Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

Designing A Self-Learning And Secured Intrusion Detection System (Ids) For A Distributed Iot- Architecture (Similar To Smart Homes) To Propulsion Systems Using Federated Learning And Sensor Data Analytics.

Dr Addapalli VN Krishna,

Professor, CSE, SOET, CHRIST University, Bengaluru-560074,

Abstract

The rapid usage of Internet of Things (IoT) devices equipped with sensors involves larger amounts of data that supports for intelligent data analytical applications. However, centralizing this data raises critical privacy and security concerns. Federated Learning (FL) offers a promising decentralized approach, enabling edge devices to collaboratively train machine learning models without sharing raw data. This work proposes a federated learning framework tailored for IoT sensor networks, integrating lightweight security mechanisms to ensure data privacy and secure communication under resource constraints typical of IoT environments.

Introduction

With the frequent usage of IoT devices in smart homes—such as security cameras, motion detectors, smart locks, and environmental sensors—these devices continuously collect and transmit sensitive data. This data is vulnerable to a wide range of cyber and physical intrusions, including unauthorized access, tampering, and eavesdropping.

Traditional centralized intrusion detection systems pose privacy risks and are often inefficient due to bandwidth limitations and the heterogeneous nature of IoT devices. Additionally, collecting all sensor data in a central server creates a single point of failure and a high-value target for attackers.

In modern manufacturing environments, Industrial IoT (IIoT) systems integrate thousands of sensors across production lines, robotics, and energy systems. These sensors collect critical real-time data, including temperature, pressure, machine state, and access logs.

However, as these networks grow, so does their attack surface—making them prime targets for cyber intrusions**,** espionage**,** and sabotage. Traditional centralized monitoring systems are unsuitable due to data privacy concerns, latency issues, and heterogeneous device types.

A federated learning-based IDS offers a powerful solution by enabling decentralized anomaly detection without sharing raw industrial data**,** thus maintaining operational security and regulatory compliance.

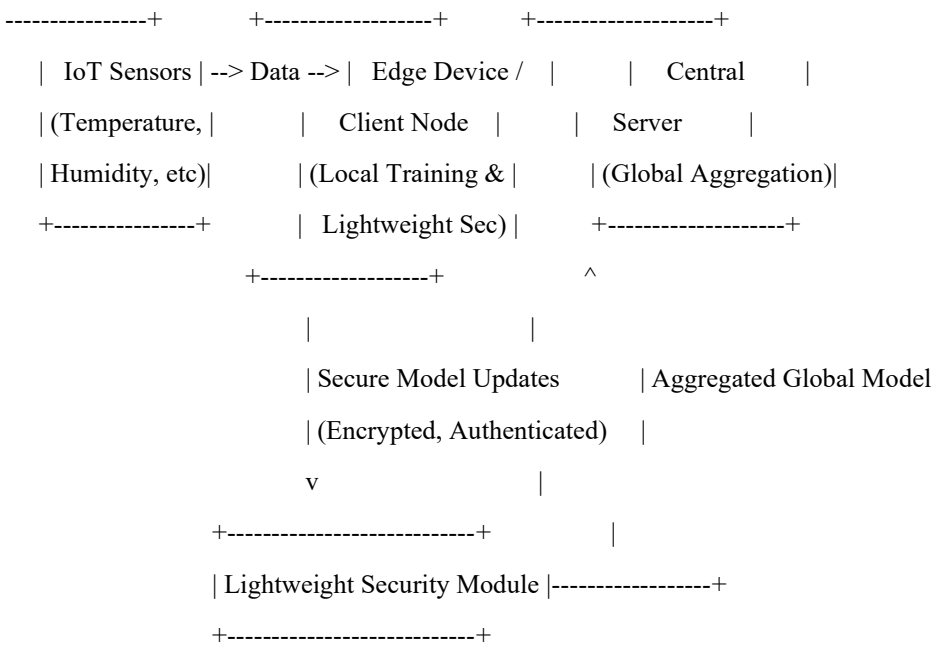
Objective**:**

To build a decentralized intrusion detection system that:

- Collecting sensor data from various IoT products (e.g., smart locks, temperature sensors, cameras).
- Computing the data by federated learning (FL) to train intrusion detection models locally on devices without sharing raw data.

- Detecting anomalous or malicious behavior (e.g., spoofing, unauthorized entry, DDoS attempts) in real-time by Statistical or rule based models
- Maintains data privacy across a network of IoT devices by Leight weight Security mechanisms.

