

Data-Privacy Focused Federated Learning Framework for Industrial IoT

Component 01 - Attack Defense and Resilience

R25-039

Project Proposal Report

Nanayakkara Y.D.T.D - IT21826368

Supervisor - *Dr. Sanika Wijesekara*

Supervisor – *Mr. Amila Senerathne*

Co-Supervisor - *Mr. Tharaniyawarma Kumaralingam*

B.S.c (Hons) Degree in Information Technology Specialized in Cyber Security

Department of Computer Systems and Engineering

Sri Lanka Institute of Information Technology


Sri Lanka

January 2025

DECLARATOIN OF CANDIDATE AND STATEMENT BY SUPERVISOR

I declare that this is our own work, and this proposal does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any other university or institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to Sri Lanka Institute of Information Technology y the nonexclusive right to reproduce and distribute m y dissertation, in whole or in part of print, electronic or other medium. I retain the right to use this context as a whole or part in future works (such as articles or books)

Member Name	Registration Number	Signature	Date
Nanayakkara Y.D.T.D	IT21826368		1/23/2025

The candidate above is carrying out research for the undergraduate dissertation under supervision of the undersigned.

Name	Role
Dr. Sanika Wijesekara	Supervisor
Mr. Amila Senerathne	Supervisor
Mr. Tharaniyawarma Kumaralingam	Co-Supervisor

ABSTRACT

The Industrial Internet of Things has transformed industries by enabling real-time monitoring, predictive maintenance, and automation, but it also introduces significant cybersecurity risks. The distributed nature of Industrial Internet of Things systems and the interconnectivity of devices create a vast attack surface, making them prone to cyberattacks, including Distributed Denial of Service attacks, model poisoning, and Byzantine attacks. Federated Learning offers a promising solution to these challenges by enabling decentralized machine learning where sensitive data is never shared, ensuring privacy preservation. However, Federated Learning also faces its own set of security issues, including the potential for malicious updates and the vulnerability of decentralized networks to advanced cyberattacks.

This research proposes a scalable, robust, and privacy-preserving Federated Learning framework that enhances the security of Industrial Internet of Things systems. The proposed framework has four modules done by individual team members, Secure Aggregation, Secure command and control, Privacy preservation and attack defense and resilience. The last one is done and explains by this report which will be aims to detect anomalies in real-time, mitigate model poisoning and Byzantine attacks, and develop defense mechanisms to address emerging cyber threats. By leveraging lightweight machine learning techniques, secure aggregation methods, and advanced intrusion detection systems, this research addresses the challenges of resource-constrained Industrial Internet of Things devices while ensuring model integrity and operational continuity with the help of the module. The findings aim to contribute to the development of secure and resilient Federated Learning frameworks for Industrial Internet of Things systems, making them more resistant to evolving cyber threats and improving the overall security posture of industrial networks.

CONTENTS

1	INTRODUCTION	6
1.1	Background Study	7
1.2	Literature Review	9
1.3	Research Problem and Gap.....	11
2	RESEARCH OBJECTIVES.....	14
2.1	Main Objective	14
2.2	Specific Objectives	14
3	METHODOLOGY	15
3.1	Framework Diagram.....	15
3.2	Component Diagram.....	16
3.3	System Process	18
3.4	Work Breakdown Structure	20
3.5	Gantt Chart	21
3.6	Anticipated Results.....	21
3.7	Commercialization	21
4	PROJECT REQUIREMENTS	22
4.1	Functional Requirements.....	22
4.2	Non-functional requirements	22
4.3	User Requirements	22
4.4	Systems requirements	22
5	REFERENCES	23
6	APPENDICES	24
6.1	Plagiarism check - Turnitin	24

TABLE OF FIGURES

Table 1: Comparison of Existing solutions	11
Table 2: Comparison of Existing Attack-Defense Systems and Proposed ADR module	14
Table 3: WBS	20
Figure 1: Framework Diagram.....	15
Figure 2: Attack Defense Resilience Architecture	16
Figure 3: Process of the ADR module	18
Figure 4 Gantt Chart	21

LIST OF ABBREVIATIONS

IIoT	Industrial Internet of Things
ML	Machine Learning
FL	Federated Learning
APT	Advanced Persistent Threats
DDOS	Distributed Denial of Service
GDPR	General Data Protection Regulation
DP	Differential Privacy
HE	Homomorphic Encryption
SMPC	Secure Multi-Party Computation
IDS	Intrusion Detection System
FedAvg	Federated Averaging
ADR	Attack Detection and Resilience

1 INTRODUCTION

The ***Industrial Internet of Things (IIoT)*** has revolutionized industries by enabling real-time monitoring, predictive maintenance, and process optimization. However, this technological transformation also introduces a substantial increase in cybersecurity threats. The interconnected nature of IIoT devices, sensors, and systems creates an expansive attack surface, making cybersecurity a critical concern in safeguarding industrial operations.

To address these challenges, ***Machine Learning (ML)*** has become a vital tool in detecting, mitigating, and responding to cyber threats. One of the most promising advancements in this domain is ***Federated Learning (FL)***, introduced by researchers at Google in 2016. FL was developed as a decentralized approach to machine learning to address the limitations of traditional, centralized methods, which often compromise data privacy and scalability. Unlike conventional ML, FL enables collaborative model training across distributed devices without sharing raw data, ensuring privacy preservation and operational efficiency.

IIoT security research has evolved from traditional defenses to machine learning-based approaches, such as anomaly detection and behavior analysis, to address the complexity of distributed systems. Our framework integrates advanced techniques like Federated Learning (FL) for privacy-preserving model training, Secure Multi-Party Computation (SMPC) for data privacy, and anomaly detection for real-time threat response. While previous research has explored these methods, gaps remain in providing a unified solution that balances privacy, scalability, and security. Our framework addresses these gaps by offering a comprehensive and resilient IIoT security solution.

In this report, we propose a ***Secure Framework*** for IIoT systems that address all critical aspects, including data collection, learning, updating, communication, command execution, and attack defense. A key focus of this framework is the ***Attack Defense and Resilience Module***, a component within a data-privacy-focused FL framework. This module aims to detect, mitigate, and recover from sophisticated cyberattacks while maintaining the integrity of the learning process and ensuring system resilience.

1.1 Background Study

The Industrial IoT has revolutionized industries by enabling real-time monitoring, predictive maintenance, and process automation. However, the integration of heterogeneous IoT networks and resource-constrained devices introduces significant security challenges. Cybercriminals exploit vulnerabilities in IIoT systems to launch attacks, such as DDoS, malware propagation, and APTs. These attacks disrupt industrial processes, compromise sensitive data, and threaten operational continuity.

To counter these threats, the adoption of ML in IIoT has shown great promise. ML can detect anomalies, predict failures, and identify potential threats in real time. However, traditional ML approaches rely on centralized data collection, which is incompatible with the distributed nature of IIoT systems. The need for privacy preservation, scalability, and real-time analysis has driven the development of FL as a decentralized alternative.

Basics of FL

FL, first introduced by Google in 2016, is a machine learning paradigm that enables multiple devices or nodes to collaboratively train a shared model without exchanging raw data. Instead, each device trains a local model on its own data and shares only model updates like gradients or weights with a central server. The central server aggregates these updates to improve the global model. [1] This approach offers several benefits like Privacy Preservation way of sensitive data remains localized on the device, ensuring compliance with data protection regulations such as GDPR, Reduced Communication Overhead with Only model updates are transmitted, significantly lowering the bandwidth requirements compared to centralized data collection and Scalability. [2]

Despite its advantages, FL introduces new challenges and vulnerabilities. The distributed nature of FL opens the door to novel attack vectors that can compromise both the learning process and the integrity of the resulting models. [3]

In the FL systems mainly y there is the Client side and the Server side. They have their own responsibilities to ensure the whole process is done perfectly.

In the server, it is a Central server that has the model creation, aggregation of the client's data, orchestration of the overall training process of the global model, and communication with all. So, Clients are connected to the server as we called local clients, they have data locally so that the sensitive data would not be exposed, and with them the local model training, and after the whole uploading the data to the server the download or the update of the model. To the client there can be lots of heterogeneity devices, also it is the side of heterogeneity management of devices are done. [4]

Then there are types of FL models categorized based on types of clients and data they hold, if they are devices that are different like smartphones and IOT devices each with small amount of data lightweight called cross-Device FL then there is Cross-Silo which has different organizations like bunch of hospitals and like.

For all these FL methods there are mainly mechanisms that do data protection, like differential privacy homomorphic encryption, secure aggregation and secure multi partitioning computation, they will be explained more broadly by other reports that collaborate with this.

When focusing on Attack and Defense Mechanisms in FL hence the name is like a security guard that protects the process, mainly those systems are vulnerable to a variety of cyberattacks where the data will be, so the central server if the whole idea compromises the process of machine learning. What we are going to do is protect the collection part and the distribution so even if the client is exposed or affected it can be fixed easily.

Mainly attacks like Model Poisoning Attacks (MP) where Malicious devices introduce incorrect updates to corrupt the global model. And Byzantine Attacks, which Malicious nodes send arbitrary or misleading updates to disrupt the training process. Will be purely focused on this. Then there are attacks like Adversarial Attacks where craft inputs are designed to mislead the model into making incorrect predictions and Data Inference Attacks which will exploit model updates to infer sensitive information from other participants. Additionally, all other server and client related cyberattacks are also going to address here

These vulnerabilities highlight the importance of robust attack defense mechanisms within FL frameworks, particularly in IIoT environments. Effective defense mechanisms must address the unique challenges of FL, including the lack of centralized oversight, the heterogeneity of devices, and the need for real-time responses.

Basic Defense Mechanisms

Already in FL most of the problems were addressed by the researches and developers but it needs more attention and care with the evolvement of the technology like ai enhanced attack. Basically, in the FL it try to apply Secure Aggregation Protocols to ensure that updates from participants are encrypted and aggregated in a manner that prevents tampering or inference of sensitive data. Then also we have the advancement of the mechanisms like DP, HE and SMPC

In the most recent there are blockchain Integration, Using blockchain for verifiable and tamper-proof recording of updates and transactions. In the authentication and authorization side.

Also, for the attackers there are Anomaly Detection for Identifying and excluding malicious or outlier updates that could compromise the global model. And Intrusion detection Systems to monitor and apply solutions.

1.2 Literature Review

Research in IIoT security and Federated Learning for intrusion detection has yielded innovative approaches to tackle cyber threats, in every proposed FL-based IOT system this is similar in the human immune system that helps to mitigate attacks and ensure the FL integrity. With the evolution of security we have new, and secure command and control, more encrypted communication methods, privacy preservation hybrid methods and secure aggregation methods. [5]

In recent years FL with Blockchain Integration had popular in several studies proposing integrating FL with blockchain to enhance data integrity, trust, and decentralized model aggregation. Blockchain ensures that updates from IIoT devices are tamper-resistant and auditable. For example, researchers have utilized differential privacy (DP) and secure multi-party computation (SMPC) in conjunction with FL to mitigate data leakage risks while preserving performance. [3] [6]

One significant challenge in FL systems is label inference attacks, where attackers attempt to infer the labels or outcomes of private data held by participants. The concept of label leakage was first introduced by [7] who highlighted the risks of such attacks in vertically federated learning. FL systems can be divided into two types: model-divided federated learning, where data and labels are partitioned, and federated learning without model partitioning. Initially, partitioning was believed to offer better security, but recent research revealed vulnerabilities. Label leakage attacks exploit the leakage of labels to gain unauthorized access to private information. Additionally, gradient leakage attacks, such as iDLG (deep leakage of gradients), allow attackers to exploit gradient leaks for data reconstruction. These attacks, explored by [6], illustrate how gradients can inadvertently expose private information to defend against label inference attacks, decentralized training has been proposed as a method to unlink data from labels, making it more difficult for attackers to infer sensitive information. However, while defense mechanisms are well-researched, detection methods for label inference attacks remain underexplored. Most studies focus on preventing these attacks rather than detecting them post-incident. [6]

Federated Learning systems are also vulnerable to Byzantine attacks, which can be categorized as untargeted or backdoor attacks. Untargeted attacks degrade model performance or hinder convergence, while backdoor attacks allow the model to maintain normal performance but introduce malicious behavior. Research has identified several defense strategies against untargeted attacks, such as label flipping, random noise injection, and gradient inversion. Methods like MKrum, which aggregates model updates by selecting nearest neighbors, and Median and TrimMean, which use statistical techniques to average model parameters, have shown promise in mitigating such attacks. The Fragment Model Poisoning Attack (FMPA) has also been proposed, which targets specific dimensions of the model to evade defenses. This

attack manipulates the model's last layer, causing more effective and harder-to-detect attacks. Using datasets like Fashion-MNIST and CIFAR-10, FMPA attacks aim to degrade the accuracy of global models by exploiting fluctuations in updates. [8] [9]

In terms of intrusion detection in IoT networks, a model combining Long Short-Term Memory (LSTM) networks and autoencoders has been proposed to address routing attacks in RPL-based IoT networks. This hybrid machine learning structure predicts future behavior of IoT nodes during the routing process, with anomalies detected by comparing predicted and actual behaviors. The model operates in either a centralized or distributed architecture, continuously learning and evaluating traffic flow data to identify malicious nodes. The evaluation focuses on detecting four major routing attacks: Blackhole, Flooding, DODAG Version Number (VN) Attack, and Destination Reply (DR) Attack. Anomalies are detected when the current routing behavior deviates from predicted patterns, helping to assess node trustworthiness. [10]

Federated Learning in IIoT also faces challenges such as data poisoning, Byzantine faults, and model inversion attacks, which involve malicious devices sending harmful updates or exposing sensitive data. While Byzantine Fault Tolerance (BFT) mechanisms are commonly used, they struggle to scale in large industrial networks, leading to performance degradation. Additionally, these defense techniques introduce significant overhead, which may limit their effectiveness in IIoT environments where low latency and high accuracy are crucial. To counter these threats, machine learning-based Intrusion Detection Systems (IDS), such as decision trees (DT), support vector machines (SVM), and neural networks, have been employed for anomaly detection in IIoT. The distributed nature of FL allows these methods to work across edge devices, enhancing detection accuracy without compromising privacy. Furthermore, frameworks like Lightweight Authentication and Authorization Frameworks (LAAFFI), utilizing Distributed Ledger Technology (DLT), have been proposed to secure communication between IIoT devices, ensuring authentication, authorization, and accountability even in constrained environments. [7]

These defense strategies and detection techniques play a pivotal role in ensuring the security and efficiency of Federated Learning systems in IIoT environments. However, as the technology evolves, it is essential to continually develop more robust and scalable solutions that can address the increasingly sophisticated nature of cyber threats in IIoT networks.

1.3 Research Problem and Gap

Table 1: Comparison of Existing solutions

Work	Industrial IOT Related	FL - Related	Focused attack nature	Features	Limitations with Existing Defense
[7]	No	yes	Label Inference Attack	<ul style="list-style-type: none"> Model for label inference and model poisoning attacks 	<ul style="list-style-type: none"> Monitoring and anomaly detection for label leakage, training data subsampling, model regularization result in poor defense for other types of attacks.
[9]	Partially	yes	Model poisoning Attack	<ul style="list-style-type: none"> Attack Detection Secure. Aggregation Technical overview 	<ul style="list-style-type: none"> Limited to specific model poisoning defenses; same as secure aggregation methods.
[8]	No	yes	Fragment Model poisoning Attack	<ul style="list-style-type: none"> Also, for Byzantine attack defense 	<ul style="list-style-type: none"> FMPA focuses on attacking specific dimensions of the model, leveraging the inherent fluctuations in federated learning. Focused on secure aggregation methods and blocking clients.
[11]	No	yes	Byzantine attacks	<ul style="list-style-type: none"> Multi-Layered Defense Architecture Optimization Strategies for Robust Learning 	<ul style="list-style-type: none"> Focused on multiple client attacks and fault tolerance High computational power use Scalability issues Euclidean Distances like Ineffectiveness for Coordinated Attacks Increased Computational Demands
[10]	No, iot based	No	Blackhole Attack, Flooding Attack	<ul style="list-style-type: none"> Traffic Behavior Monitoring Anomaly Detection Predictive Analysis 	<ul style="list-style-type: none"> Scalability Issues Dynamic Attack Patterns Trust-based Routing Defenses
[12]	No	NO	IoT related anomaly defense	<ul style="list-style-type: none"> Attack Detection using ASAE (Adversarial Sparse Autoencoder) Data Normalization 	<ul style="list-style-type: none"> Adaptability to Dynamic Environments Lack of Real-Time Detection Resource Constraints in IoT Devices Handling Complex and Diverse Attacks

Despite advancements in FL and IIoT security, significant gaps remain:

1. Resilience Against Advanced Threats:

While FL provides distributed security, it remains vulnerable to advanced attacks such as backdoor attacks. In backdoor attacks, adversaries manipulate the global model without detection, compromising the system's effectiveness. Existing countermeasures, like differential privacy, are insufficient to address all forms of adversarial behavior and are unable to prevent these attacks entirely.

2. Energy and Resource Constraints:

IIoT devices typically operate under tight constraints in terms of computational power, memory, and energy. This makes it challenging to design energy-efficient and lightweight security solutions that do not compromise the accuracy of attack detection. Research in this area remains an open challenge, as most existing solutions fail to balance security with the limited resources available in IIoT devices.

3. Dynamic and Heterogeneous Environments:

IIoT systems are highly heterogeneous, consisting of devices with varying capabilities, connectivity, and operating conditions. Designing robust and scalable FL frameworks capable of detecting diverse attack patterns in such dynamic environments is a difficult task. Solutions must account for these variabilities while maintaining performance and security.

4. Data and Model Integrity:

Federated Learning relies on aggregating updates from numerous devices, which expose the system to potential poisoning and gradient inversion attacks. In gradient inversion attacks, adversaries exploit shared gradients in FL to reconstruct sensitive local data. Although cryptographic methods like homomorphic encryption are used to ensure privacy, they introduce significant computational overhead, limiting their practicality for resource-constrained IIoT devices.

5. Integration of Real-Time Feedback Loops:

Current research lacks strong integration of real-time intrusion detection and response mechanisms within FL frameworks for IIoT systems. Such mechanisms are essential for identifying and mitigating threats before they escalate into significant security breaches.

Specific Attack Types in IIoT and FL Frameworks should be addressed

- Model Poisoning Attacks
- Byzantine Attacks
- Data Poisoning Attacks
- Gradient Inversion Attacks
- Backdoor Attacks
- Distributed Denial of Service (DDoS)
- Eavesdropping and Man-in-the-Middle
- Adversarial Example Attacks

This research aims to address these gaps and challenges by enhancing attack defense and resilience mechanisms within a privacy-focused Federated Learning framework for IIoT systems. Specifically, it will explore efficient, lightweight methods to detect and prevent model poisoning, gradient inversion, backdoor attacks, and other adversarial threats in heterogeneous environments.

2 RESEARCH OBJECTIVES

2.1 Main Objective

To develop a Scalable, Robust, and Data-Privacy-preserving Federated Learning framework that enhances Machine learning in Industrial IoT systems.

2.2 Specific Objectives

To develop a scalable, lightweight, Attack Defense and Resilience Module that seamlessly integrated with the whole farmwork to enhance the security of IIoT systems by implementing real-time anomaly detection, mitigating model poisoning and Byzantine attacks, and proactively addressing evolving cyber threats.

So as the result of the Comparison of Existing Attack-Defense Systems and Proposed Framework, the proposed framework is expected to provide

Table 2: Comparison of Existing Attack-Defense Systems and Proposed ADR module

Aspect	Existing FL Attack-Defense Systems	Proposed Framework
Attack Detection Scope	Detects specific attacks like model or data poisoning	Covers model/data poisoning, gradient inversion, backdoor attacks, etc.
Byzantine Fault Tolerance	Limited scalability and efficiency in IIoT.	Scalable, combining FedAvg and anomaly detection (Autoencoders/Isolation Forests).
Attack Recovery	Limited focus of post-attack recovery and resilience.	Includes rollback, adaptive strategies, and learning from patterns.
Real-Time Defense	Rarely incorporates real-time feedback and response mechanisms.	Enables real-time detection and automated actions.
Cross-Device Collaboration	Limited collaboration and coordination among devices.	Improved coordination using decentralized anomaly sharing.
Defense Against Adversarial Attacks	Minimal focus on adversarial robustness in FL models.	Uses adversarial training and robust aggregation for protection.

3 METHODOLOGY

The methodology section outlines the systematic approach used to design, develop, and implement the proposed attack-detection system.

3.1 Framework Diagram

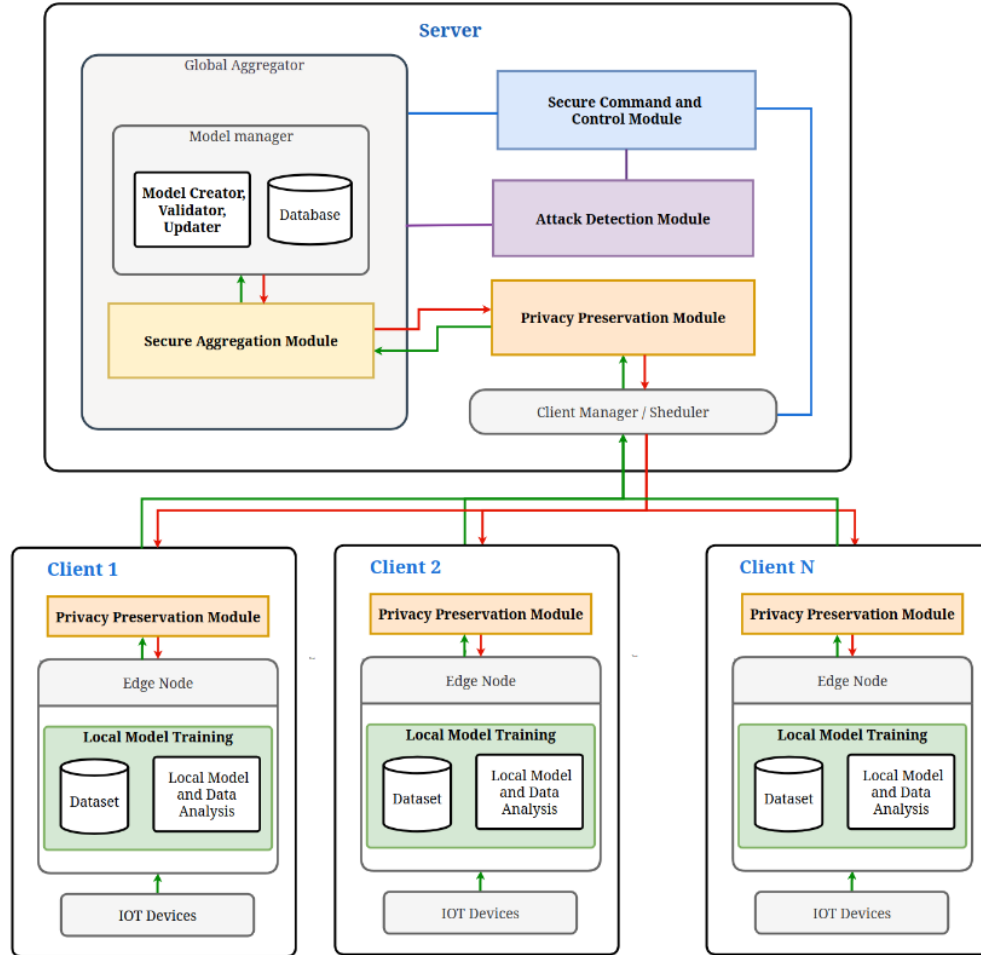


Figure 1: Framework Diagram

Member Name	Sub Objective
Nanayakkara Y.D.T. D	Attack Detection and Resilience
Mendis H.R.M	Privacy Preservation
Weerasinghe K.M.	Secure Aggregation
Dissanayaka K.D.A.R. A	Secure Command and Control

3.2 Component Diagram

The proposed attack detection system employs a hybrid architecture that integrates the following components to achieve the primary objective of detecting and mitigating security threats in real-time.

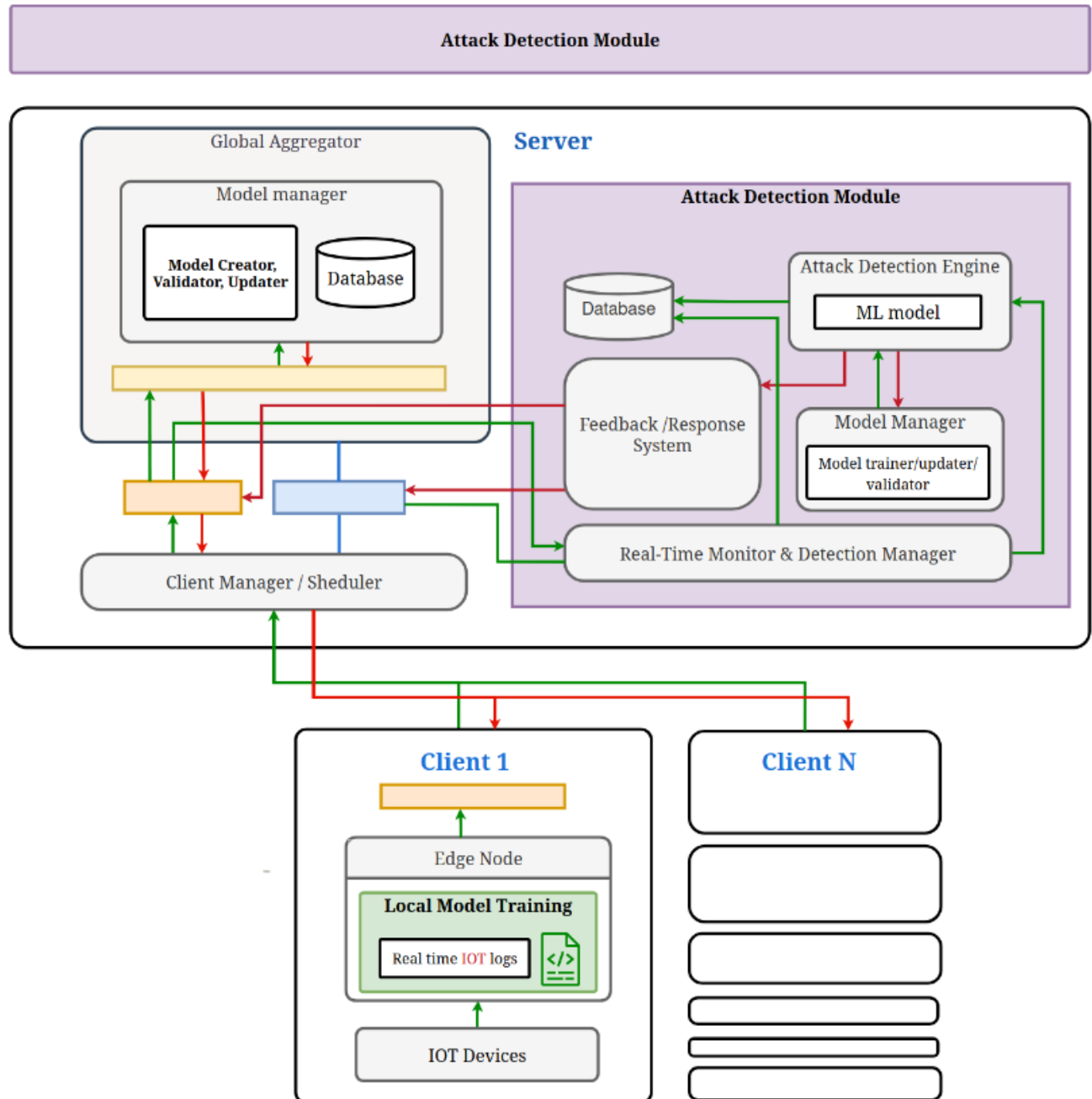


Figure 2: Attack Defense Resilience Architecture

Inside the Server Module

Global Aggregator: Which includes the model manager, database, Secure Aggregation module, Client manager.

- Model Manager: Manages machine learning models by creating, validating, and updating them.
- Database: Stores models, updates, and configurations required for global aggregation.
- Client Manager/Scheduler: Coordinates communication between clients and the server, scheduling updates and aggregations efficiently.

Attack Detection Module:

- Attack Detection Engine: Uses machine learning models to detect anomalies in received data.
- Feedback/Response System: Facilitates a secure feedback loop with clients, ensuring model updates and mitigating anomalies.
- Real-Time Monitor & Detection Manager: Monitors client activity and updates in real-time to detect deviations or threats.

In every Client side

Edge Nodes:

- Local Model Training: Performs local updates using real-time IoT data from sensors and devices.
- IoT Devices: Provide real-time logs for local model training.
- Client Communication:
- Encrypted channels are used for transmitting local model updates to the global server, ensuring secure aggregation.

3.3 System Process

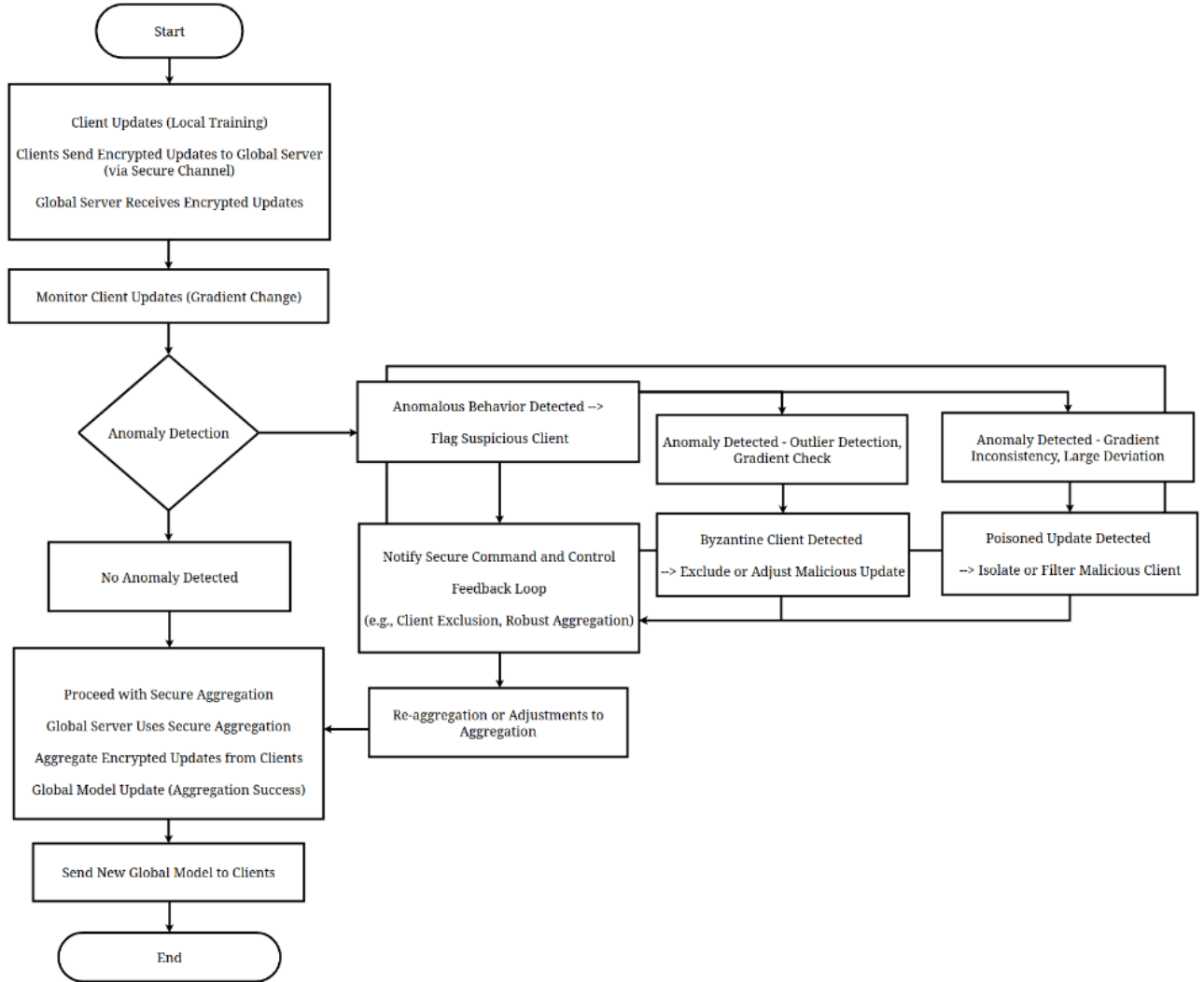


Figure 3: Process of the ADR module

The system follows a structured process to detect and mitigate attacks effectively:

1. Client Updates and Local Training
 - Each client performs localized model training using IoT logs, generating gradient updates.
2. Secure Transmission to the Server
 - Encrypted gradient updates are securely transmitted to the global server using a secure channel.
3. Monitoring and Anomaly Detection
 - The server monitors the received updates to detect anomalies such as gradient inconsistencies or large deviations. Detection methods include outlier detection, gradient inversion checks, and anomaly detection models like Isolation Forests or Autoencoders.
4. Real-Time Feedback and Defense
 - If an anomaly is detected:
 - Byzantine Fault Tolerance mechanisms exclude malicious updates.
 - Poisoned Updates are isolated or filtered.
 - The system adjusts aggregation methods to maintain robustness.
5. Global Model Update
 - The server performs secure aggregation and updates the global model, which is then distributed to clients.
6. Continuous Feedback Loop
 - The feedback system ensures iterative improvements, refining anomaly detection and model updates dynamically.

3.4 Work Breakdown Structure

This is the ADR Work Break down Structure

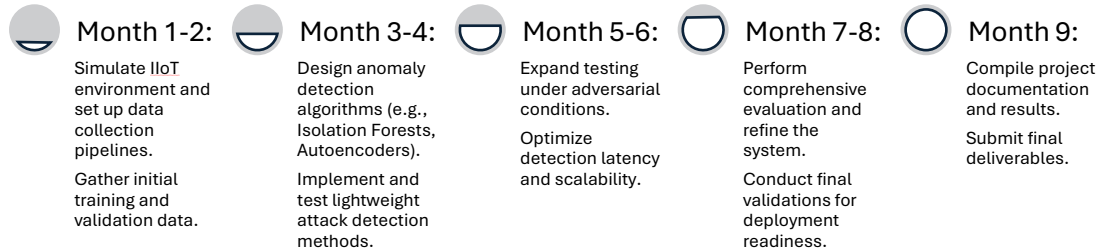


Table 3: WBS

WBS ID	Stage	Task	Description
1	IIoT Environment Setup	Simulate IIoT Environment	Create a simulated IIoT environment with heterogeneous devices.
1.1		Design Data Collection Pipelines	Set up pipelines to collect data from IIoT devices.
1.2		Collect Training Data	Gather normal and anomalous training data.
2	Machine Learning Development	Train Models	Train machine learning models using Isolation Forests and Autoencoders.
2.1		Build Attack Module	Develop modules for Byzantine and poisoning attack detection.
2.2		Test Initial Models	Perform initial testing of models.
3	Adversarial and Optimization	Adversarial Testing	Test models under adversarial conditions.
3.1		Optimize Performance	Enhance model scalability and reduce latency.
4	System Validation	Comprehensive Evaluation	Evaluate the system's performance across various metrics.
4.1		Refine System	Refine the system based on evaluation results.
5	Documentation and Integration	Compile Documentation	Document processes, results, and findings.
5.1		Integration with Other Modules	Integrate the developed system with existing frameworks or modules.
6	Deliverables	Submit Deliverables	Submit the final project deliverables.

3.5 Gantt Chart

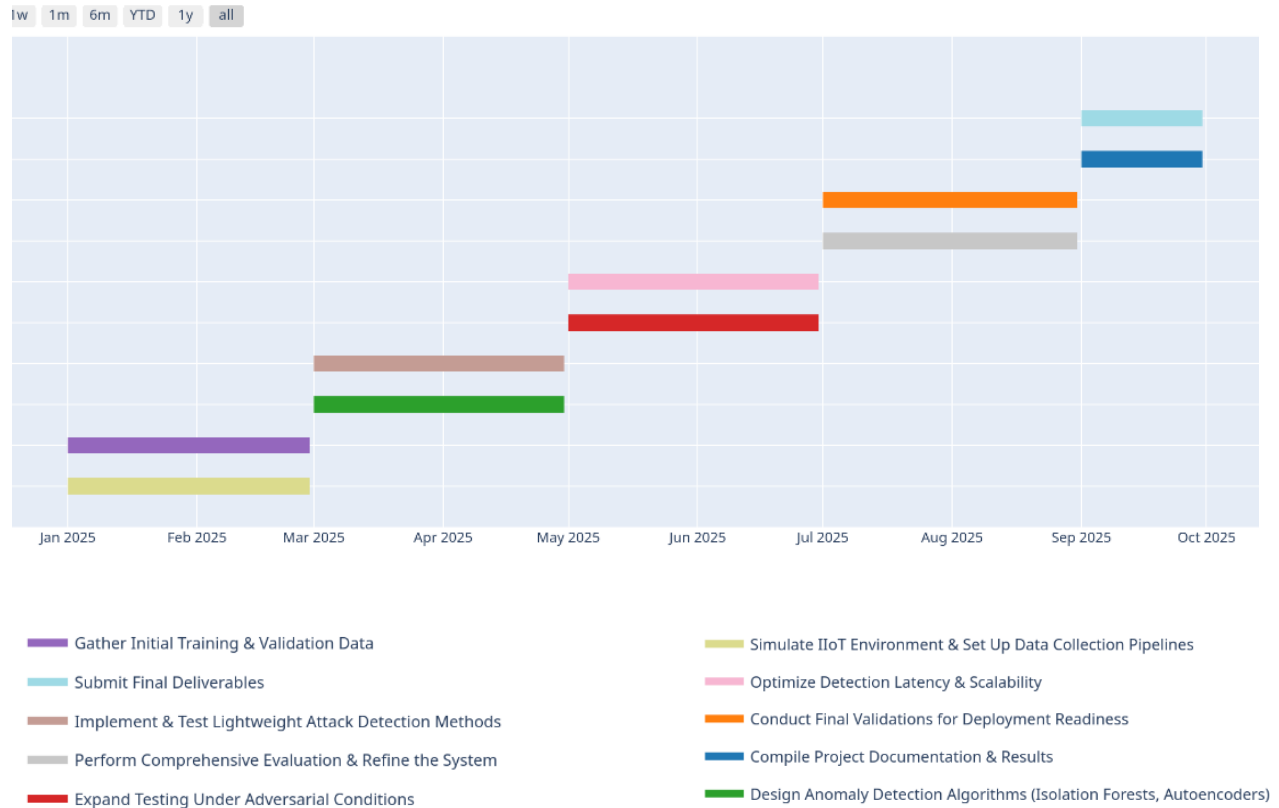


Figure 4 Gantt Chart

3.6 Anticipated Results

- The module will provide comprehensive attack detection and defense for FL systems, with enhanced privacy-preserving capabilities and real-time feedback mechanisms.
- It should be scalable and provide more efficiency, making it suitable for resource-constrained devices in IIoT environments.

3.7 Commercialization

The proposed framework can be commercialized by targeting sectors such as manufacturing, energy, and healthcare, where clients require a reliable security solution to protect their data and ensure ease of deployment. While the framework has not yet been discussed of the deployment in the market, it has the potential to be offered as a Software-as-a-Service (SaaS) model. This approach would provide scalable, plug-and-play IIoT security solutions tailored to meet the specific needs of various industries.

4 PROJECT REQUIREMENTS

4.1 Functional Requirements

- Federated Learning-based attack detection module.
- Lightweight resource utilization.
- Heterogeneity attack adaptation.

4.2 Non-functional requirements

- High scalability to accommodate diverse IIoT devices.
- Minimal latency for real-time operations.
- Energy-efficient design is suitable for constrained devices.

4.3 User Requirements

A Federated Learning system framework ensuring data confidentiality, integrity, and availability while providing scalability and robustness for industrial environments. This includes:

- Privacy-preserving intrusion detection.
- A secure command-and-control workflow.
- Real-time anomaly detection and response.
- Seamless integration with existing IIoT ecosystems.

4.4 Systems requirements

- Hardware: Computational power, if external hardware needed (Raspberry Pi)
- Software: Python, TensorFlow, libraries and other related tools.
- Resources: Datasets for training and evaluation, simulation tools for IIoT scenarios.


5 REFERENCES

- [1] "google.com," google, 2017. [Online]. Available: <https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/>.
- [2] *, ., K. S. a. ., S. W. a. ., F. G. a. ., Y. G. Nguyen Truong a, "Privacy preservation in federated learning: An insightful survey from the GDPR perspective".
- [3] M. A. 1. 2. a. U. B. 1. 2, "Federated Learning For IoT: Applications, Trends, Taxonomy, Challenges, Current Solutions, and Future Directions," January, 2024..
- [4] P. i. F. Learning, "Privacy in Federated Learning," 2024.
- [5] E. D. *, "Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications".
- [6] S. P. R. M. Q.-V. P. K. D. Parimala M, "Fusion of Federated Learning and Industrial Internet of Things: A Survey".
- [7] H. B. 1. ., Q. L. 2. F. Z. 3. *. Z. Z. 4. J. H. 5. a. S. D. 6. Liansheng Ding 1, "Threshold Filtering for Detecting Label Inference Attacks in Vertical Federated Learning".
- [8] X. C. C. Q. Zhiqiang Ren, "FMPA: Fragment Model Poisoning Attack in Federated Learning," 2024.
- [9] A. D. H. K. G. S. a. R. M. P. Abbas Yazdinejad, "A Robust Privacy-Preserving Federated Learning Model Against Model Poisoning Attacks," 2024.
- [10] K. Ahmadi, "A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation," 2024.
- [11] 2. G. V. R. Sahithi Godavarthi1, "Federated Learning's Dynamic Defense Against Byzantine Attacks: Integrating SIFT-Wavelet and Differential Privacy for Byzantine Grade Levels Detection," 2024.
- [12] K. S. Prasad, "Augmenting cybersecurity through attention based stacked autoencoder with optimization algorithm for detection and mitigation of attcks on IoT assisted networks.," 2024.

6 APPENDICES

6.1 Plagiarism check - Turnitin

Tharindu Nanayakkara | User Info | Messages | Student | English | Community | Help






Class PortfolioMy GradesDiscussionCalendar

NOW VIEWING: HOME > 4TH YEAR IT 1ST SEMESTER 2025 > 4TH YEAR ASSIGNMET

About this page

This is your assignment dashboard. You can upload submissions for your assignment from here. When a submission has been processed you will be able to download a digital receipt, view any grades and similarity reports that have been made available by your instructor.

> 4th year Assignmet ?

Paper Title	Uploaded	Grade	Similarity
draft - PPReport - IT21826368 - Attack Defense and Resilience.pdf	03 Feb 2025 20:06	--	<div><div></div>9%</div> <div></div>