

**DATA-PRIVACY  
FOCUSED  
FEDERATED LEARNING FRAMEWORK  
FOR  
INDUSTRIAL IOT**

R25 - 039

# PROJECT GROUP

## Team



Nanayakkara Y.D.T.D  
IT21826368



Mendis H.R.M  
IT21822612

## Supervisors



Mr. Amila Nuwan Senarathne  
Supervisor



Weerasinghe K.M  
IT21831904

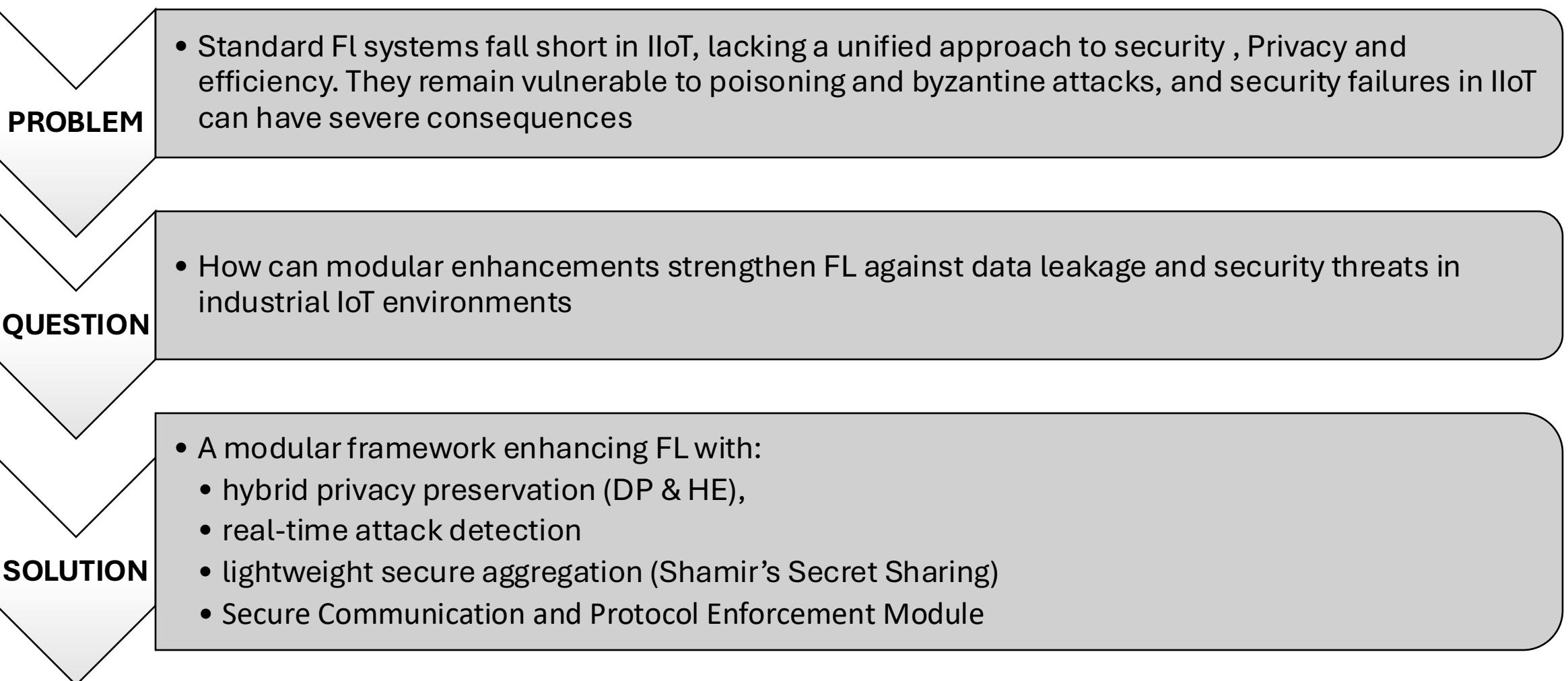


Dissanayaka K.D.A.R.A  
IT21828348



Mr. Tharaniwarma Kyumaralingam  
Co-Supervisor

# RESEARCH FOCUS



# OBJECTIVES

## MAIN OBJECTIVES

Design and implement a secure and efficient Federated Learning framework for Industrial IoT that ensures privacy, resilience, and reliability.

## SUB OBJECTIVES

- Boost Resilience: Real-time detection & mitigation of poisoning/Byzantine threats.
- Secure Aggregation: Hide individual updates & ensure fault tolerance.
- Secure Communication: Prevent eavesdropping & tampering.
- Evaluate Framework: Measure security, privacy & efficiency in IIoT.

