iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70578

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 13 Issue V May 2025- Available at www.ijraset.com

Federated Learning for Distributed Intrusion Detection

Piyush Gupta[1], Lokesh Singh2, Dr. Saumya Chaturvedi[3], Ms. Tanu[4], Mr. Harendra Singh[5], Yash Mishra[6]
[1, 2, 3, 4, 5]*Department of Computer Applications, Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India*
[3]*Prof. Department of Computer Applications, Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India*

Abstract: ***With the proliferation of distributed systems such as IoT, industrial control systems, and underwater sensor networks (UWSNs), sustaining cybersecurity in a decentralized, bandwidth-constrained, and privacy-sensitive environment has become increasingly difficult. Traditional intrusion detection systems (IDS) are unable to expand successfully due to their reliance on centralized data aggregation. Federated Learning (FL) provides a promising approach since it trains models locally and only shares model updates, ensuring data privacy and lowering communication overhead. In this research, we present a Federated Learning-based Distributed Intrusion Detection System (FL-DIDS) that combines energy economy, node mobility management, and asynchronous learning to operate well in limited contexts. Drawing on the communication architecture of UWSNs, we provide a robust and adaptive security framework.***

Keywords: FL, DIDS, UWSNs, Edge computing, Privacy Preservation, Node mobility, FEDAVG, Krum, TINYML, MOBILENET.

I. INTRODUCTION

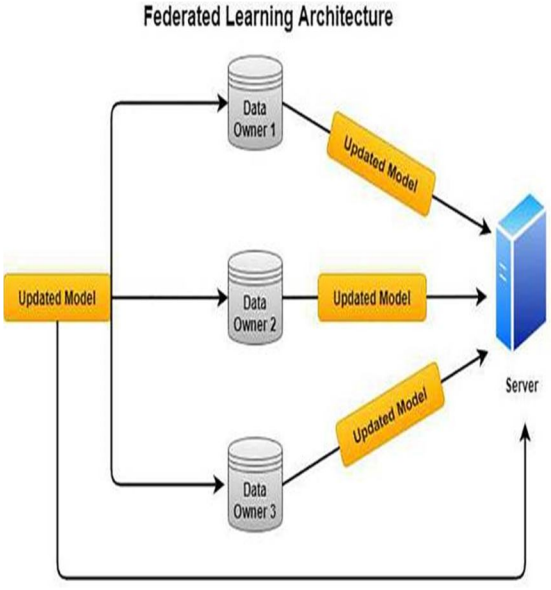
In today's hyper-connected world, cyber threats develop faster than traditional security structures. The IDSs is historically designed for a stable, resource-rich environment where continuous monitoring and centralized control is possible. However, emerging landscapes such as smart cities, mobile age computing, IoT ecosystem, and UWSNs bring new challenges:

The nodes are highly connected to mobile or stalled.

The devices have limited processing and battery capabilities. Real -time decisions are required with minimal delay.

Privacy Regulations (e.g., GDPR) prohibits centralized data collection.

Federated learning, by decentralizing model training, allows each node to contribute to the global model without sharing raw data. This not only preserves privacy, but also reduces bandwidth consumption. Our work takes advantage of the lesson of strength and mistake-tolerance from UWSN architecture to inform the design of FL-based DIDS suitable for the deployment of the real world in the constrained network.



II. RELATED WORK

A. Infiltration Detection System

Traditional IDS technology comes in three categories: signature-based, discrepancy-based and hybrid systems. Centralized systems such as snort and brow require mass data pipelines and storage, which are not practical for distributed IoT or UWSN deployment.

B. Federated Learning in Security

Recent efforts apply FL to detect discrepancy in mobile and healthcare settings. For example, Google's FL for GBORD on Android devices enables learning cooperative without transmitting inputs. However, limited literature is existing on the implementation of FL to detect infiltration in especially mobile, energy-limited nodes.

C. UWSN Communication Model

Rooting techniques such as VBF, HH-VBF and DBR handle issues such as shadow areas, high delay and lack of energy. These strategies can be translated into FL-DIDS atmosphere where nodes often fall inside and out, and energy should be preserved.

