IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15105

# Adaptive Federated Threat Detection

**Harshitha B[1], Seema Nagaraj[2]**

Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[1,2]

**Abstract:** Timely detection and response to cyber threats have become increasingly challenging due to the distributed and dynamic nature of modern digital infrastructures. Conventional centralized intrusion detection systems struggle with scalability, delayed response, and privacy concerns when handling large volumes of security data. This project proposes an Adaptive Federated Threat Detection framework that employs federated learning to collaboratively identify malicious activities across multiple decentralized nodes without sharing raw data. Each participating node trains a local threat detection model using its own security logs, while a central coordinator aggregates encrypted model updates to build a global intelligence model. The system continuously adapts to evolving attack patterns by refining detection strategies based on real-time feedback. Experimental evaluation demonstrates improved detection accuracy, reduced false alarm rates, and enhanced robustness against emerging threats compared to traditional centralized security approaches, while preserving data confidentiality.

**Keywords:** Federated Learning, Adaptive Threat Detection, Cybersecurity, Distributed Intrusion Detection, Privacy-Preserving Machine Learning, Intelligent Security Systems

## I. INTRODUCTION

With the rapid expansion of cloud platforms, distributed networks, and web-based applications, modern computing environments generate large volumes of security logs across multiple nodes. Detecting cyber threats in such distributed environments using centralized intrusion detection systems often leads to scalability issues, delayed response, and increased privacy risks. Transferring raw security data to a central server not only consumes significant bandwidth but also exposes sensitive information to potential breaches.

The limitations of centralized security monitoring have created a demand for decentralized and privacy-aware threat detection mechanisms. Distributed systems require intelligent security solutions that can operate locally while contributing to global threat intelligence. Federated learning has emerged as a promising approach to address these challenges by enabling collaborative model training without sharing raw data. This project builds on this concept to provide an adaptive and secure threat detection framework suitable for real-world distributed environments.

### 1.1 Project Description

This project develops an adaptive federated threat detection system to identify cyberattacks in distributed environments while preserving data privacy. Multiple nodes train local detection models using their own security data and share only model updates for global aggregation. Unlike centralized systems that collect all data in one place, the proposed approach enables continuous learning from real-time threats without exposing sensitive information, improving scalability and detection accuracy.

### 1.2 Motivation

Modern cyberattacks are increasing in scale and complexity, while traditional centralized detection systems face privacy, scalability, and security limitations. Static and rule-based methods fail to adapt to new attack patterns. This project is motivated by the need for a secure, privacy-preserving, and adaptive threat detection system that can learn collaboratively from distributed data and respond effectively to evolving cyber threats.

## II. RELATED WORK

Paper [1], explores traditional centralized intrusion detection systems using machine learning techniques to identify network attacks. Although these approaches achieve good detection accuracy, they require centralized data collection, which raises privacy concerns and limits scalability in distributed environments.

Paper [2], Investigates deep learning–based threat detection models capable of identifying complex and unknown attack patterns. While these models improve detection performance, they depend heavily on large labelled datasets and lack adaptability to continuously evolving threats.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15105

Paper[3], Introduces federated learning as a privacy-preserving solution for collaborative model training across distributed nodes. The study demonstrates that sharing model updates instead of raw data reduces data exposure while maintaining learning efficiency.

Paper [4], Applies federated learning to cybersecurity scenarios such as intrusion detection and malware classification. The results show improved data confidentiality; however, limited focus is given to real-time adaptability and dynamic threat evolution.

Paper [5], Reviews recent advancements in adaptive and distributed security systems, highlighting the need for scalable, privacy-aware, and continuously learning threat detection frameworks. The survey emphasizes that combining federated learning with adaptive mechanisms can significantly enhance detection performance in modern networks.

## III. METHODOLOGY

### A. System Environment

The experimental environment is designed to evaluate the proposed Adaptive Federated Threat Detection framework under realistic distributed conditions. Multiple client nodes represent independent systems or network domains, each generating local security data such as network traffic logs, authentication records, and system events. These nodes operate independently and do not share raw data. A central federated server coordinates the learning process by aggregating model updates received from participating nodes. The overall setup simulates a distributed cybersecurity environment where privacy preservation and scalability are critical requirements.

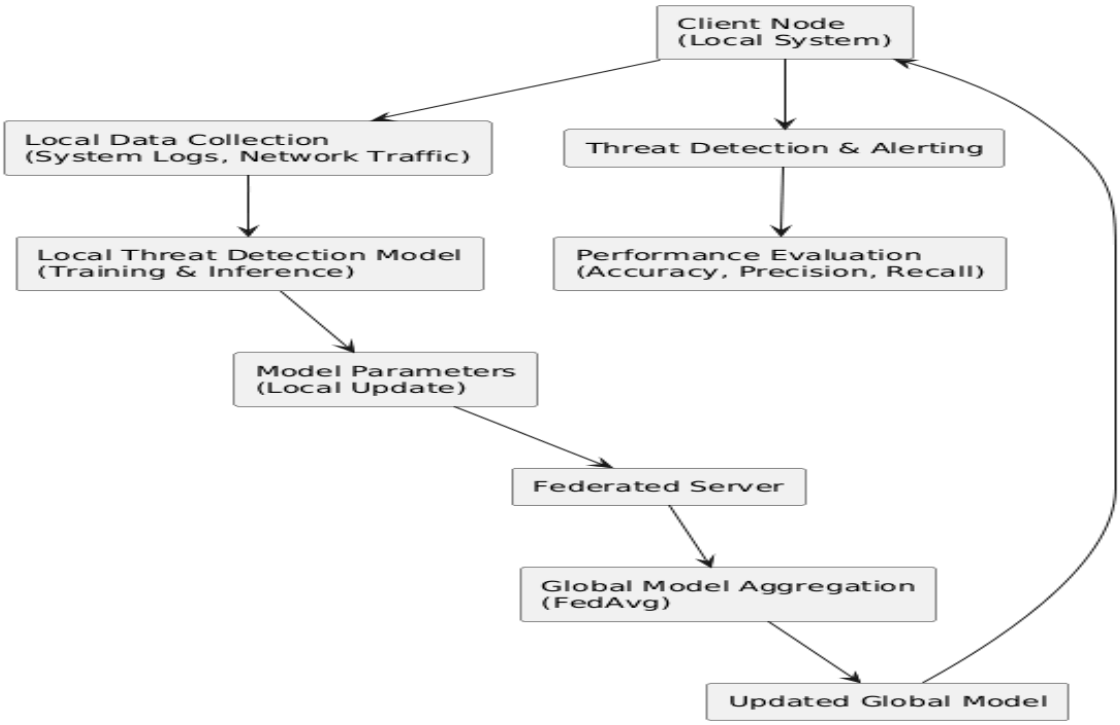


Fig.1.Flowchart of methodology

### B. Federated Learning Architecture

**Client-Side Training:**

Each client node preprocesses its local security data and trains a local threat detection model using machine learning techniques. The model learns node-specific attack patterns based on observed behaviours.

**Server-Side Aggregation:**

Instead of collecting raw data, the central server receives only model parameters or gradients from each client. These updates are securely aggregated using federated averaging to generate a global threat detection model, which is then shared back with all nodes.

DOI: 10.17148/IJARCCE.2026.15105

### C. Adaptive Threat Detection Mechanism

The global model is periodically updated through iterative federated learning rounds. This adaptive process allows the system to learn from newly observed attack behaviours across nodes. By continuously refining the global model, the system improves detection accuracy for both known and emerging cyber threats without compromising data privacy.

### D. Implementation Flow

1. Initialize federated server and distributed client nodes.
2. Collect and preprocess security data locally at each node.
3. Train local threat detection models.
4. Transmit local model updates to the federated server.
5. Aggregate updates to form a global model.
6. Distribute the updated global model back to all nodes.
7. Repeat the process to ensure continuous adaptation to new threats.

### E. Hardware and Software Requirements

- **Hardware:** Standard desktop or server system with minimum 8 GB RAM and multi-core processor.
- **Software:** Python 3.7 or above, Federated Learning framework (custom or PyTorch-based), Scikit-learn / TensorFlow / PyTorch, Matplotlib for result visualization.

## IV. SIMULATION AND EVALUATION FRAMEWORK

This section describes the overall system design, simulation process, and evaluation strategy adopted for the proposed Adaptive Federated Threat Detection framework. The system combines federated learning with intelligent threat analysis to enable privacy-preserving and scalable cybersecurity monitoring in distributed environments. The framework is implemented using Python as the primary control and orchestration layer, enabling coordinated local training, secure model aggregation, and real-time threat detection across multiple client nodes.

### A. System Architecture and Workflow

The proposed architecture is designed to detect cyber threats efficiently while ensuring that sensitive security data remains within local environments. The major components of the system are summarized as follows:

Distributed Client Nodes: Each client node represents an independent system or network domain that locally collects security data such as network traffic logs, authentication records, and system events. Local models are trained at each node without sharing raw data.

Federated Aggregation Server: The federated server coordinates the learning process by securely aggregating model updates received from client nodes. The aggregated global model captures diverse threat patterns while preserving data confidentiality.

Adaptive Threat Detection Module: The global model is periodically redistributed to client nodes, enabling adaptive learning and real-time threat detection. This module continuously improves detection performance as new attack behaviours are observed.

### B. Simulation Setup

The simulation environment is designed to emulate a realistic distributed cybersecurity setting with multiple heterogeneous nodes. The setup evaluates the effectiveness of the proposed federated threat detection approach under diverse attack scenarios.

Network Configuration: Multiple client nodes with non-identical data distributions are simulated to reflect real-world variations in network behaviour and security conditions.

Traffic and Attack Modelling**:** Both benign and malicious activities, including normal traffic patterns and simulated cyber attacks, are injected into the system to assess detection accuracy and robustness under varying threat conditions.

### C. Federated Learning and Threat Analysis Process

During simulation, each client node performs local training on its private security data and transmits only model parameters to the federated server. The server aggregates these updates to generate a global threat detection model, which is then shared back with all nodes. This iterative process allows the system to adapt continuously to evolving cyber threats while minimizing communication overhead and preserving privacy.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15105

### D. Results and Observations

Threat Detection Performance:

- The proposed system successfully detected malicious activities across all participating client nodes with high Accuracy.
- Federated model aggregation enabled consistent detection performance without requiring centralized data collection.