# PROVEN GAPS AND LIMITATIONS

- **Data Leakage:** Standard FL is prone to inference attacks, compromising client data privacy.
- **Ineffective Defenses:** Lacks real-time detection for advanced threats like model poisoning and Byzantine attacks.
- **Insecure Communications:** channels often lack robust security, risking tampering.

# FRAMEWORK COMPONENTS

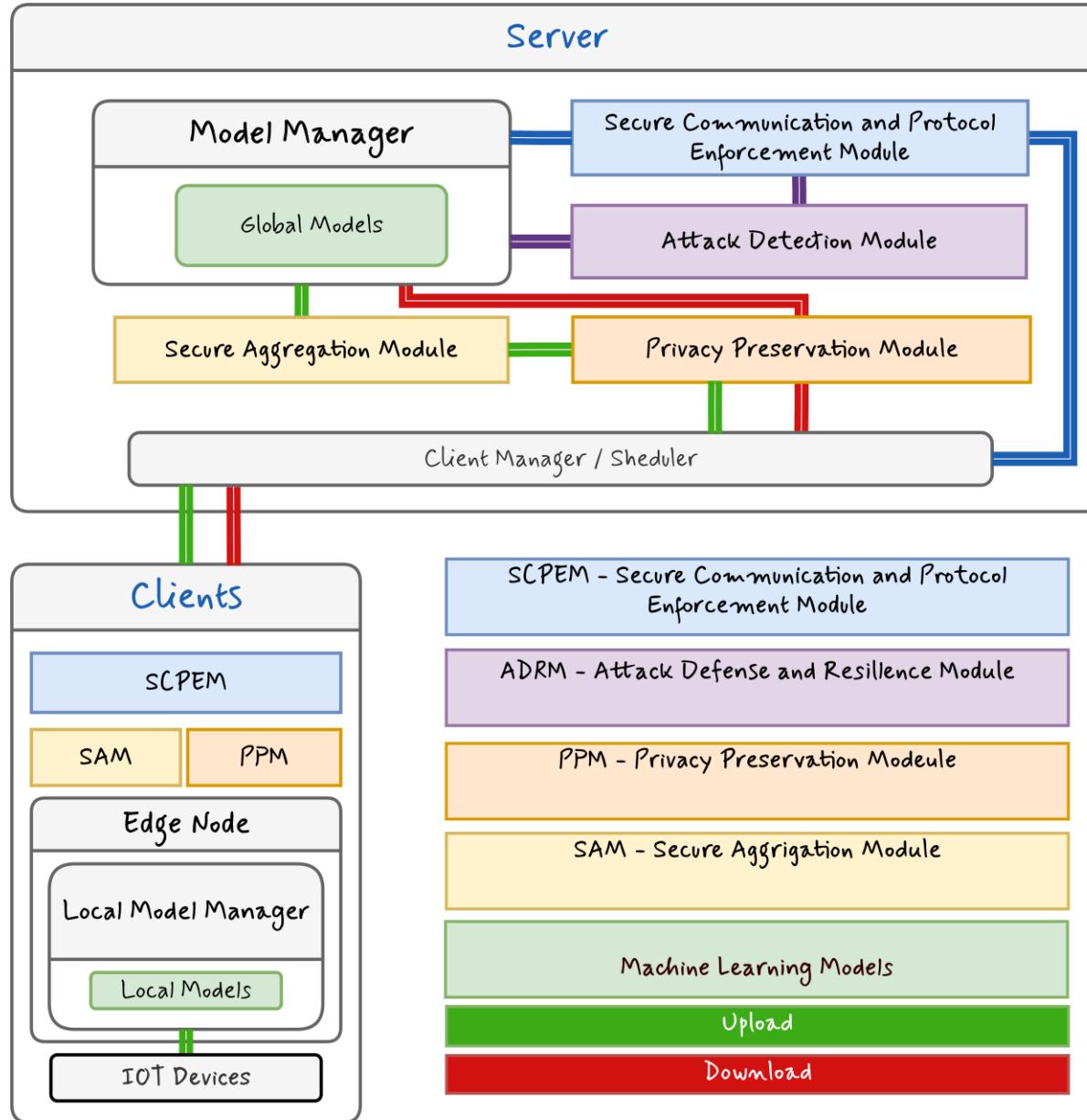
**Attack Defence  
And Resilience  
Module**

**Privacy  
Preservation  
Module**

**Secure  
Aggregation Module**

**Secure  
Communication and  
Protocol  
Enforcement Module**

# OVERALL ARCHITECHTURE



- **Modular Design:** Security & privacy integrated in stages of FL
- **Core Components:** Server + Distributed Individual Clients
- **Server:** Orchestrates FL, manages models, coordinates clients, Logging & Monitoring
- **Clients:** Train locally; share only secure updates.
- Security Modules:
  - **SCPM** – Secure communication and protocol enforcement module
  - **ADRM** – Attack Detection & Resilience module
  - **PPM** – Privacy Protection module
  - **SAM** – Secure Aggregation module

# Proposed System – Frontend Terminal User Interface(TUI)

Federated Learning Framework v2.0 2025-09-15 12:15:23

(1) Overview | (2) Model Manager | (3) Client Health | (4) Modules | (5) Logs | (6) TUI Details

## Overview

**Server Overview**

Server State:	Online
Progress:	Round 0 of 1
Round Duration:	N/A
Last Aggregation:	No aggregation yet

**Orchestrator**

Is Training In Progress:	True
Current State:	WAITING_FOR_UPDATES
Current Round:	1
Number:	
Total Rounds:	100
Clients Per Round:	3
Updates Received:	2
Selected Clients:	3
Count:	
Round Start Time:	1757918572.9624703
Round Timeout:	1000

**Secure Aggregation Module**

Aggregation:	SecAgg
Protocol:	
Security Level:	High
Updates In Queue:	2
Failed Sessions:	0
Last Aggregation:	N/A
Time:	
Status:	active

**Attack Defense And Resilience Module**

Status:	running_ml_mode
Blocked Clients:	0
Count:	
Champion Is:	False
Trained:	
Challenger Is:	True
Trained:	
Challenger:	2
Training Buffer Size:	
Performance:	Champion: 0.0 Challenger: 0.0
History:	[]

**Client Manager**

Total Clients:	3
Connected Clients:	3
Status Checker:	True
Running:	

**Model Manager**

Version:	0
Status:	N/A

**Privacy Preserving Module**

Module Name:	PPM
Status:	active
Epsilon:	1.0
Delta:	1e-05
Is Active:	True
Description:	Privacy-Preserving Mechanism for policy auditing.

**Server Communication And Protocol Enforcement Module**

Module Name:	SCPM
Status:	active
TLS Enabled:	False
Client:	False
Authentication:	
Enabled:	
Last Security Event:	System initialized.
Active Protocols:	gRPC, REST API
Description:	Manages communication protocols and server state.

## Client Health Status (Total: 3, Active: 3, Blocked: 0)

Client ID	Status	Reputation	Uptime	Client Type	Details
client_2	Connected	100	0:06:08	gRPC	unknown
client_1	Connected	100	0:06:08	gRPC	unknown
client_80	Connected	100	0:02:31	gRPC	unknown

## Recent Logs

2025-09-15 12:15:21 INFO	Dashboard status updated: Connected clients count is 3.
2025-09-15 12:15:21 INFO	Preparing global model for client client_1 for round 1.
2025-09-15 12:15:21 INFO	127.0.0.1 [15/Sep/2025:12:15:21 +0530] "GET /api/overview HTTP/1.1" 200 655 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 12:15:21 INFO	127.0.0.1 [15/Sep/2025:12:15:21 +0530] "GET /api/model/metrics_details HTTP/1.1" 200 389 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 12:15:21 INFO	127.0.0.1 [15/Sep/2025:12:15:21 +0530] "GET /api/client_health HTTP/1.1" 200 1383 "-" "Python/3.10 aiohttp/3.12.15"

# Proposed System – Model Manager

Federated Learning Framework v2.0 2025-09-15 02:28:45

(1) Overview | (2) Model Manager | (3) Client Health | (4) Modules | (5) Logs | (6) TUI Details

Model Manager | p: Plot | +/-: Scroll

Model Status  
Model Version: 38  
Convergence Status: Training  
Last Update: 2025-09-15 02:27:08

Best Performance  
Accuracy: 33.88%  
Loss: 1.8766

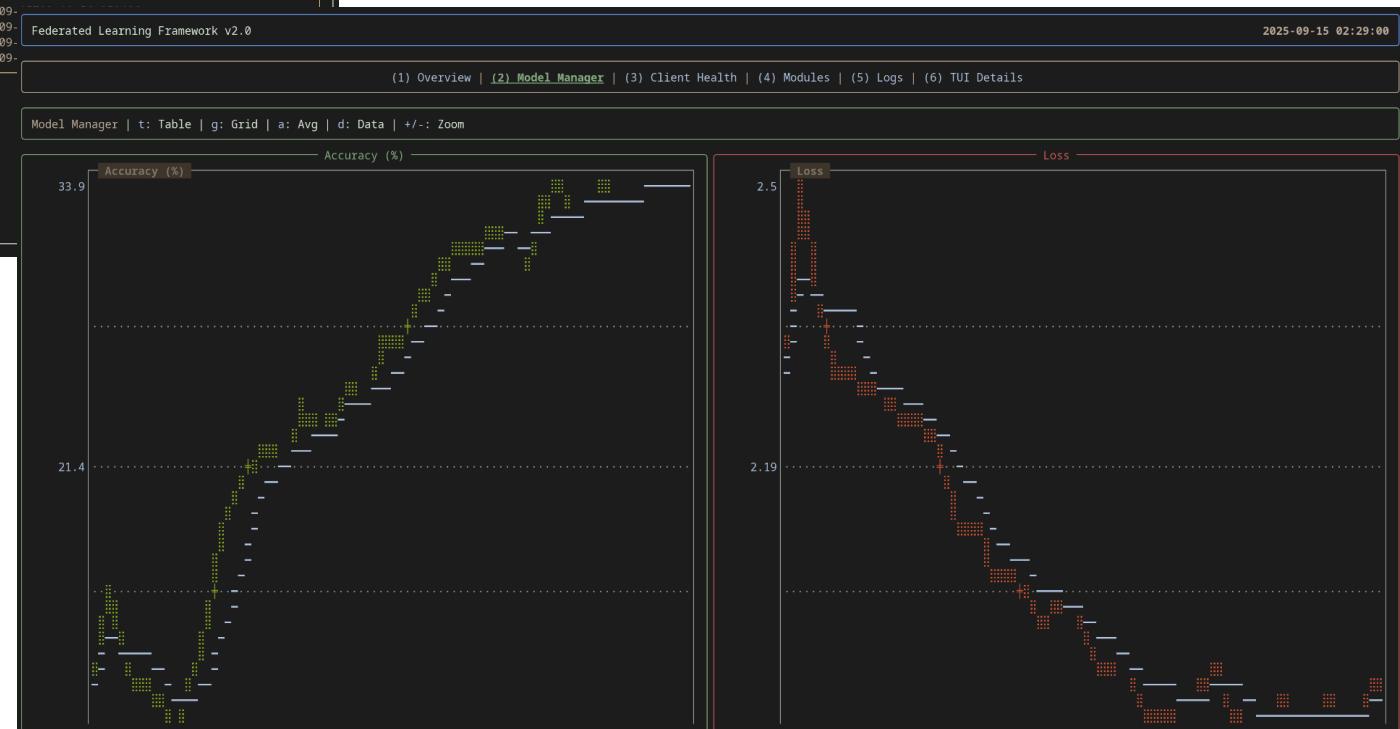
Training Progress  
Round 38/100 (38.00%)

Round	Accuracy (%)	Loss	Agg. Method	Timestamp
1	11.26	2.2831	N/A	2025-09-15T02:16:57.462493
2	15.06	2.5019	N/A	2025-09-15T02:17:08.320216
3	11.73	2.3586	N/A	2025-09-15T02:17:18.971671
4	10.74	2.2818	N/A	2025-09-15T02:17:28.893967
5	10.58	2.2850	N/A	2025-09-15T02:17:39.329314
6	8.89	2.2720	N/A	2025-09-15T02:17:49.392638
7	11.27	2.2657	N/A	2025-09-15T02:17:59.638800
8	14.22	2.2307	N/A	2025-09-15T02:18:09.879189
9	18.33	2.2386	N/A	2025-09-15T02:18:20.727648
10	20.64	2.2072	N/A	2025-09-15T02:18:30.348283
11	21.21	2.1592	N/A	2025-09-15T02:18:41.717847
12	21.50	2.1091	N/A	2025-09-
13	20.87	2.1053	N/A	2025-09-
14	24.07	2.0629	N/A	2025-09-
15	22.56	2.0506	N/A	2025-09-

Showing rows 1-15 of 38. Use +/- to scroll.

Img 2: Global model plot

Img 1: Global model table



# Proposed System – Client Manager

Client Health Status									
Client ID	Status	Reputation	Latency (ms)	Uptime	Client Type	Last Success Rnd	IP Address	Last Heartbeat	Details
client_2	Connected	100	N/A	0:05:07	gRPC	0	unknown	2025-09-15 06:44:17 UTC	
client_1	Connected	100	N/A	0:05:07	gRPC	0	unknown	2025-09-15 06:44:16 UTC	
client_80	Connected	100	N/A	0:01:30	gRPC	0	unknown	2025-09-15 06:44:15 UTC	

Img 3: Client Health table

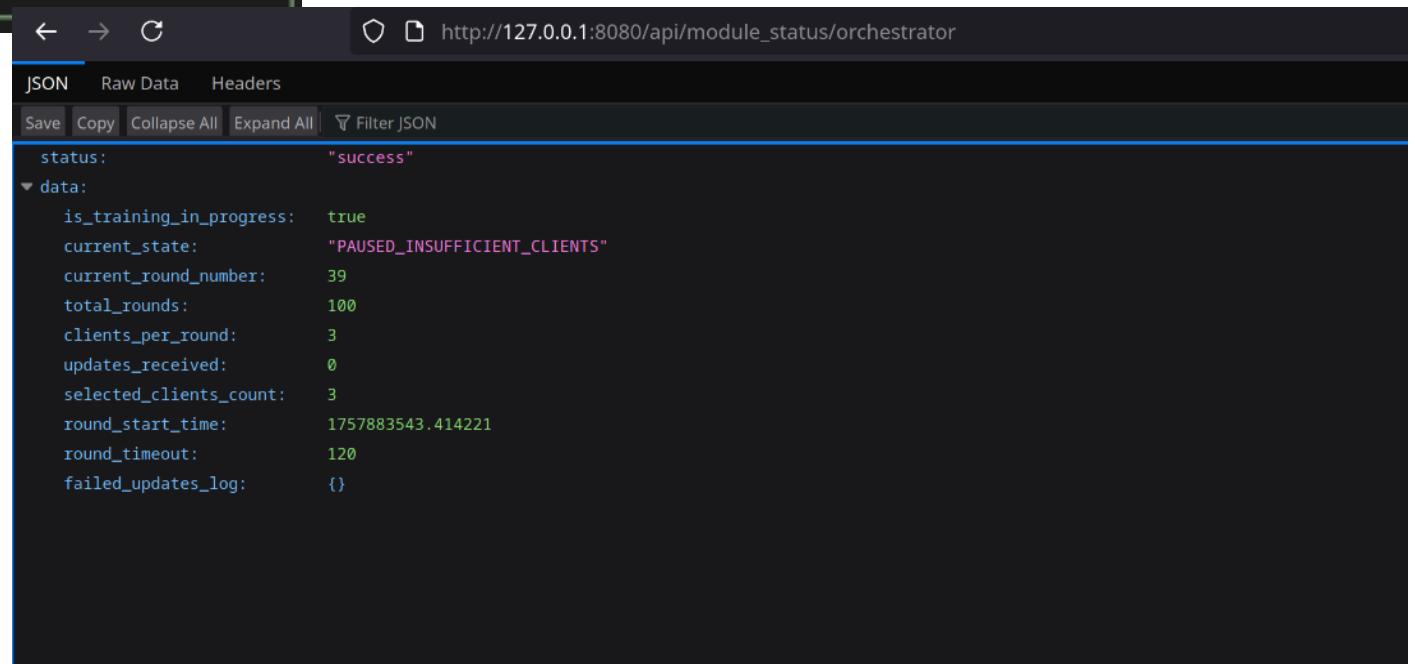
# Proposed System – Orchestration

Orchestrator

Is Training In True  
Progress:  
Current State: PAUSED\_INSUFFICIENT\_CLIENTS  
Current Round 39  
Number:  
Total Rounds: 100  
Clients Per 3

Img 4: training round details

Img 5: Orchestrator API



The screenshot shows a browser developer tools Network tab with a single request listed. The URL is `http://127.0.0.1:8080/api/module_status/orchestrator`. The response is a JSON object:

```
status: "success"
data:
  is_training_in_progress: true
  current_state: "PAUSED_INSUFFICIENT_CLIENTS"
  current_round_number: 39
  total_rounds: 100
  clients_per_round: 3
  updates_received: 0
  selected_clients_count: 3
  round_start_time: 1757883543.414221
  round_timeout: 120
  failed_updates_log: {}
```

# System process –Frontend – API calls

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 1024
Date: Mon, 18 Sep 2023 02:32:32 GMT
Connection: keep-alive
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.12-1+ubuntu22.04.1+deb.sury.org+1

{
    "status": "success",
    "data": [
        {
            "asctime": "2025-09-15 02:32:32,676",
            "levelname": "INFO",
            "name": "ServerControlPlaneManager",
            "process": 17691,
            "thread": 140431767912640,
            "funcName": "update_client_count",
            "lineno": 212,
            "message": "Dashboard status updated: Connected clients count is 4.",
            "component": "ServerControlPlaneManager"
        },
        {
            "asctime": "2025-09-15 02:32:32,678",
            "levelname": "WARNING",
            "name": "Orchestrator",
            "process": 17691,
            "thread": 140431767912640,
            "funcName": "prepare_model_for_client",
            "lineno": 115,
            "message": "Denied model request from client_2. Orchestrator state is 'PAUSED_INSUFFICIENT_CLIENTS'.",
            "component": "Orchestrator"
        },
        {
            "asctime": "2025-09-15 02:32:34,612",
            "levelname": "INFO",
            "name": "aiohttp.access",
            "process": 17691,
            "thread": 140431767912640,
            "funcName": "log",
            "lineno": 214,
            "message": "127.0.0.1 [15/Sep/2025:02:32:34 +0530] \"GET /api/overview HTTP/1.1\" 200 688 \"Python/3.10 aiohttp/3.12.15\"",
            "remote_address": "127.0.0.1",
            "request_start_time": "[15/Sep/2025:02:32:34 +0530]",
            "first_request_line": "GET /api/overview HTTP/1.1",
            "response_status": 200,
            "response_size": 688,
            "request_header": {
                "Referer": null
            }
        }
    ]
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 1024
Date: Mon, 18 Sep 2023 02:32:32 GMT
Connection: keep-alive
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.12-1+ubuntu22.04.1+deb.sury.org+1

{
    "status": "success",
    "data": {
        "status": "running",
        "uptime_seconds": 1394,
        "connected_clients": 4,
        "last_heartbeat_timestamp": 1757884838,
        "modules": {
            "client_manager": {
                "total_clients": 4,
                "connected_clients": 4,
                "status_checker_running": true
            },
            "model_manager": {
                "model_version": 39,
                "last_node_update": "2025-09-15 02:29:17",
                "training_progress": "39/100",
                "status": "ready",
                "comprised": false
            },
            "aggregation_summary": {
                "first_aggregation": null,
                "last_aggregation": null
            },
            "secure_aggregation_module": {
                "aggregation_protocol": "SecAgg",
                "security_level": "High",
                "updates_in_queue": 0,
                "failed_sessions": 0,
                "last_aggregation_time": "2025-09-15 02:29:17",
                "status": "active"
            },
            "attack_detection_response_module": {
                "status": "running_ml_mode",
                "blocked_clients_count": 0,
                "champion_is_trained": false,
                "challenger_1_is_trained": true,
                "challenger_2_is_trained": false,
                "challengers_training_buffer_size": 17
            },
            "performance": {
                "champion": 0.0 (±0),
                "challenger": 0.0 (±0),
                "history": []
            },
            "privacy_preservation_module": {}
        }
    }
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 1024
Date: Mon, 18 Sep 2023 02:32:32 GMT
Connection: keep-alive
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.12-1+ubuntu22.04.1+deb.sury.org+1

{
    "status": "success",
    "data": [
        {
            "metrics_history": [
                {
                    "round": 1,
                    "timestamp": "2025-09-15T02:16:57.462493",
                    "aggregation_method": "homomorphic_aggregation",
                    "metrics": {
                        "accuracy": 11.26,
                        "loss": 2.28309572122658
                    }
                },
                {
                    "round": 2,
                    "timestamp": "2025-09-15T02:17:08.320216",
                    "aggregation_method": "homomorphic_aggregation",
                    "metrics": {
                        "accuracy": 15.06,
                        "loss": 2.501911580942239
                    }
                },
                {
                    "round": 3,
                    "timestamp": "2025-09-15T02:17:18.971671",
                    "aggregation_method": "homomorphic_aggregation",
                    "metrics": {
                        "accuracy": 11.73,
                        "loss": 2.3586631433882986
                    }
                },
                {
                    "round": 4,
                    "timestamp": "2025-09-15T02:17:28.893967",
                    "aggregation_method": "homomorphic_aggregation",
                    "metrics": {
                        "accuracy": 18.74,
                        "loss": 2.281817973799087
                    }
                },
                {
                    "round": 5,
                    "timestamp": "2025-09-15T02:17:39.329314",
                    "aggregation_method": "homomorphic_aggregation",
                    "metrics": {
                        "accuracy": 18.58,
                        "loss": 2.28499679960263
                    }
                }
            ]
        }
    ]
}
```

```
('GET', '/api/status', self.get_server_status),
('GET', '/api/overview', self.get_overview_data),
('GET', '/api/orchestrator_progress', self.get_orchestrator_progress),

# Model & Metrics
('GET', '/api/metrics', self.get_model_metrics_data),
('GET', '/api/metrics_history', self.get_metrics_history),
('GET', '/api/model/metrics_details', self.get_model_metrics_details),
('GET', '/api/model', self.get_global_model_json),
('GET', '/api/model/bytes', self.get_global_model_bytes),
('POST', '/api/submit_update', self.submit_model_update),
('GET', '/api/evaluate_model', self.evaluate_model),

# Client Status
('GET', '/api/client_health', self.get_client_health),
('GET', '/api/client_privacy_methods', self.get_client_privacy_methods),
('GET', '/api/client_heartbeat', self.client_heartbeat),

# System Internals & Logs
('GET', '/api/logs', self.get_logs),
('GET', '/api/module_status/mm', self.get_mm_status),
('GET', '/api/module_status/sam', self.get_sam_status),
('GET', '/api/module_status/adrm', self.get_adrm_status),
('GET', '/api/module_status/ppm', self.get_ppm_status),
('GET', '/api/module_status/scpm', self.get_scpm_status),
('GET', '/api/module_status/orchestrator', self.get_orchestrator_status),

# Admin Endpoints for ADRM
('POST', '/api/admin/adrm/unblock/{client_id}', self.admin_unblock_client),
('DELETE', '/api/admin/adrm/history/{client_id}', self.admin_reset_client_history),
('PUT', '/api/admin/adrm/config', self.admin_update_adrm_config),
```



# Attack Detection and Resilience

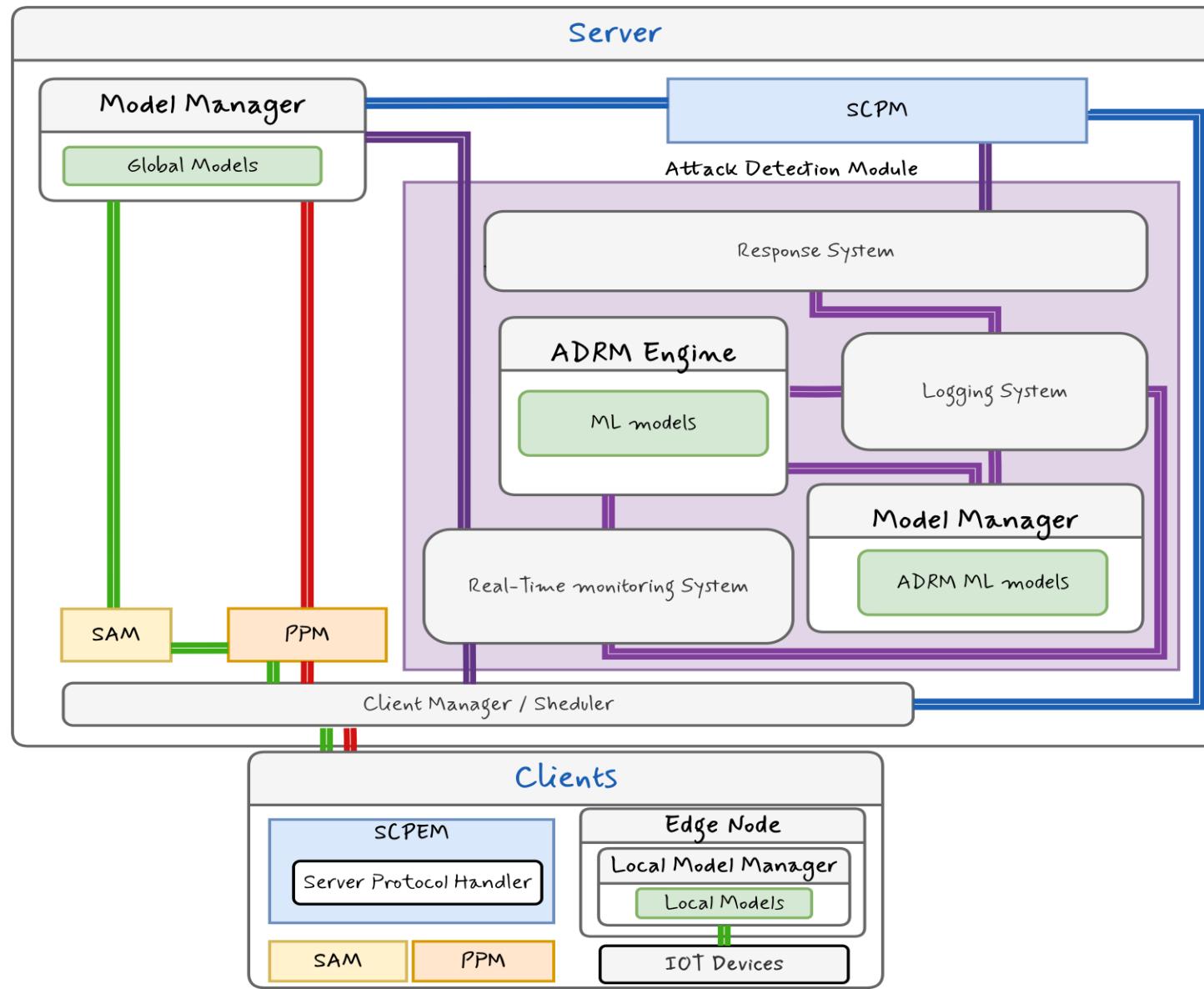
IT21826368 | Nanayakkara Y.D.T.D

- **Background**
  - Federated learning is a promising privacy preserving solution for IIoT security, but its decentralized nature create a new and significant attack surface for malicious actors
  - **Significance** : Without active defenses, Global model integrity is at risk, making robust security vital for industrial applications
- **RESEARCH GAP**
  - **Limitations**: Existing FL defenses are siloed, Targeting single threats, and its also too resource heavy for scalable IIoT
  - High Overhead makes many solutions impractical for IIoT. Also, There are not any unified lightweight approach
- **RESEARCH PROBLEM**
  - How can we design and integrate a lightweight, scalable, and effective attack detection and resilience system directly into the Federated Learning process to protect the global model's integrity in real-time?

# SOLUTION: ATTACK DETECTION & RESILIENCE MODULE

- **Main Objective:** To develop a scalable and lightweight module that enhances the security of FL in IIoT by detecting and mitigating malicious activities in real-time
- The Multi-Layered Approach:
  - **Real-Time Anomaly Detection:** Detects malicious updates with unsupervised learning
  - **Enhanced Resilience:** Ensures continuity with recovery mechanisms like rollbacks
  - **Client reputation grading system** – Reduce client points based on detection

# DEVELOPED SOLUTION – MODULE ARCHITECTURE



# ADRM ARCHITECTURE

Attack Defense And Resilience Module   Privacy Preserving Module   Secure Aggregation Module   Server Communication And Protocol Enforcement Module				
Status:		Attack Defense And Resilience Module Details		
Blocked Clients Count:		running_ml_mode		
Champion Is Trained:		0		
Challenger Is Trained:		False		
Challenger Training Buffer Size:		False		
Performance:		12		
		Champion: 0.0		
		Challenger: 0.0		
		History: []		
Client Health Status (Total: 4, Active: 3, Blocked: 1)				
Client ID	Status	Reputation	Details	
client_1	Connected	100	unknown	
client_2	Connected	100	unknown	
client_3	Blocked	75	Flagged as a statistical outlier compared to peers in the same round.	
client_4	Connected	100	unknown	

Img 1: reputation grading and client blocking

# DETECTION & MITIGATION PROCESS FLOW

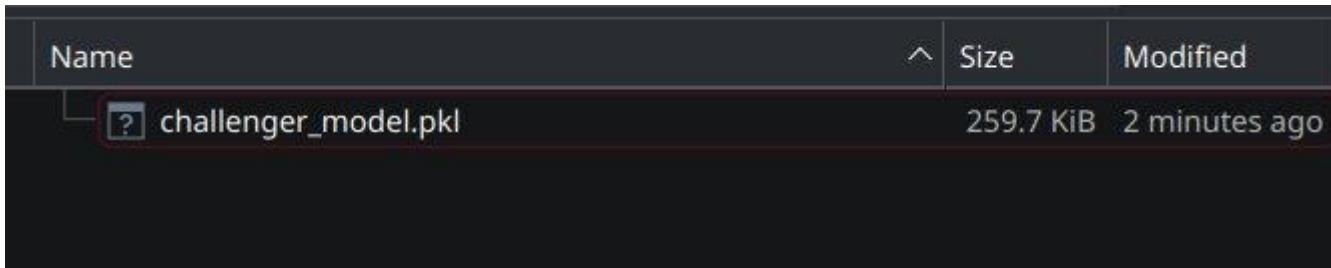


- Clients send encrypted updates via secure channels
- ADRM analyzes gradients, flags deviations
- Detects model anomalies
- Isolates/filter malicious clients; only verified updates aggregated
- Blocks and reduce reputation

# Attack detection and Defense