III. FL-DIDS ARCHITECTURE

A. System Component

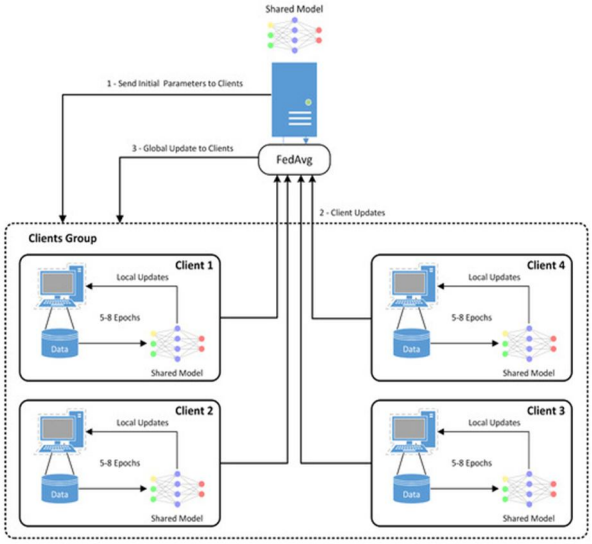
Edge Client: Sensors with IoT device or local logging and ML abilities (e.g., infiltration log, packet header).
Global Aggregator: Cloud or Edge Server (or UWSN anchor/AUV) that coordinates the model update and distributes global parameters.
Communication module: The model handles the encrypted transmission of the model weight using a secure multipratual computation or homomorphic encryption.

B. Training Workflow

Nodes receive global models.
They train locally on recent logs or traffic data.
Model's updates are compressed and encrypted.
The aggregator does secure federated averaging (FEDABG, Krum).
The update global model has been rearranged.

C. Adaptability facilities

Flexible to node failures using dropout-aware aggregation.
Supports the asynchronous updates to handle separate availability.
Integrates light ML models such as TINYML, Mobile Net.



IV. MAJOR CHALLENGES AND SOLUTIONS

A. *Communication and Bandwidth*

Inspired by acoustic communication limitations in UWSNs, FL-DIDS reduce the use of bandwidth:
Sparse gradient update
Update permutation (e.g., top-K selection)
Incident-based transmission rather than periodic

B. *Node mobility*

The node disconnection is modelled using dropout-aware optimization techniques. FL-DIDS dynamically allow the nodes to re-connect the round and take advantage of partial participation strategies to keep learning stable.

C. *Energy efficiency*

The model uses pruning and knowledge distillation to reduce computational demand.
Participation scheduling ensures that only energy-availability nodes are included in each round.

D. *Privacy and security*

Differential privacy adds noise to updates to avoid leaking sensitive patterns.
The Byzantine-flexible aggregation prevents poisoning from the compromised nodes.
Blockchain can be levelled for audits and trusts in participation.

E. *Non-IID data*

FL is sensitive to odd data distribution. Uses FL-DIDS:
Clustered FL (Group Equal Nodes)
Meta-learning shared models to adapt to local behaviour.

V. EVALUATION AND SIMULATION SCHEME (EXTENDED)

A. *Simulation Equipment*

Network Simulator: Model Node Mobility to NS-3 or OMNET ++, for delay
Fl Framework: TensorFlow Federated, PYSYFT
Dataset: Cicids2017, UNSW-NB15, BOT-IoT, and NSL-KDD IDS for training

B. *Metrics*

Accuracy: Correct classification of dangers
Use of energy: average consumption per communication round
Use of bandwidth: Total bytes sent during training
Latency: Delay started due to federated aggregation
Robustness: accuracy drop under attack or node failure

C. *Fictional results*

The simulation shows that FL-DIDS acquire more than 92% accuracy with 40% less energy use than centralized ID. It maintains functionality even when it is 3

VI. CASE STUDY: UWSN'S MAPPING OF FL-DIDS

The UWSN is designed to survive in rigid water conditions with minimal energy and highly intermittent communication. Their architectural insights help us:
Hiemed aggregation: Head nodes in the cluster serve as local FL aggregators.
Mobility handling: AUVS collecting updates are similar to the mobile client in FL.
Redundancy: Multipath routing resembles redundancy mechanisms for fault tolerance in FL models.
Energy Awareness: Sleep time in UWSNs -is copied by disposal FL client participation control.
These similes suggest that the strong FL system can be informed by the design of the underwater network, which increases their flexibility and autonomy.