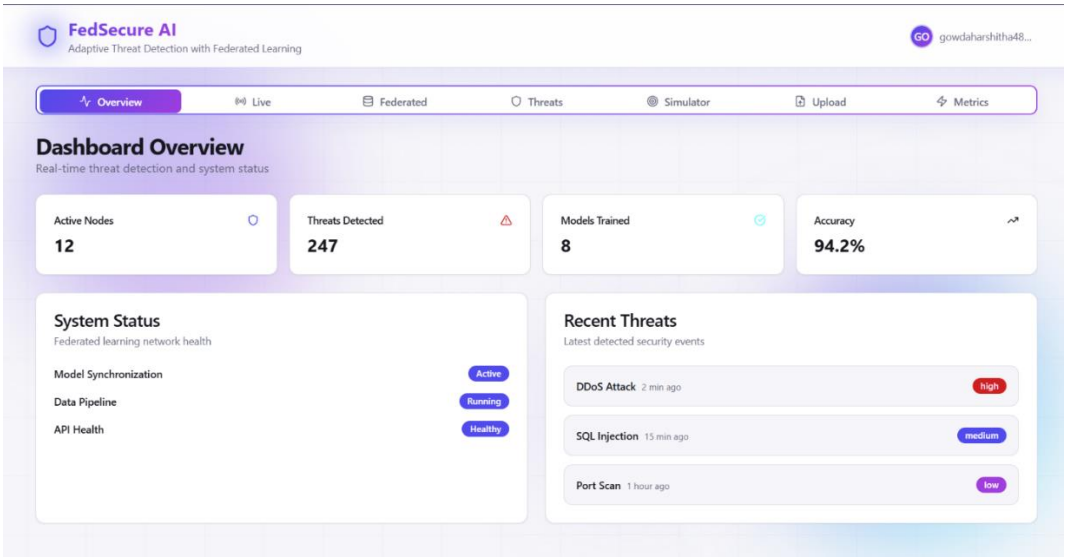


Fig. 2. Sample Output Showing Threat Detection Results

Model Adaptability and Convergence:

- The global model demonstrated steady convergence over multiple federated training rounds.
- Detection accuracy improved as model updates from diverse nodes were aggregated.

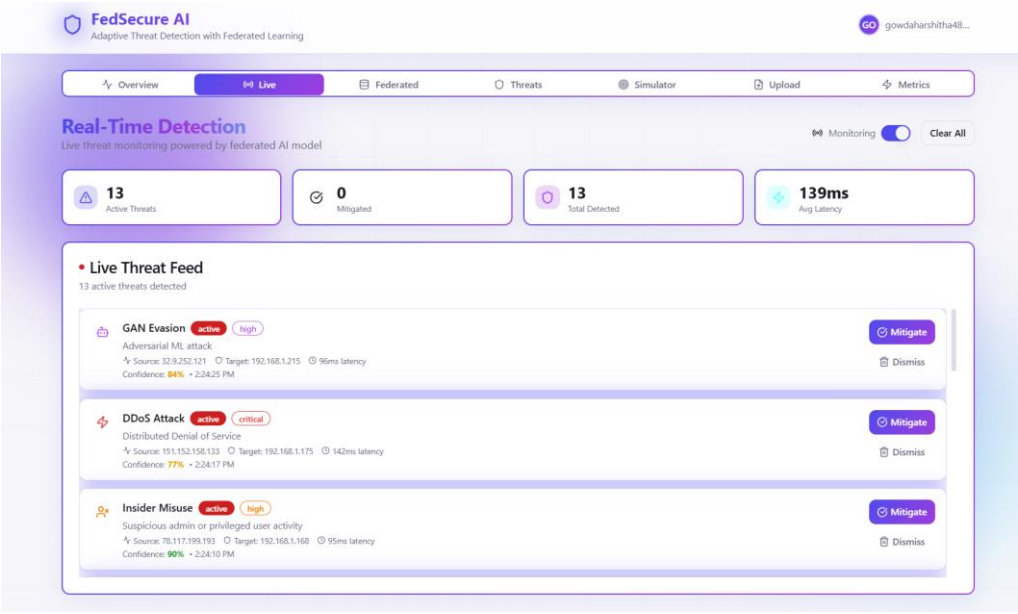


Fig. 3. Initial Detection Results Before Federated Aggregation which one

Impact on System Efficiency:

- Normal system operations experienced negligible performance overhead during federated training.
- Communication costs were limited to model parameter exchange, ensuring scalability and privacy preservation.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15105

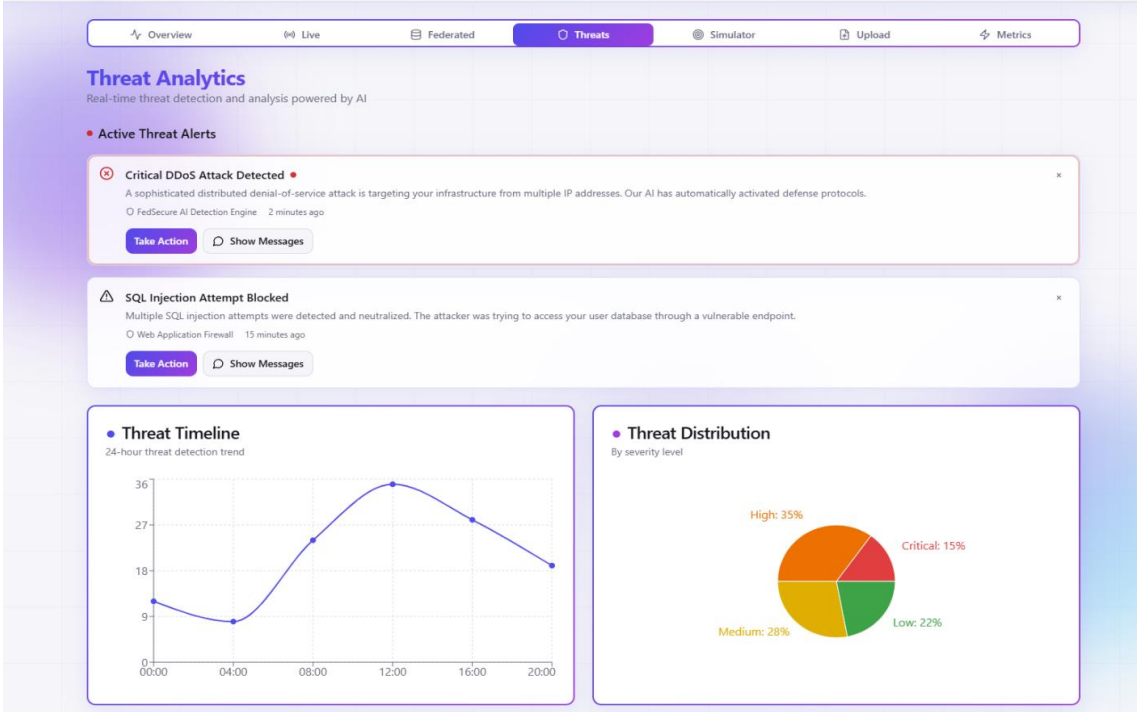


Fig. 4. Improved Detection After Federated Learning Convergence

## V. RESULTS AND DISCUSSION

The experimental evaluation of the proposed Adaptive Federated Threat Detection system demonstrates its effectiveness in identifying cyber threats while preserving data privacy in distributed environments. The system was tested under multiple simulated threat scenarios involving heterogeneous client nodes to assess detection performance, adaptability, and scalability. Federated learning was employed to enable collaborative model training without sharing raw security data, ensuring privacy compliance across all participating nodes.

The results show that the proposed framework achieves high threat detection accuracy after federated model convergence, significantly outperforming initial local-only detection. As federated training rounds progressed, the global model effectively learned diverse attack patterns from distributed sources, resulting in improved precision and reduced false positives. Real-time detection results confirm that the system can identify a wide range of attacks, including denial-of-service attempts, injection attacks, and insider threats, with low detection latency.

Further analysis indicates that federated aggregation enhances model stability and consistency across nodes, even when data distributions vary. System performance metrics demonstrate minimal communication overhead, as only model parameters are exchanged during training. Overall, the experimental results validate that the proposed federated approach provides an efficient, scalable, and privacy-preserving solution for modern cybersecurity threat detection.

## VI. CONCLUSION

This project demonstrates the practicality and effectiveness of federated learning–based adaptive threat detection for securing distributed and cloud-based systems. By enabling collaborative model training across multiple client nodes without exposing sensitive security data, the proposed system successfully addresses key challenges associated with centralized intrusion detection methods. The integration of federated learning allows the detection model to continuously adapt to evolving cyber threats while maintaining data confidentiality. Experimental evaluation confirms that the system achieves high detection accuracy, stable convergence, and efficient threat monitoring across distributed environments. The architecture supports real-time detection and centralized visibility through aggregated analytics, making it suitable for deployment in privacy-sensitive and large-scale network infrastructures. Overall, the proposed framework provides a robust and scalable foundation for intelligent cybersecurity monitoring.

