TRUSTFED-SDN

A PRIVACY-PRESERVING AND VERIFIABLE FEDERATED LEARNING FRAMEWORK FOR CROSS-TENANT THREAT DETECTION IN SDN-ENABLED CLOUD NETWORKS

Pritom Kumar Bhowmik (2101005), MD Naimur Rashid (2101042)
Supervised By: Saurav Chandra Das, Lecturer, Department of IRE, UFTB

1. Introduction

- **Problem**: SDN multi-tenant clouds need collaborative threat detection, but tenants don't trust each other with their data.
- **Solution**: Federated Learning (FL) addresses this by enabling joint training of an intrusion detection model across tenants, where only model updates are shared instead of raw network traffic data.
- **Gap**: No existing SDN-FL work combines real testbed validation, verifiable aggregation, poisoning robustness, and adaptive privacy together.
- **Proposal**: TrustFed-SDN—tested on a real Mininet+OVS+RYU testbed, with verifiable aggregation, poisoning-robust defense, and adaptive differential privacy.

2. Related Work

Ref/Year	Core Contribution	Limitation
Wang & Wang (HFHE-Cloud, 2026)	Selective homomorphic encryption for FL privacy on cloud platforms; 94.25% accuracy.	No real SDN testbed, no verifiability, no poisoning robustness. Only 13% encryption overhead even after optimization
Mateus & Lusilao Zodi (2024)	LSTM-based FL for DDoS detection, 99.96–99.99% accuracy on CICIDS2019.	Dataset-driven simulation only, no real network emulation, no privacy or robustness mechanism
Uddin & Kumar (2023)	Only reviewed work with a real Mininet+OVS+RYU SDN testbed for FL.	Plain weight averaging, no verifiability, no DP, accuracy only 79.47%
Ali et al. (2023)	Weighted FL for DDoS detection in SDN control plane, 98.85% accuracy.	Weights fixed by manual hit-and-trial tuning, no SDN emulation, no privacy/verifiability

