Dynamic Trust-Weighted Federated Aggregation for Robust DDoS Detection in Cloud-Edge Networks

[1]Dr.A. Peter Soosai Anandaraj, [2]Dr.S.Hemalatha

[1]Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia, [2]Panimalar Engineering College, Chennai;

[1]karunya.ieeeproj@gmail.com,[2]pithemalatha@gmail.com

Abstract

Cloud-edge networks are seriously threatened by Distributed Denial-of-Service (DDoS) attacks. Intrusion Detection Systems (IDS) based on Federated Learning (FL) allow privacy-preserving collaborative learning, although they are still susceptible to poisoning attempts and malicious model updates. A Dynamic Trust-Weighted Federated Aggregation (DTWFA) architecture for reliable DDoS detection is presented in this paper. Based on detection accuracy, update consistency, and past behavior, the framework gives participating edge nodes trust scores. These scores are then incorporated into the federated aggregation process. DTWFA increases resilience against adversarial attacks and improves detection performance by lessening the impact of faulty nodes. In dynamic cloud-edge scenarios, experimental results show better robustness, reduced false-positive rates, and superior accuracy when compared to traditional FedAvg-based FL techniques.

Keywords: ***Federated Learning, DDoS Detection, Intrusion Detection System, Cloud-Edge Computing, Trust-Based Aggregation, Model Poisoning.***

1. Introduction

While real-time services have improved due to the growing use of cloud-edge and IoT technology, DDoS attacks have become more likely. Privacy-preserving intrusion detection is made possible by Federated Learning (FL), although traditional FedAvg is susceptible to malicious and erratic client updates. The suggested Dynamic Trust-Weighted Federated Aggregation (DTWFA) addresses this by allocating trust scores according to past behavior, update consistency, and detection accuracy. DTWFA increases detection accuracy, lowers false positives, and fortifies resilience to poisoning assaults while protecting data privacy by granting trustworthy nodes more power.

2. Literature Review

Ref.	Domain / Sub-Domain	Target Environment	Objective	Techniques Used	Key Challenges	Research Gap	Future Direction
1. Lilhore et al. (2026)	IoT Security / FL & Anomaly Detection	Edge IoT	Secure FL and anomaly detection	Blockchain, FL, CNN-LSTM, trust	Attacks, privacy, overhead	Limited integrated security	Lightweight, real-time FL

2. Bhagyalakshmi et al. (2026)	WSN Security / Trust-aware FL	Resource-constrained WSN	Accurate anomaly detection	CNN-GRU, FedTrust, Top-k, client selection	Energy, unreliable links	Trust, energy and accuracy not jointly optimized	Adaptive lightweight FL
3. Alandjani (2025)	IIoT Security / Trust & Quantum Security	Industrial IoT	Secure quantum-resistant FL	MARL, blockchain, PQC, FL	Quantum attacks, scalability	Limited unified quantum-trust FL	Scalable PQC and MARL
4. Tariq et al. (2024)	FL Security / Trust & Client Selection	Edge/Distributed FL	Select reliable clients	DQN, trust, data quality	Poor data, unreliable clients	Limited joint trust-data optimization	Adaptive client selection
5. Jha & Bhargavi (2025)	Secure FL / Trust & Anomaly Detection	Distributed FL	Detect malicious updates	Dynamic trust, anomaly detection, robust aggregation	Poisoning, scalability	Limited adaptive trust mechanisms	Adaptive attack-resistant FL

3. Method, Experiments and Results

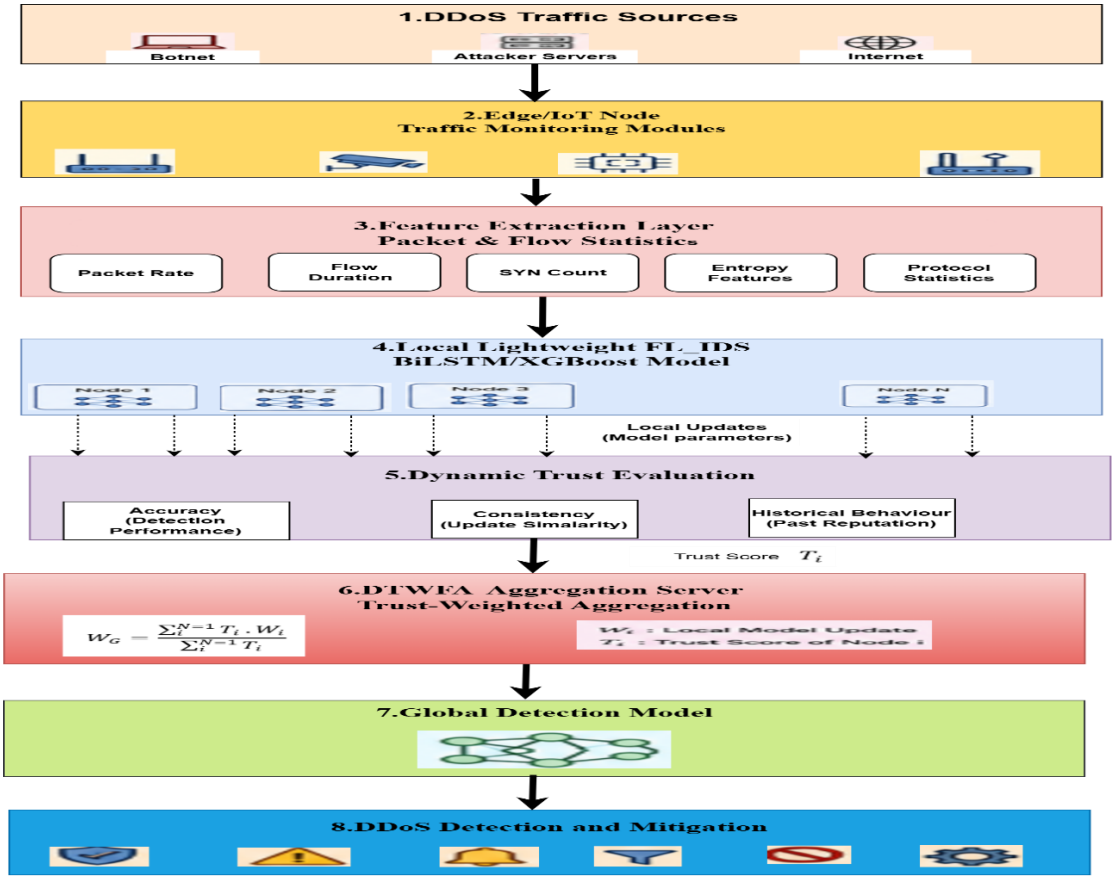


Fig.3.1. Workflow of the Proposed DTWFA-Based Intrusion Detection System

In a cloudedge setting, several edge nodes can cooperatively train a DDoS detection model without exchan ging raw network data thanks to the suggested Dynamic TrustWeighted Federated Aggregation (DTWA) fr amework, protecting privacy.While each edge node conducts local training and simply transmits model upd ates, the cloud server initialises and distributes the global model.Based on detection accuracy, update consis tency, and past behaviour, the server determines a dynamic trust score for every client.While suspicious or l owtrust updates are downweighted or eliminated, hightrust clients are given higher aggregation weights.For upcoming training cycles until convergence, the aggregated model is sent back to reliable edge nodes.DT WFA increases resistance to poisoning and Byzantine attacks, decreases false positives, and increases the a ccuracy of DDoS detection.

3.1 Dynamic Trust-Weighted Federated Aggregation (DTWFA)

The traditional FedAvg, which assumes all clients are reliable and primarily weights client updates based on local data size, is replaced by the suggested DTWFA. FedAvg is hence susceptible to fraudulent

and subpar updates.DTWFA uses historical reliability, update consistency, and detection accuracy to determine a dynamic trust score for each client. After that, the global model is aggregated by assigning suspicious clients lower weights and trusted clients higher weights.Therefore, in cloud-edge DDoS detection, DTWFA increases model accuracy, lowers false positives, and fortifies defence against poisoning and Byzantine attacks.

- The conventional FedAvg aggregation is given by:

$$FedAvg = \sum \frac{N_i}{N} W_i$$

3.2 Traffic Monitoring and Feature Extraction

Key statistical characteristics, including packet rate, SYN packet count, flow duration, connection frequency, source IP entropy, and protocol statistics, are extracted from each edge node's monitoring of local network traffic. For the purpose of training local DDoS detection models, these features are normalised into vectors. Federated learning minimises communication overhead and protects privacy by sharing just model updates.

3.3 Local Lightweight DDoS Detection

During this stage, each edge node uses extracted network properties to locally train a lightweight IDS model, protecting sensitive data. Sequential and aberrant DDoS patterns are effectively detected using lightweight BiLSTM, Autoencoder, and XGBoost models. Only the updated model parameters are forwarded to the federated server for aggregation following local training, which lowers communication overhead and permits scalable, privacy-preserving DDoS detection.

3.4 Dynamic Trust Computation

During this stage, the suggested methodology assigns a dynamic trust score to each participating edge node in order to assess its dependability. The suggested method evaluates each node's reliability before including its model update into the global aggregation process, in contrast to traditional federated learning techniques that handle all client updates identically. This method reduces the impact of malicious or untrustworthy individuals on the global model.

The trust score for the *i*th edge node is computed as

$$T_i = \alpha A_i + \beta B_i + \gamma H_i$$

where (A_i) represents the local detection accuracy, indicating how accurately the node classifies normal and DDoS traffic using its local validation data.. Large deviations may indicate abnormal or poisoned model

updates. (H_i) represents the historical reliability, reflecting the node's long-term contribution and trustworthy behavior over multiple communication rounds. The coefficients (alpha), (beta), and (gamma) are weighting factors that determine the relative importance of each trust component, with (\alpha + \beta + \gamma = 1).

3.5 Trust-Weighted Federated Aggregation

In this stage, Dynamic Trust-Weighted Federated Aggregation (DTWFA) is used to combine local models from participating edge nodes. In contrast to FedAvg, DTWFA gives nodes with strong trust scores larger weights and nodes that are dubious or untrustworthy lower weights. In order to improve model accuracy,

convergence, and resistance to poisoning attempts, the aggregated global model is then distributed to all edge nodes for the subsequent training cycle.
The global model parameters are computed as:

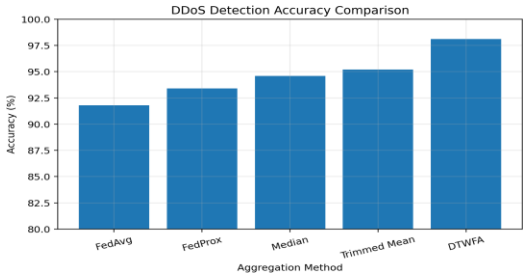
$$W_G = \frac{\sum_{i=1}^{n} T_i W_i}{\sum_{i=1}^{n} T_i}$$

where **(** W_i **)** represents the local model parameters learned by the *i*th edge node, **(** T_i **)** denotes the corresponding dynamic trust score, and **(**W_G **)** is the aggregated global model. The trust score acts as a weighting factor, determining the contribution of each node during model aggregation.

4. Experimental results

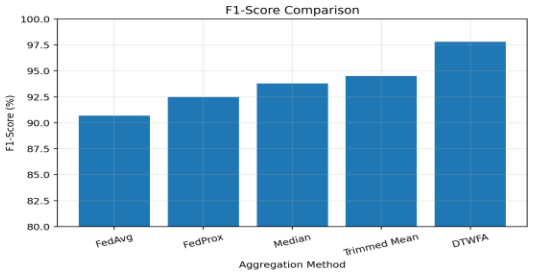
1. Accuracy comparison

DDoS Detection Accuracy Comparison. Illustrative comparison of federated aggregation methods under a poisoning-attack scenario.



2. F1-Score Comparison

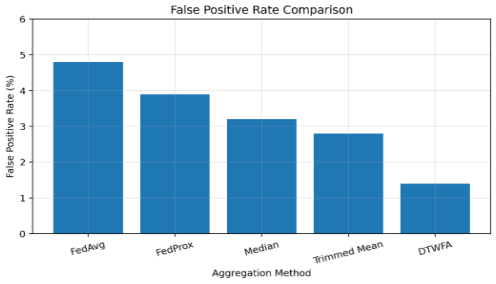
Illustrative F1-score comparison between conventional and trust-aware federated aggregation methods.



3. False Positive Rate

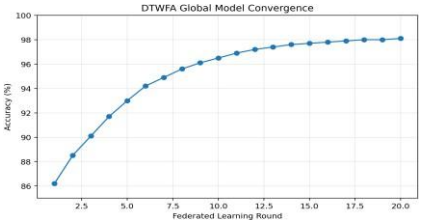
False Positive Rate Comparison

Illustrative false-positive rates for different federated aggregation methods



4. DTWFA convergence

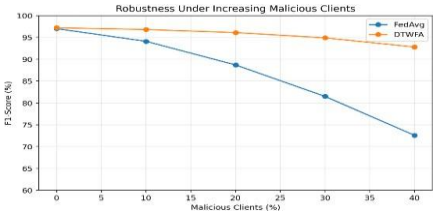
The following is the type of convergence graph you should generate from your results after running the code .DTWFA Global Model Convergence. Illustrative global accuracy across federated learning rounds.



5. Robustness against malicious clients

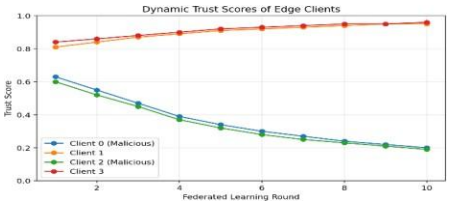
This is one of the most important graphs for your DTWFA paper, because your main contribution is

resistance to poisoning/Byzantine clients. Robustness Under Increasing Malicious Clients. Illustrative F1-score degradation as the proportion of malicious clients increases.



6. Dynamic trust scores

This graph demonstrates the central idea of your DTWFA methodology: malicious clients should progressively receive lower trust scores.Illustrative evolution of trust scores across federated learning rounds.



5. References

[1] M. G. Camila, "A Multi-Tenant Cloud Security Framework Using Zero-Trust Architecture and AI-Based Anomaly Detection," *American International Journal of Computer Science and Technology*, vol. 6, no. 4, pp. 1–13, Jul. 2024, doi: 10.63282/3117-5481/AIJCST-V6I4P101.

[2] N. Mathivanan and B. Lanitha, "An integrated methodology for intrusion detection and mitigation to optimize cloud security," *Journal of Cloud Computing*, vol. 15, no. 18, 2026.

[3] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam and O. M. Elkomy, "Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2523-2537, March 2022, doi: 10.1109/TITS.2021.3119968.

[4] Abubakar, A. A., Liu, J., & Gilliard, E. (2023). An efficient blockchain- based approach to improve the accuracy of intrusion detection systems. Electronics Letters, 59(18), e12888,doi.org/10.1049/ell2.12888.

[5] Ceviz, O., Sadioglu, P., Sen, S., & Vassilakis, V. G. (2025). A novel federated learning-based IDS for enhancing UAVs privacy and security. Internet of Things, 31, 101592, doi.org/10.1016/j.iot.2025.101592.

[6] G. Karatas, O. Demir and O. Koray Sahingoz, "Deep Learning in Intrusion Detection Systems," *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, Ankara, Turkey, 2018, pp. 113-116, doi: 10.1109/IBIGDELFT.2018.8625278.

[7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam and M. Shorfuzzaman, "Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11,
pp. 8065-8073, Nov. 2022, doi: 10.1109/TII.2022.3161631.

[8] Q. -A. Huang and Y. -W. Si, "A Trust-Based Privacy-Preserving Data Retrieval Scheme in Edge-Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2026.3662007.

[9] Mahdi Hosseini, S., Broumandnia, A. & Karimi, R. Blockchain-enabled hybrid evolutionary scheduling for cloud resource optimization. Computing 108, 4 (2026) https://doi.org/10.1007/s00607-025-01574-0.