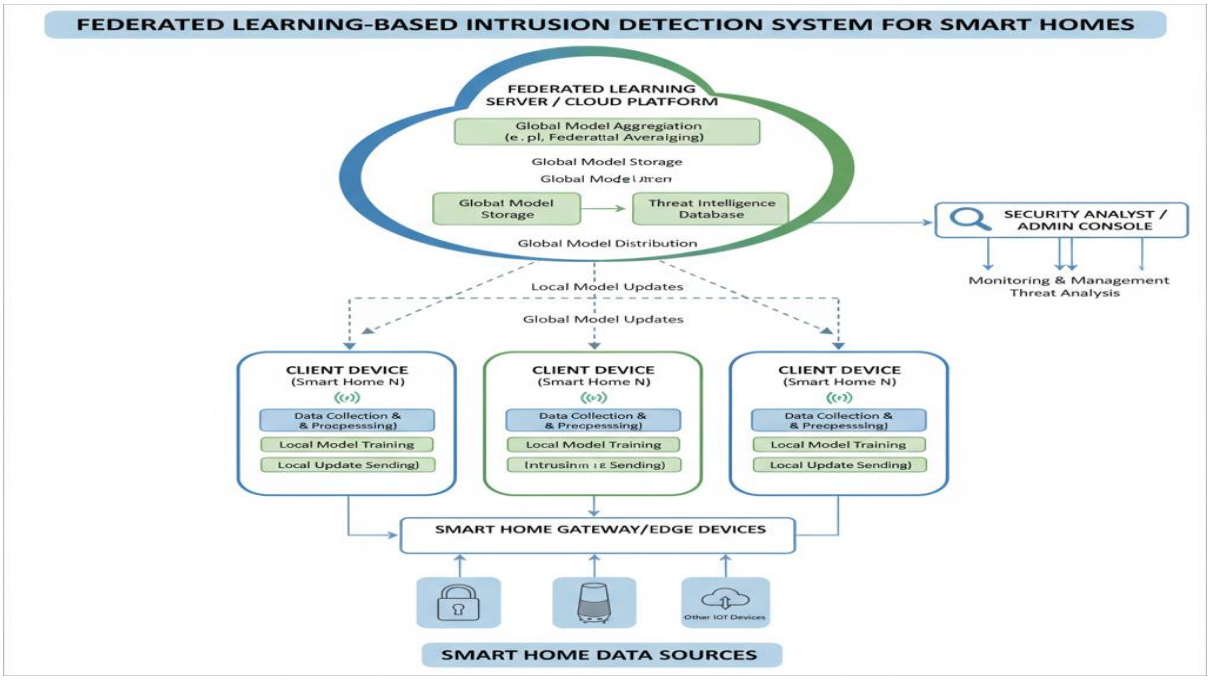
Block Diagram: Federated Learning system with IoT sensors and lightweight security



Key Components:

1. IoT Devices with Sensors:
   - Motion sensors, door/window sensors, smart locks, cameras, temperature/humidity sensors, etc.
2. Federated Learning Framework:
   - Aggregates model updates from individual devices to improve a global IDS model without sharing raw data on Local and Global models
3. Intrusion Detection Engine:
   - Uses statistical for pattern and profile recognition and Rule based models on maintaining threshold values to identify intrusions.
4. Communication Protocols:
   - Secure, lightweight communication between devices for model updates and coordination.

Architectural Diagram



Federated Learning Models

Local Level (Client-Side) Modeling

$$W_{t+1}^{k} = w_t - \eta \nabla F_k(w_t)$$

Where w refers to weight at the respective round, η refers to learning rate and F_k refers to loss function.

Global Level (Server-Side) Modeling

The central server maintains the global model. After clients finish local updates, they send their updated parameters W_{t+1}^{k} back to the server. The server aggregates these updates, typically by weighted averaging and sends back to local nodes. The process repeated till a final optimum value to attained being used for Intrusion detection purpose.

Security Model: Algorithms like ECC can be used for providing security to data in leight weight environments like IOT.

Sample data set for Different homes

Sample Home 1	Temp	Humidity	Motion	Light	Energy	Label
1	23	58	1	310	115	Occupied
	25	59	0	118	80	Idle
2	24	60	1	325	120	Occupied
	25	61	1	301	98	Idle
3	26	65	1	350	140	Occupied
	25	66	0	160	95	Idle

On exection in Federated Learning environment

Sample Home(Local)	Round 1 (Accuracy)	Round 2 (Accuracy)	Round 3 (Accuracy)	Round 4 (Accuracy)
1	.82	.82	.82	.82
2	.83	.83	.83	.83
3	.92	.92	.92	.92

Each Sample Home trains its data locally and only parameters which have value will be sent to central server.

Suitable algorithms of Machine Learning for IDS in Federated Learning environment are Common algorithms include: Logistic Regression, Random Forest, Autoencoders (anomaly detection) and LSTM for sequential sensor data

Sensor Reading

Sample Home	Time	Motion	Door	Activity
1	2 AM	1	Open	Suspicious

Research Challenges:

- Handling heterogeneous sensor data and inconsistent data quality.
- Designing lightweight FL models suitable for resource-constrained IoT devices.
- Balancing privacy, efficiency, and accuracy in real-time detection.
- Mitigating **poisoning** attacks or adversarial inputs in federated learning.

11. Conclusion

This work addresses the critical need for privacy-aware, decentralized intrusion detection in smart homes. By combining IoT sensors**,** federated learning**,** and anomaly detection, it aims to deliver a product that is both technically robust and aligned with the privacy expectations of modern users. Thus the defined architecture may have applications along with Rocket propulsion test facilities and also in Electric vehicle propulsion systems, Marine propulsion engines, Aircraft engine health monitoring and Smart industrial turbines

References

1. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). *Communication-Efficient Learning of Deep Networks from Decentralized Data*. In Proceedings of AISTATS 2017.
2. Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). *Advances and Open Problems in Federated Learning*. Foundations and Trends® in Machine Learning.
3. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). *Internet of Things: Vision, Applications and Research Challenges*. Ad Hoc Networks, 10(7), 1497-1516.
4. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). *Security, Privacy and Trust in Internet of Things: The Road Ahead*. Computer Networks, 76, 146-164.