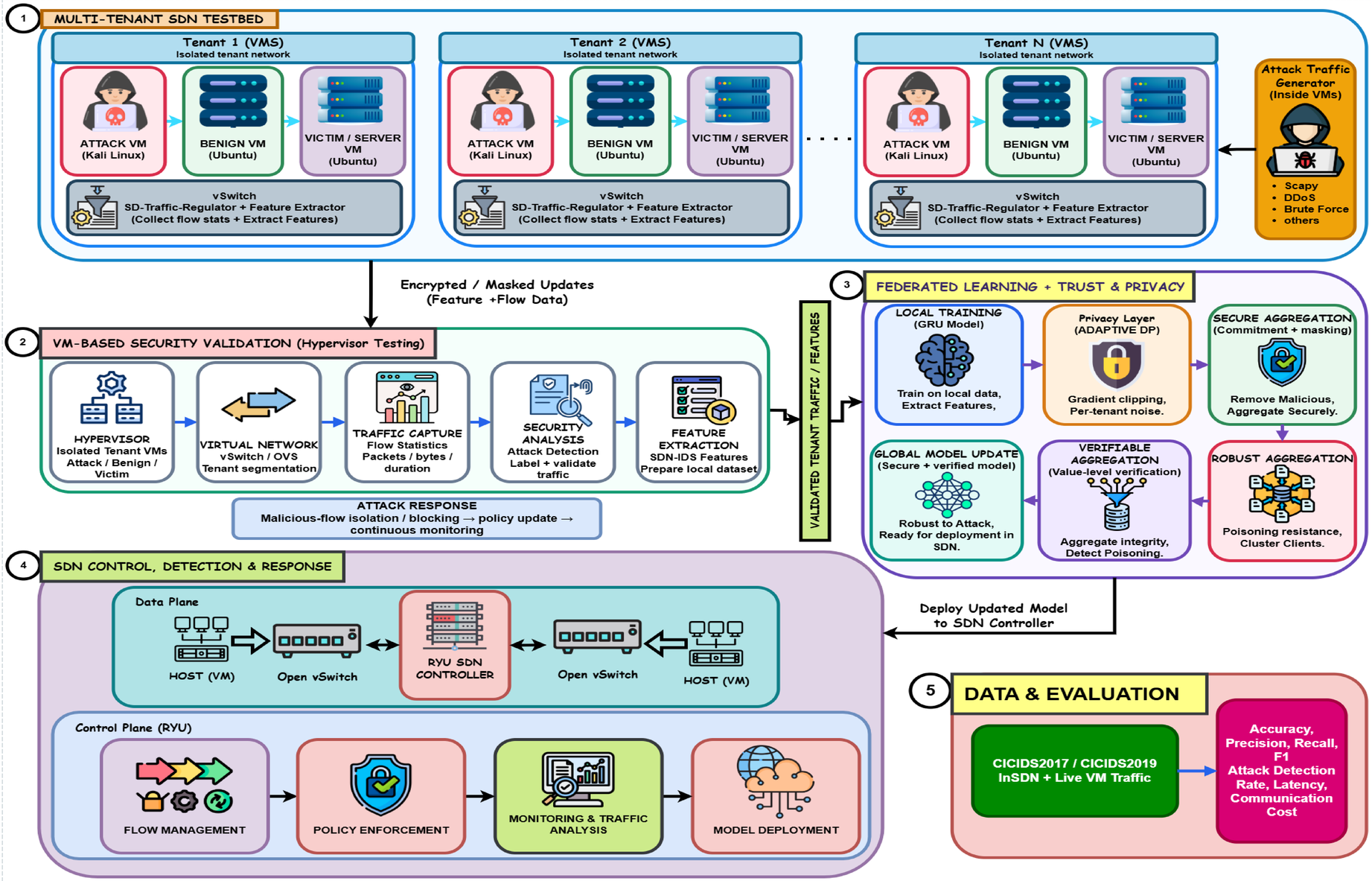
3. Research Gap

- **No real SDN testbed + verifiable aggregation combined:** prior works either use a real network testbed or verifiable aggregation, never both together.
- **Poisoning/Byzantine robustness rarely validated on live SDN traffic:** most robustness mechanisms are tested only on generic/toy datasets (MNIST, CIFAR), not real network flows.
- **Adaptive per-tenant differential privacy is missing:** existing methods apply uniform noise across all tenants, ignoring each tenant's individual data sensitivity.

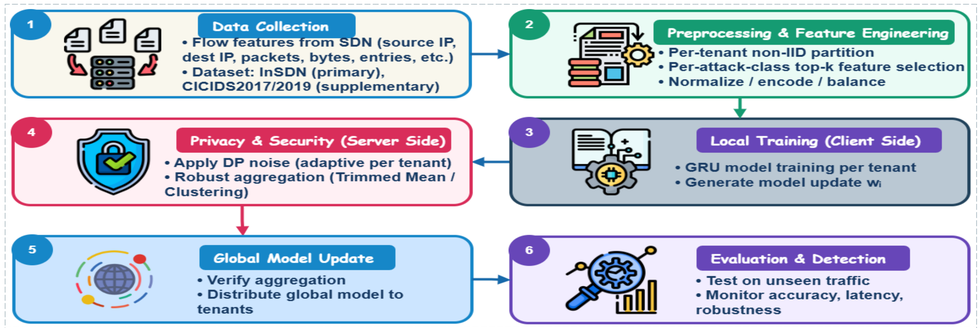
4. Objectives

1. **SDN-integrated FL architecture:** Design an SDN-integrated FL architecture with VM-isolated tenants (Attack VM/Benign VM/Victim VM per tenant), giving each tenant genuine hypervisor-level isolation.
2. **Poisoning-robust aggregation:** Design and evaluate coordinate-wise trimmed mean and similarity clustering, tested against label-flipping, backdoor, and gradient-scaling attacks.
3. **Full testbed evaluation:** Provide component-wise ablation evaluation (FedAvg → +DP → +Robust Agg → +Verifiable Agg → Full TrustFed-SDN) on a real SDN testbed.

5. Methodology



6. Workflow



7. References & QR Code

[1] J. Wang and Y. Wang, "Privacy Protection Optimization Method for Cloud Platforms Based on Federated Learning and Homomorphic Encryption," Sensors, vol. 26, no. 3, p. 890, 2026. DOI: 10.3390/s26030890

[2] J. Mateus and G.-A. Lusilao Zodi, "Federated Learning-Based Solution for DDoS Detection in SDN," in Proc. 2024 Int. Conf. Comput., Netw. Commun. (ICNC), Cape Town, South Africa, 2024. DOI: 10.1109/ICNC59896.2024.10556115

[3] H. Zhou, G. Yang, Y. Huang, H. Dai, and Y. Xiang, "Privacy-Preserving and Verifiable Federated Learning Framework for Edge Computing," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 565–580, 2023. DOI: 10.1109/TIFS.2022.3227435

[4] R. Uddin and S. A. P. Kumar, "SDN-Based Federated Learning Approach for Satellite-IoT Framework to Enhance Data Security and Privacy in Space Communication," IEEE J. Radio Freq. Identif., vol. 7, pp. 424–440, 2023. DOI: 10.1109/JRFID.2023.3279329

[5] M. N. Ali, M. Imran, M. S. ud din, and B.-S. Kim, "Low Rate DDoS Detection Using Weighted Federated Learning in SDN Control Plane in IoT Network," Appl. Sci., vol. 13, no. 3, p. 1431, 2023. DOI: 10.3390/app13031431

https://trustfed.naimurrashid.dev/