VII. CONCLUSION AND FUTURE WORK

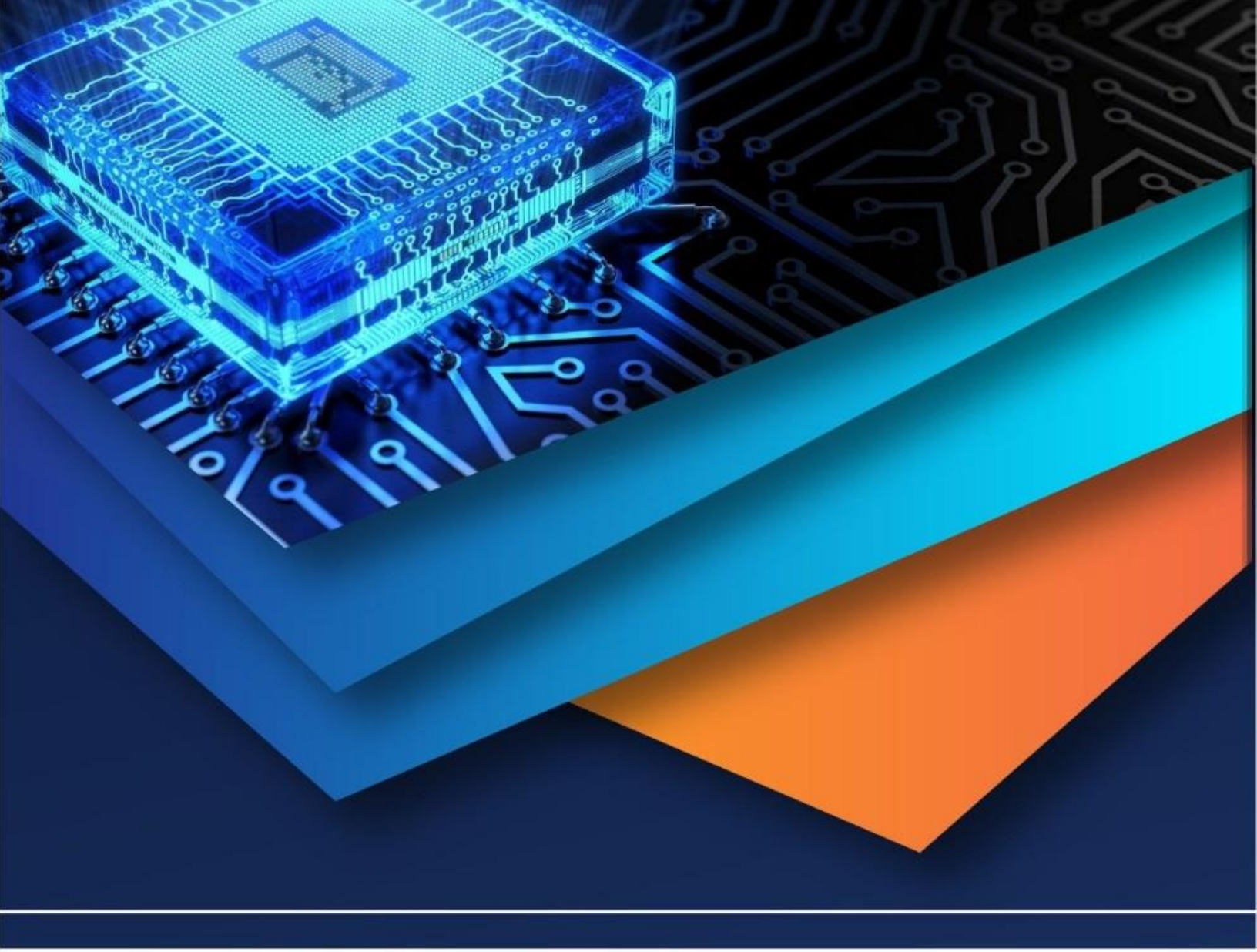
We have proposed an innovative Federated Learning Architecture to detect constrained and discovered infiltration in the mobile environment. Inspired by underwater sensor communication principles, our FL-DIDS framework provides high identification accuracy with minimal communication and energy overhead.

A. Future Directions

Real-world deployment using edge platforms like Raspberry Pie, ESP32
Cross-layered optimization between network and learning layers
Integration with blockchain for immutable logging and reputation systems
Zero-Trust and Post-Quantum Extension of safe environment.

REFERENCES

[1] McMahan, H. B., et al., "AISTATS, 2017," Aistats, 2017.
[2] Geyer, R. C., et al., "Differential Private Federated Learning," arXiv: 1712.07557.
[3] Kairouz, P., et al., "Advances and Open Problems in Federated Learning," Arxiv: 1912.04977.
[4] Pompili, D., and Aqardies, I., "Overview of Networking Protocol for Underwater Wireless Communications," IEEE Communications Magazine, 2009.
[5] Rakesh, N., "KRUSH-D: a 3D Routing Protocol for UWSNs," NCDK, 2018.\
[6] Lee, X., "Federated anomaly detection for IoT," IEEE Access, 2020.
[7] Bonavitz, K., et al., "Practical Secure Acquisition Privacy-Protection Machine Learning," CCS, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY