruption, which causes more downtime and uneven security policies. To overcome these issues, the developed framework proposes secure model that preserve constancy of federated learning models and explanation-based mitigation regulations throughout learning rounds and controller breakdowns. The architecture facilitates the synchronized detection models and mitigation policies using authenticated synchronization between distributed controllers without compromising the privacy of collected data because the raw traffic is local to each controller. It allows one to recover reliably, ensure consistent security, and engage in joint learning in dynamic multi-controller SDN settings.

III. PROPOSED METHODOLOGY

The suggested framework works in multi-controller SDN settings whereby the InSDN dataset[28] is first cleansed and processed into a form of exploratory data analysis to identify key flow-level characteristics. The dataset is then divided into nonIID distributions in order to mimic the conditions of the heterogeneous network under the realism of three clients with each controller controlling a different traffic pattern and attack distribution. Every controller is a federated client, where it trains an MLP-based intrusion detection model on its partitions of data, and then cooperates with one another through a federated server which accumulates updates to the models with the FedAvg algorithm, but without exchanging actual traffic data. SHAP-based explainability is then used to explain both global and attack-specific detection decisions using features that explain the most. Lastly, a dynamically translated XAI-directed mitigation module converts these insights on feature importance dynamically into specific OpenFlow rules executed in the SDN control plane and targeted to neutralize any threats detected in a context-sensitive fashion. The entire methodology can be formalized by four main algorithms: Algorithm 1 uses local training as implemented on the client-side, where the controllers are expected to optimize the global model on the local data of the domain, Algorithm 2 implements the

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

coordination of federated aggregation of all the distributed controllers, which is necessary to implement collaborative learning, Algorithm 3 calculates SHAP values to give explainable reasoning about the model predictions, and Algorithm 4 converts explainability knowledge into adaptive attack-sensitive mitigation strategies executed through OpenFlow rules.

Algorithm 1: Local Client Training
Input: Global model parameters θ_{global}, Local dataset D_{local}
Output: Updated local parameters θ_{local}, Dataset size $|D_{local}|$, Training loss L_{train}
1. Initialize local model with global parameters: $\theta_{local} \leftarrow \theta_{global}$
2. For each local training epoch do
3. For each mini-batch (X, y) in D_{local} do
4. Compute predictions: $\hat{y} \leftarrow f_\theta(X)$
5. Calculate loss: $L \leftarrow CrossEntropy(\hat{y}, y)$
6. Compute gradients: $\nabla\theta \leftarrow \partial L/\partial\theta$
7. Update parameters: $\theta \leftarrow \theta - \alpha\nabla\theta$
8. End For
9. End For
10. Evaluate model on local data
11. Calculate accuracy and precision metrics
12. Return θ_{local}, $|D_{local}|$, L_{train}

Algorithm 2: Federated Server Orchestration
Input: Number of rounds R, Minimum clients C_{min}
Output: Final global model θ_{global}, Metrics history M
1. Initialize global model θ_{global} randomly
2. For round t = 1 to R do
3. Wait for at least C_{min} clients to connect
4. Broadcast θ_{global} to selected clients
5. For each client k in parallel do
6. Receive local updates (θ_k, $|D_k|$, L_k) from CLIENT_TRAIN 7. End For
8. Aggregate models using FedAvg: $\theta_{global} \leftarrow \Sigma(|D_k|/N) \times \theta_k$
9. Evaluate global model and collect metrics
10. Store round statistics in M
11. End For
12. Return θ_{global}, M

Algorithm 3: SHAP Value Computation
Input: Model f, Background data B, Instances to explain $X_{explain}$
Output: SHAP values matrix Φ
1. Initialize DeepExplainer with model f and background data B
2. Compute expected values E[f(B)] over background
3. Select N instances from $X_{explain}$
4. For each instance x do
5. For each feature i do
6. Compute SHAP value $\varphi_i(x)$ using marginal contributions
7. End For
8. End For
9. Return Φ (SHAP values for all classes, instances, and features)

Algorithm 4: XAI-Guided Mitigation Action Generation
Input: SHAP values Φ, Detected instance x, Predicted class c
Output: Mitigation action A

1. Extract SHAP values for predicted class: φ_c ← Φ[c][x]
2. Rank features by absolute SHAP values
3. Select top K = 3 most important features
4. If 'packets_per_second' is in top features then
5. Install rate limiting rule
6. Else if 'destination_port_count' is in top features then
7. Block source IP for specified duration
8. Else if 'inter_arrival_time' is in top features then
9. Apply probabilistic packet dropping
10. Else if 'bytes_per_packet' is in top features then
11. Redirect traffic to deep packet inspection
12. Else
13. Generate alert only
14. End If
15. Translate action A into OpenFlow rule
16. Install flow table entry with high priority
17. Log mitigation with timestamp and SHAP justification
18. Return A

IV. RESULT

A non-IID distribution of traffic among controllers is used to experiment on a multi-controller SDN testbed. The application of Federated training is based on the Flower framework, whereas SHAP-based explainable AI is used to explain detection decisions and drive transparent mitigation.

A. Federated Learning Performance Evaluation

The convergence behavior of the proposed federated learning framework is shown in Fig. 1 and Fig. 2. Client-level accuracy steadily improves across federated rounds, while training loss consistently decreases, indicating stable local learning under nonIID data conditions. The global model loss, illustrated in Fig. 3, shows smooth and monotonic convergence, confirming effective aggregation and model stability across distributed SDN controllers. Overall detection accuracy of the global model is close to 99% along with balanced precision, recall, and F1-score.

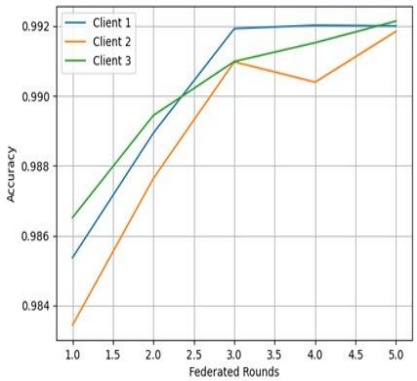


Fig. 1. Client accuracy vs. federated rounds

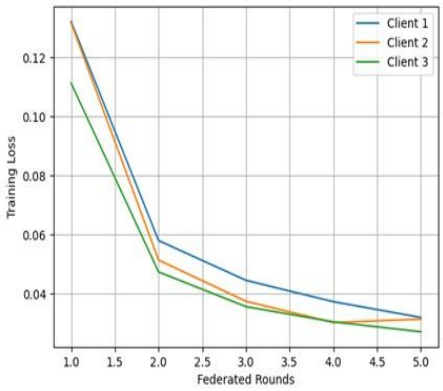


Fig. 2. Client training loss vs. federated rounds

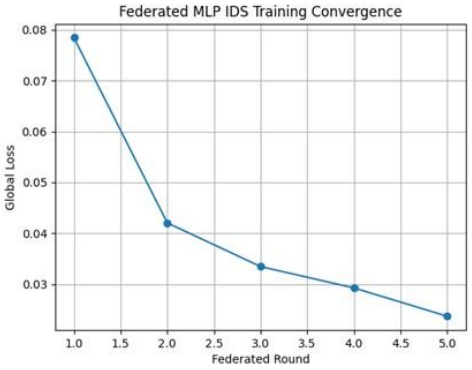


Fig. 3. Global model loss vs. federated rounds

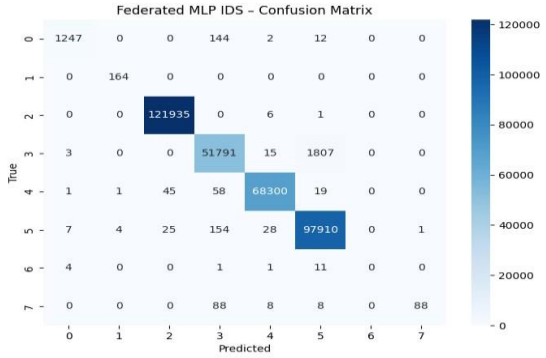


Fig. 4. Confusion matrix of multi-class attack detection

B. Multi-Class Attack Detection Results

The multi-class detection capability of the federated MLP-based IDS is presented using the confusion matrix in Fig. 4. The results show strong diagonal dominance, indicating high classification accuracy across normal and attack classes. High-volume attacks such as DDoS are detected with particularly high accuracy, while limited confusion is observed among structurally similar attack categories. Overall, the results demonstrate that the proposed IDS generalizes well across multiple attack types in a federated SDN setting.

C. Multi-Class Attack Detection Results

To improve transparency, SHAP-based explainability is applied to analyze model decisions. The global SHAP feature importance plot in Fig. 5 shows that destination port, source port, protocol, and flow-level statistics are the most influential features in intrusion detection. A class-wise SHAP analysis for DDoS attacks, shown in Fig. 6, highlights features related to traffic rate and header characteristics, which are consistent with known DDoS behavior. These explanations validate that the model relies on meaningful traffic features and supports explainability-driven mitigation.

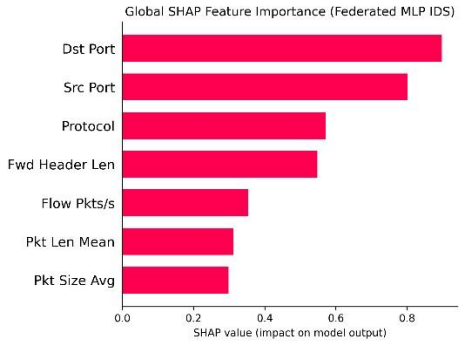


Fig. 5. Global SHAP feature importance

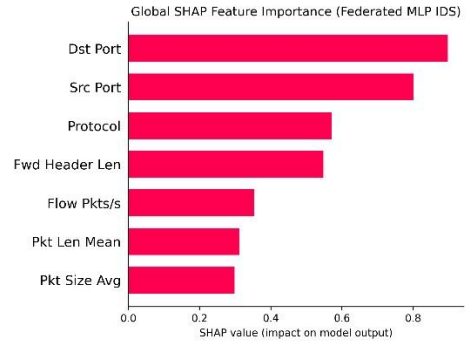


Fig. 6. Class-wise SHAP feature importance for DDoS

The findings indicate that the suggested structure can be used to attain credible federated convergence, effective multi-class intrusion detecting, and meaningful explainability. Federated learning maintains the privacy of data across the distributed SDN controllers, whereas SHAP-based explanations can be used to make interpretable and actionable choices on security. The properties render the framework applicable to the implementation in dynamic multi-controller SDN environments.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

V. CONCLUSION

The paper proposed a federated learning seen framework of intrusion detection and mitigation in multi-controller SDN environments, which is explainable. The developed methodology combines federated learning and SHAP-based explainability to deal with the problem of scalability and privacy of SDN security and transparency. The results of the experiments confirm that the framework is highly sensitive to detect big network attacks and give understandable explanations of the decisions of the models. This category of explainability is directly used to create XAI-inspired, attack-specific mitigation responses, which allow the SDN controller to implement context-driven OpenFlow policy. Connecting detection, explanation, and mitigation, the framework increases the level of trust in the operations and minimizes the use of fixed defense policies. The next step in work will be real-time deployment in SDN controllers and combining blockchain-based trust sharing between distributed controllers.

VI. ACKNOWLEDGMENT

The authors of this article acknowledge research support provided by Department of Artificial Intelligence and Machine Learning, OmDayal Group of Institutions, Uluberia, Howrah for their work.