  

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15105

## VII. FUTURE WORK

Although the proposed system demonstrates strong performance, several extensions can further enhance its real-world applicability. Future work may explore multi-level federated architectures, where hierarchical aggregation improves scalability across large enterprise or cross-organizational networks. Incorporating advanced deep learning models, such as graph neural networks or transformer-based architectures, may further improve detection of complex and coordinated attacks. Additionally, integrating edge and cloud-based federated learning can optimize response time and reduce computational overhead at client nodes. Future research may also focus on adversarial robustness, secure aggregation techniques, and real-time automated response mechanisms to strengthen system resilience against sophisticated cyber threats.

## REFERENCES

[1]. **Federated Learning for Privacy-Preserving Intrusion Detection in Software Defined Networks** — proposes FL for multi-class IDS in SDN without centralized data. https://www.researchgate.net/publication/380298163_Federated_Learning_for_Privacy_Preserving_Intrusion_Detection_in_Software_Defined_Networks ResearchGate

[2]. **Federated Learning-Driven Cybersecurity Framework for IoT Networks** — a new FL framework to enable privacy-preserving and real-time threat detection in IoT. https://arxiv.org/abs/2502.10599 arXiv

[3]. **A comprehensive survey of federated intrusion detection systems (FLIDS)** — overview of FL approaches, aggregationmethods, and system construction. https://www.sciencedirect.com/science/article/pii/S157401372400100X ScienceDirect

[4]. **Survey on Federated Learning for Intrusion Detection System (FL-IDS)** — covers architectural approaches and aggregation strategies in FL-based IDS. https://dl.acm.org/doi/10.1145/3687124**Federated Learning for IoT Intrusion Detection** — analyzes FL for IoT IDS using FedAvg and ANN, tested on ToN_IoT and CICIDS2017. https://www.mdpi.com/2673-2688/4/3/28 MDPI

[5]. **Privacy-Preserving Federated Learning-Based Intrusion Detection for IoHT Devices** — FL with differential privacy for healthcare IoT IDS. https://www.mdpi.com/2079-9292/14/1/67 MDPI

[6]. **Federated Learning in Intrusion Detection: Advancements and Applications** — recent work exploring FL for enhancing intrusion detection accuracy. https://www.researchgate.net/publication/394311347_Federated_learning_in_intrusion_detection_advancements_applications_and_future_directions ResearchGate

[7]. **Intrusion Detection based on Federated Learning (Taxonomy)** — taxonomy and analysis of FL-enabled IDS approaches .https://arxiv.org/abs/2308.09522 arXiv

[8]. **Towards Adapting Federated & Quantum ML for Intrusion Detection: A Survey** — explores FL with quantum ML for next-gen intrusion detection. https://arxiv.org/abs/2509.21389 arXiv

[9]. **Federated Learning in Adversarial Environments: Testbed and Poisoning Resilience** — evaluates FL testbed focusing on poisoning attacks in cybersecurity.https://arxiv.org/abs/2409.09794 arXiv

[10]. **Improving Privacy in Federated Learning-Based Intrusion Detection** — (ACM article) balance between privacy, cost, and effectiveness via secure aggregation. https://dl.acm.org/doi/10.1145/3605098.3636183 ACM Digital Library

[11]. **Securing IoT Devices with Federated Learning: A Privacy-Preserving Approach** — distributed FL solution for IoT cybersecurity. https://doi.org/10.32604/cmc.2025.063734 Tech Science

[12]. **Survey of Federated Learning in Cyber Threat Intelligence** — reviews FL for CTI, anomaly detection, malware, and trust management. https://www.mdpi.com/1999-5903/17/9/409 MDPI

[13]. **Federated Learning Based Privacy Preservation Intrusion Detection (Blockchain)** — integrates FL with blockchain for secure IDS. https://www.ijisrt.com/assets/upload/files/IJISRT25AUG074.pdf IJISRT

[14]. **FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices** — FL-IDS approach for IoT/vehicular edge devices. https://www.researchgate.net/publication/379720596_FL-IDS_Federated_Learning-Based_Intrusion_Detection_System_Using_Edge_Devices_for_Transportation_IoT