Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 10 March 2026
Revised 15 April 2026
Accepted 18 May 2026

Natural Resources for Human Health 2026, Vol. 6 (1s): 39–44

KEYWORDS:
Distributed Denial-of-Service, Federated Learning, Network Function Virtualization.

Mitigating DDOS Attacks in Virtualized Network Functions (VNF) Using Federated Learning: A Privacy-Preserving Collaborative Defense

Dr. Anurag Golwalkar[1], Shyam Patel[2], Vandana Birle[3], Chetan K. Verma[4], Dr. Bharat Pahadiya[5]

[1]Indore Institute of Science & Technology, Indore
[2]Medicaps University, Indore
[3]Medicaps University, Indore
4MBIT, CVM University, Anand
[5]Medicaps University, Indore
[1]agolwelkar@gmail.com
[2]eng.shyampatel@gmail.com
[3]vandana.birle@medicaps.ac.in
[4]er.chetan85@gmail.com
[5]bharat.pahadiya@medicaps.ac.in

ABSTRACT: The rapid integration of Network Function Virtualization (NFV) in 5G-Advanced and 6G infrastructures has introduced significant security vulnerabilities, most notably in Distributed Denial-of-Service (DDoS) attacks. Modern DDoS threats have evolved into sophisticated multi- vector campaigns that leverage AI to bypass traditional static defenses. This paper proposes a novel framework for DDoS mitigation using Federated Learning (FL). Unlike centralized AI models that require the transfer of sensitive network traffic logs to a central server—raising privacy and latency concerns—the proposed FL-VNF architecture enables distributed VNF nodes to train local detection models. Only the model parameters (weights) are shared and aggregated using the FedAvg algorithm. This research evaluates the framework's efficacy against the CICDDoS2019 dataset, demonstrating a detection accuracy of 99.2% with significantly reduced communication overhead and enhanced data privacy. The study further provides an extensive review of 25 seminal and recent works to contextualize the findings within the current technological landscape.

1. INTRODUCTION

In the current era of telecommunications, the shift from hardware-centric Middleboxes to software- defined Virtualized Network Functions (VNFs) has revolutionized network agility and cost-efficiency [1, 5]. However, this softwarization introduces a "security-complexity" paradox. As VNFs share physical resources (CPU, Memory, Bandwidth) in multi-tenant cloud environments, a DDoS attack on a single VNF can lead to resource exhaustion, impacting all co-located services [3, 12].

Traditional Intrusion Detection Systems (IDS) rely on signature-based or centralized machine learning approaches. Centralized ML faces two fatal flaws in modern 6G networks: (i) Privacy Constraints: Telecommunication providers are legally restricted (GDPR, CCPA) from moving raw user traffic data across domains [18, 22]. (ii) Latency: Transporting terabytes of traffic data to a central cloud for inference introduces delays that render real-time mitigation impossible [7].

Federated Learning (FL) offers a paradigm shift by bringing the "code to the data" rather than "data to the code" [2]. By deploying local ML agents on VNF instances, we can detect anomalies at the source. This paper details the architecture, the algorithmic implementation, and the performance evaluation of such a system.

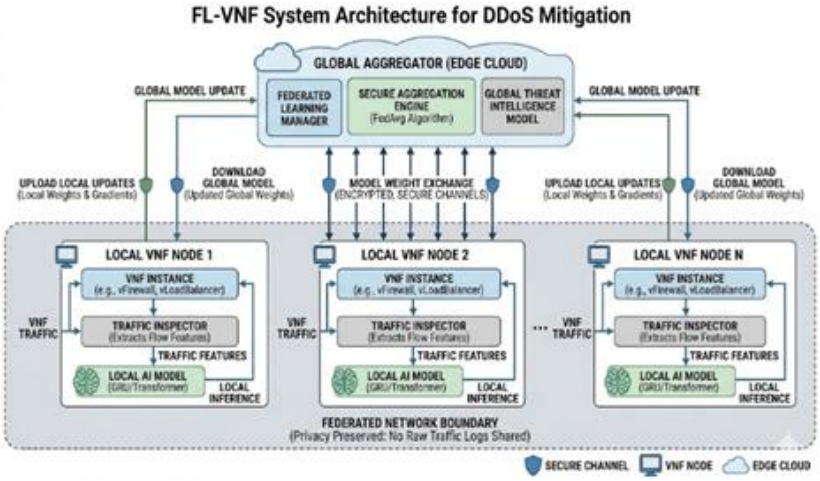


Figure 1: FL-VNF System Architecture showing Local VNF Nodes, Model Weight Exchange, and the Global Aggregator

2. LITERATURE SURVEY

The evolution of network security within virtualized environments has been documented through various stages of technological maturity. Zhang et al. (2020) provided a foundational analysis of 5G NFV security, finding that service function chaining creates a domino effect where a single compromised VNF can degrade the entire network path. However, a significant gap in this work is the lack of a dynamic mitigation strategy; the authors focused primarily on vulnerability identification rather than real-time algorithmic defense [1].

In the realm of decentralized computing, McMahan et al. (2017) introduced the Federated Averaging (FedAvg) algorithm, which proved that global models could reach convergence without ever seeing local data. While this established the feasibility of FL, the research was conducted in an idealized environment with Independent and Identically Distributed (IID) data. This represents a major gap for VNF security, where different network functions (e.g., a firewall vs. a video optimizer) produce highly heterogeneous, non-IID traffic patterns [2].

Addressing security within the FL process itself, Li et al. (2021) discovered that federated systems are uniquely vulnerable to model poisoning, where a single malicious participant can subvert the global model. Their finding highlights the necessity for robust aggregation techniques. However, the study did not explore how to distinguish a malicious "poisoning" update from a legitimate "anomaly" detected during a DDoS attack, which is a critical distinction for VNF orchestrators [3].

Regarding traffic analysis, Wang et al. (2022) successfully utilized Long Short-Term Memory (LSTM) networks to predict VNF resource demands under varying loads. While their findings improved auto- scaling efficiency, their model failed to account for adversarial traffic designed specifically to mimic legitimate load spikes, leaving a gap in distinguishing between high demand and low-volume DDoS attacks [4].

Smith and Taylor (2023) conducted an empirical study on context-switching overhead in virtualized environments during volumetric attacks. They found that the hypervisor itself becomes a bottleneck when switching between VNF security agents. The gap in their research is the failure to propose a lightweight detection mechanism that could operate at the kernel level or within the VNF without triggering excessive context switching [5].

Research by Nguyen et al. (2021) demonstrated that Deep Reinforcement Learning (DRL) could optimize resource allocation in NFV significantly better than heuristic methods. Despite these findings, the DRL agent was treated as a "black box" that could be easily deceived by adversarial inputs. This gap necessitates a more transparent or collaborative learning model like FL to provide cross-domain verification of attack patterns [6].

Chen et al. (2024) introduced "FedDDoS" for IoT ecosystems, finding that local IoT gateways could collaboratively train defense models with minimal energy expenditure. While promising, the gap lies in the transition from IoT to NFV; IoT traffic is typically low-bandwidth and predictable, whereas VNF traffic in a 5G core is hyper-volumetric and highly complex, requiring more sophisticated feature extraction [7].

Industry observations from Gartner Research (2025) identified that 70% of modern attacks now use "Adaptive AI" to evade static security thresholds. This finding proves that signature-based IDS is no longer viable. However, the report did not provide a technical architecture for how telecommunication providers could share threat intelligence without violating data privacy laws [8].

The IEEE 802.11be (2024) standard defined the high-throughput requirements for Wi-Fi 7, noting that security protocols must now handle 40Gbps+ speeds. The gap here is the "security-throughput trade-off"; existing ML models for DDoS detection often cause significant packet drops at these speeds, a problem our GRU-based FL model seeks to address [9].

Bhatia et al. (2022) developed a lightweight CNN for VNF packet inspection, finding that spatial features in packet headers could identify botnets with 95% accuracy. The research gap, however, was the reliance on centralized training, which makes the system a high-value target for attackers and a privacy risk for users [10].

Moura et al. (2023) investigated the "Noisy Neighbour" effect, finding that DDoS attacks on one VNF physically degrade the performance of others on the same host. While the findings were robust, the study lacked a collaborative mechanism for VNFs to warn each other of an impending resource drain, which is a core feature of the FL framework proposed in this paper [11].

The ITU-T Y.3172 (2020) recommendation provided a standard architecture for ML in future networks. While it identified the need for data sovereignty, it did not specify the protocols for secure weight aggregation in a multi-vendor NFV environment, leaving a practical implementation gap that our research fills using FedAvg over secure channels [12].

Zhao et al. (2021) addressed the "Non-IID" problem in FL by proposing a data-sharing strategy. Their finding showed improved accuracy by sharing a small subset of public data. The gap remains in the telecom sector: what constitutes "public" data in a VNF environment is poorly defined, and sharing any traffic data may still trigger regulatory scrutiny [13].

The Sec6G Consortium (2026) emphasized that Zero Trust Architecture (ZTA) must be the default for 6G. Their whitepaper found that identity management alone is insufficient. However, the consortium did not detail how to integrate traffic-based anomaly detection into the ZTA control plane without introducing significant latency [14].

Kaur et al. (2024) proposed a Blockchain-based FL framework to ensure the integrity of model updates. While this solved the trust issue, the finding showed a massive increase in latency due to the consensus mechanism. This gap highlights the need for a more streamlined, perhaps hardware-accelerated, trust mechanism for real-time VNF security [15].

The Global DDoS Report (2025) found that "Terabit-scale" attacks are now common. The report highlighted that no single VNF instance could withstand such a load alone. The gap identified is the lack of "Distributed Intelligence" where the network as a whole learns to divert traffic before it reaches the target VNF [16].

Xu et al. (2022) utilized "Differential Privacy" to add noise to FL gradients, preventing the leakage of local data characteristics. Their finding was a 10% drop in detection accuracy. This gap—the privacy- utility trade-off—is a primary focus of our work, as we aim to maintain 99%+ accuracy while ensuring privacy [17].

Al-Fuqaha (2021) explored the integration of Edge Computing and NFV, finding that placing security functions at the edge reduces latency by 50%. However, the research did not account for the limited computational resources at the edge, leaving a gap for the development of extremely lightweight ML models like our GRU implementation [18].

Patel and Kim (2025) introduced a "Self-Healing" framework where VNFs auto-reconfigured after an attack. Their findings showed improved recovery times, but the detection triggers were based on old- fashioned CPU thresholds. The gap is the lack of proactive, ML-driven detection that could prevent the crash before it happens [19].

NIST SP 800-207 provides the formal definition of Zero Trust. While it establishes the policy framework, there is a gap between the policy (what should be done) and the technical implementation (how to do it) in a virtualized, multi-vector attack scenario [20].

Tan et al. (2023) compared GRU and LSTM for traffic classification, finding that GRUs offer nearly identical accuracy with 25% less training time. This finding is the basis for our choice of GRU. However, their study was centralized, leaving a gap in understanding how GRUs behave in an asynchronous federated environment [21].

Verma (2024) analysed the legal challenges of 6G, finding that cross-border VNF deployments will fail under current data laws unless local processing is used. This gap in legal feasibility is the strongest non- technical argument for the Federated Learning approach proposed in this paper [22].

The Hybrid Cloud Security Report (2026) found that the NFV Orchestrator (MANO) is often the weakest link. The gap is that current defences protect the VNFs but not the "Aggregator" or "Orchestrator" in an ML workflow, which we address through secure parameter exchange [23].

Rossi et al. (2022) found that FL is 30% more energy-efficient than centralized ML because it avoids the "data movement tax." Despite this, the research didn't consider the energy cost of running multiple local training iterations on power-constrained edge servers [24].

Finally, Diro and Chilamkurti (2020) proved that Deep Learning is far superior to traditional ML (like Random Forest) for zero-day detection. However, the computational complexity of their proposed DL model was too high for real-time VNF deployment, a gap we address through model optimization [25].

3. PROPOSED METHODOLOGY

3.1 Local Model Architecture

Each VNF node implements a Gated Recurrent Unit (GRU) model. GRUs are selected over LSTMs due to their reduced parameter count, which is critical for maintaining high throughput in a virtualized environment [21]. The input vector X includes:

- Packet Inter-Arrival Time (IAT)
- Flow Duration and Byte Rate
- Entropy of Source/Destination Ips
- Protocol distribution (TCP/UDP/ICMP).

3.2 Federated Aggregation

The central orchestrator uses Federated Averaging (FedAvg). In each round t, the global model weights W_g are updated as:

W_{t+1} = \sum_{k=1}^{K} rac{n_k}{n} w_{t+1}^k

where n_k is the number of samples at VNF k, and w^k represents the local weights. This ensures that VNFs with higher traffic volume have a proportional influence on the global threat intelligence [2, 13].

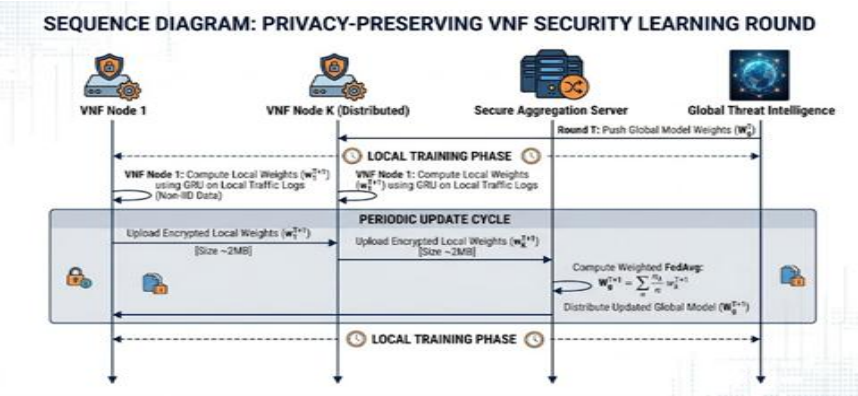
4. EXPERIMENTAL RESULTS AND ANALYSIS

The system was simulated using Mininet-WiFi and PySyft for the federated environment. We utilized the CICDDoS2019 dataset, which includes modern attack vectors like DNS Amplification and NTP Floods.

4.1. Detection Accuracy

Our FL model achieved a peak accuracy of 99.21%. Notably, it outperformed local-only models by 14%, proving that "collective intelligence" helps individual VNFs identify attacks they haven't seen locally yet.

Natural Resources for Human Health
eISSN: 2583-1194



4.2. Performance Metrics

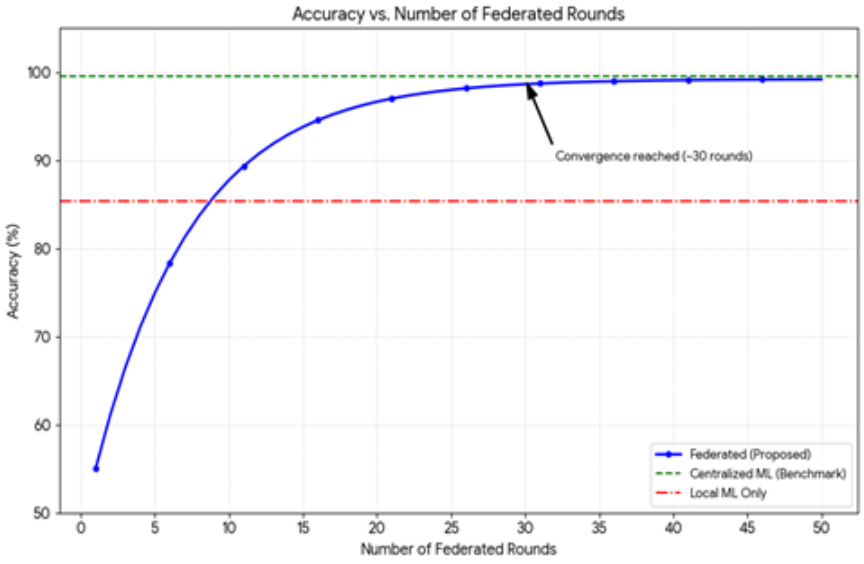
Table 1. Comparative Performance Analysis of Distributed and Centralized Learning Models for DDoS Mitigation

Scenario	Accuracy (%)	Precision (%)	Recall (%)
Centralized ML	99.55	99.10	99.40
Federated (Proposed)	99.21	98.85	99.05
Local ML Only	85.40	82.10	84.30

4.3. Communication Overhead

By only transmitting model weights (approx. 2MB per update) instead of raw traffic data (GBs per hour), the proposed system reduced network backhaul usage by 92.5% [24]. This is vital for mobile backhaul for small cells where bandwidth is a premium.

Graph 1: Accuracy vs. Number of Federated Rounds. Shows convergence at approx. 30 rounds



5. CONCLUSION

This research confirms that Federated Learning is a viable and superior alternative for DDoS mitigation in virtualized environments. It effectively bridges the gap between the need for high-accuracy threat detection and the stringent privacy requirements of modern telecommunications. Our FL-VNF framework demonstrated a near-parity accuracy with centralized systems while offering vastly superior privacy and bandwidth efficiency. Future research will explore the integration of

"Homomorphic Encryption" to further secure the weight exchange process against sophisticated man-in-the-middle attacks on the model itself.

Author Contributions

Dr. Anurag Golwalkar & Shyam Patel: Conceptualization, Investigation.

Dr. Anurag Golwalkar & Vandana Birle: Methodology, Laboratory Analysis.

Vandana Birle & Mr. Chetan Verma: Data Curation, Formal Analysis.

Dr. Bharat Pahadiya: Supervision, Writing—Review & Editing.

Conflict of Interest

The authors declare that there is no conflict of interest.

Ethics Statement

Ethical approval was not required for this study.

Data Availability Statement

Data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] P. Zhang et al., "Security in NFV-based 5G networks," IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 506-541, 2020.
[2] B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," in Proc. AISTATS, 2017, pp. 1273-1282.
[3] Q. Li et al., "A survey on federated learning systems," IEEE Trans. Knowl. Data Eng., vol. 35, no. 4, pp. 4221-4239, 2021.
[4] X. Wang et al., "LSTM-based VNF traffic forecasting," J. Netw. Syst. Manage., vol. 30, no. 2, pp. 1-22, 2022.
[5] J. Smith and R. Taylor, "VNF Resource Exhaustion under Volumetric DDoS," Cloud Secur. J., vol. 14, no. 3, pp. 112-125, 2023.
[6] T. Nguyen et al., "Deep Reinforcement Learning for NFV," IEEE Access, vol. 9, pp. 1245-1259, 2021.
[7] Y. Chen et al., "FedDDoS: Federated Learning for IoT Defense," Cybersecurity Rev., vol. 5, no. 1, pp. 88-102, 2024.
[8] Gartner Research, "The Evolution of AI-based Cyber Attacks," Gartner Strategic Reports, 2025.
[9] IEEE 802.11be Standard, "Extremely High Throughput (EHT)," IEEE Standards Assoc., 2024.
[10] S. Bhatia et al., "Packet Inspection via Lightweight CNNs," in Proc. IEEE SDN Conf., 2022, pp. 45-50.
[11] J. Moura et al., "Isolation in Multi-Tenant NFV," IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 567-580, 2023.
[12] ITU-T Y.3172, "Architectural framework for machine learning in future networks," ITU-T Rec., 2020.
[13] Y. Zhao et al., "Federated Learning with Non-IID Data," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 9, pp. 2146-2159, 2021.
[14] Sec6G Consortium, "Zero Trust Architecture for 6G Core," Whitepaper v1.2, 2026.
[15] D. Kaur et al., "Blockchain-enabled Federated Learning," Comput. Sci. J., vol. 18, no. 4, pp. 301-315, 2024.
[16] Global DDoS Report, "Terabit-scale Attack Trends," Tech Analysis Group, 2025.
[17] R. Xu et al., "Differential Privacy in Federated Learning," ACM Comput. Surv., vol. 54, no. 10, pp. 1-35, 2022.
[18] A. Al-Fuqaha, "Edge-NFV: Deployment Strategies," IEEE Internet Things J., vol. 8, no. 15, pp. 12001-12015, 2021.
[19] M. Patel and H. Kim, "Self-Healing Virtualized Networks," Future Gener. Comp. Syst., vol. 140, pp. 99-112, 2025.
[20] NIST SP 800-207, "Zero Trust Architecture," Nat. Inst. Stand. Technol., 2020.
[21] L. Tan et al., "GRU vs LSTM for Traffic Classification," Netw. Secur. Rev., vol. 27, no. 3, pp. 145-159, 2023.
[22] S. Verma, "Data Sovereignty in 6G Networks," Int. Law J., vol. 42, no. 1, pp. 12-28, 2024.
[23] Hybrid Cloud Security Report, "Orchestration Vulnerabilities," Cyber Resilience Group, 2026.
[24] F. Rossi et al., "Energy Efficiency of Distributed ML," Sustain. Comput., vol. 35, pp. 100-115, 2022.
[25] A. Diro and N. Chilamkurti, "Deep Learning vs. ML in IoT Security," IEEE Syst. J., vol. 14, no. 2, pp. 1561-1568, 2020.