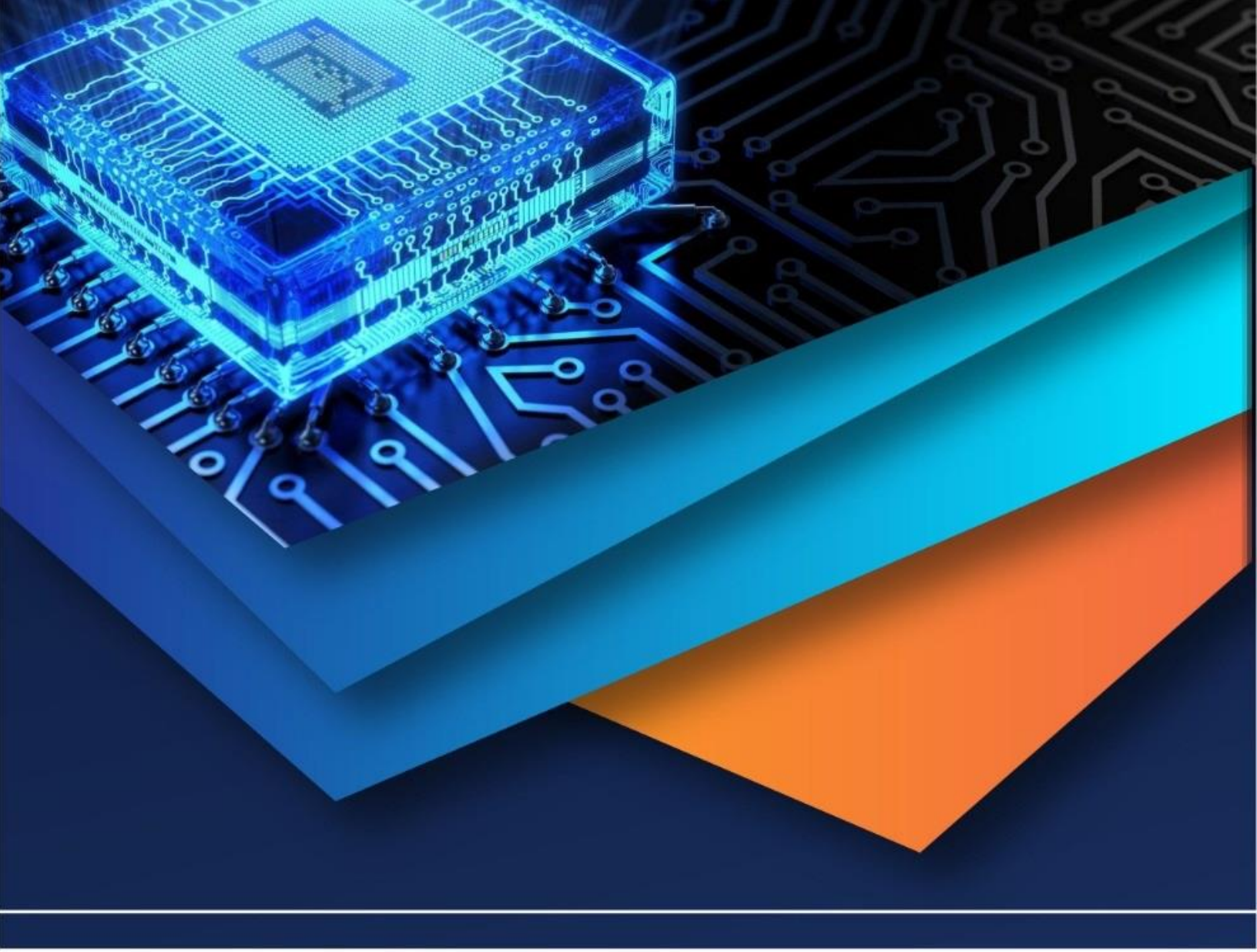
REFERENCES

[1] Adhikari, T., Khan, A. K., & Kule, M. (2025). An analytical review of security issues in centralized and distributed SDN environments. Information Security Journal: A Global Perspective, 34(6), 713–746.
[2] Batewela, S., Liyanage, M., Zeydan, E., Ylianttila, M., Ranaweera, P.: Security Orchestration in 5G and Beyond Smart Network Technologies. IEEE Open Journal of the Computer Society 6, 554–573 (2025).
[3] Bhuiyan, Z.A., Islam, S., Islam, M.M., Ullah, A.B.M.A., Naz, F., Rahman, M.S.: On the (In)Security of the Control Plane of SDN Architecture: A Survey. IEEE Access 11, 91550–91582 (2023).
[4] Wang, J., Wang, L.: SDN-Defend: A Lightweight Online Attack Detection and Mitigation System for DDoS Attacks in SDN. Sensors 22, 8287 (2022).
[5] Kim, J., Seo, M., Lee, S., Nam, J., Yegneswaran, V., Porras, P., Gu, G., Shin, S.: Enhancing Security in SDN: Systematizing Attacks and Defenses from a Penetration Perspective. Computer Networks 241, 110203 (2024).
[6] Badotra, S., Gurusamy, M.: SecuNet 4D: A Comprehensive Framework for Distributed SDN Security and Resilience. Scientific Reports 15, 15996 (2025).
[7] Aslam, N., Srivastava, S., Gore, M.M.: A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN. Arabian Journal for Science and Engineering 49, 3533–3573 (2024).
[8] M. Raza, M. Jasim Saeed, M. B. Riaz and M. Awais Sattar, "Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks," in IEEE Access, vol. 12, pp. 69551-69567, 2024
[9] Preety Prasad, Mohammad Tahir, Jouni Isoaho, Enhancing Explainability of Artificial Intelligence for Threat Detection in SDN-based Multicast Systems,Procedia Computer Science,Volume 257 ,Pages 569-574,ISSN 1877-0509, 2025
[10] Lundberg, S.M., Lee, S.-I.: A Unified Approach to Interpreting Model Predictions. In: Advances in Neural Information Processing Systems, vol. 30, pp. 4765–4774 (2017)
[11] Badotra, S.; Tanwar, S.; Bharany, S.; Rehman, A.U.; Eldin, E.T.; Ghamry, N.A.; Shafiq, M. A DDoS Vulnerability Analysis System against Distributed SDN Controllers in a Cloud Computing Environment. Electronics, 11, 3120, 2022.
[12] A. Kanwal, M. Nizamuddin, W. Iqbal, W. Aman, Y. Abbas and S. Mussiraliyeva, "Exploring Security Dynamics in SDN Controller Architectures: Threat Landscape and Implications," in IEEE Access, vol. 12, pp. 56517-56553, 2024
[13] Arevalo-Herrera, J., Camargo Mendoza, J., Martínez Torre, J.I. et al. Assessing SDN Controller Vulnerabilities: A Survey on Attack Typologies, Detection Mechanisms, Controller Selection, and Dataset Application in Machine Learning. Wireless Pers Commun 140, 739–775 (2025)
[14] Debashis Das, Sourav Banerjee, Kousik Dasgupta, Pushpita Chatterjee, Uttam Ghosh, and Utpal Biswas,Blockchain-Enabled SDN Framework for Security Management in 5G Applications. In: Proceedings of ICDCN 2023. ACM (2023)
[15] Ahmed A. Toony, Fayez Alqahtani, Yasser Alginahi, Wael Said, MULTI-BLOCK: A novel ML-based intrusion detection framework for SDN-enabled IoT networks using new pyramidal structure, Internet of Things, Volume 26, 101231, ISSN 2542-6605, 2024
[16] Cui, M., Chen, J., Qiu, X. et al. Multi-class intrusion detection system in SDN based on hybrid BiLSTM model. Cluster Comput 27, 9937–9956 (2024).
[17] A. Zainudin, R. Akter, D. -S. Kim and J. -M. Lee, "Federated Learning Inspired Low-Complexity Intrusion Detection and Classification Technique for SDN-Based Industrial CPS," in IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2442-2459, 2023
[18] Quoc H. Nguyen, Soumyadeep Hore, Ankit Shah, Trung Le, and Nathaniel D. Bastian. 2025. FedNIDS: A Federated Learning Framework for PacketBased Network Intrusion Detection System. Digital Threats 6, 1, Article 4 (2025)
[19] Chetouane, Ameni, and Kamel Karoui. "New Continual Federated Learning System for Intrusion Detection in SDN-Based Edge Computing." Concurrency and Computation: Practice and Experience 37.2, e8332, 2025
[20] Preety Prasad, Mohammad Tahir, Jouni Isoaho, Enhancing Explainability of Artificial Intelligence for Threat Detection in SDN-based Multicast Systems, Procedia Computer Science, Volume 257, Pages 569-574, ISSN 1877-0509, 2025.
[21] Muddasar Laghari, Yuanchang Zhong, Muhammad Junaid Tahir, Muhammad Adil, SIoV-IDS: SDN-enabled zero-trust framework for explainable intrusion detection in IoVs using Variational Autoencoders and EX-LSTM, Journal of Network and Computer Applications, Volume 245, 104389, ISSN 1084-8045, 2026.
[22] A. Asiri, W. Wang, F. Wu, H. Vo and S. Yu, "FedXAI for Detecting DDoS on IoT Edge Networks in Federated Learning," 34th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, 2024, pp. 1-6, 2024.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[23] Fatema, K., Dey, S. K., Anannya, M., Khan, R. T., Rashid, M. M., Su, C., & Mazumder, R. Federated XAI IDS: An Explainable and Safeguarding Privacy Approach to Detect Intrusion Combining Federated Learning and SHAP. Future Internet, 17(6), 234, 2025
[24] M. Tserenkhuu, M. D. Hossain, Y. Taenaka and Y. Kadobayashi, "Intrusion Detection System Framework for SDN-Based IoT Networks Using Deep Learning Approaches With XAI-Based Feature Selection Techniques and Domain-Constrained Features," in IEEE Access, vol. 13, pp. 136864-136880, 2025.
[25] A. A. Alashhab et al., "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," in IEEE Access, vol. 12, pp. 51630-51649, 2024
[26] Doğan, S.M., Koçak, A. & Alkan, M. Detection and mitigation of cyber-attacks in software defined networks using machine learning/deep learning: a systematic literature review, research challenges and future directions. Int. J. Inf. Secur. 24, 209 (2025)
[27] Ohri, P., Daniel, A., Neogi, S.G. et al. Blockchain-based security framework for mitigating network attacks in multi-SDN controller environment. Int. j. inf. tecnol. 17, 5591–5603 (2025).
[28] Elsayed, Mahmoud & Le-Khac, Nhien-An & Jurcut, Anca. (2020). InSDN: A Novel SDN Intrusion Dataset. IEEE Access.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)