```
python3 main.py ~/D/F/s/TUI
Federated Learning Framework v2.0
2025-09-14 02:24:55
(1) Overview | (2) Model Manager | (3) Client Health | (4) Modules | (5) Logs | (6) TUI Details
Modules
Attack Defense And Resillence Module | Privacy Preserving Module | Secure Aggrigation Module | Server Communication And Protocol Enforcement Module
Status: running
Total Updates Processed: 181
Suspicious Updates Detected: 1
Blocked Clients Count: 1
Learned Clients Count: 3
Attack Defense And Resillence Module Details
Currently Blocked Clients
Client ID Reason Blocked At
client_1 Update magnitude 0.1513 exceeded threshold (3.0 std devs from mean 0.0754) 2025-09-14T02:22:14.291929
```

# DETECTION METHOD



Created ML Model for anomaly detection

# Monitoring and Logging

```
1 | 2025-09-15 01:44:30,497 - ADRM General - INFO - Initializing ADRM ML Model Manager...
2 | 2025-09-15 01:44:30,498 - ADRM General - WARNING - Model file not found at database/adrm_models/champion_model.pkl. Creating a new, untrained model.
3 | 2025-09-15 01:44:30,498 - ADRM General - WARNING - Model file not found at database/adrm_models/challenger_model.pkl. Creating a new, untrained model.
4 | 2025-09-15 01:44:30,498 - ADRM General - INFO - ADRM ML Model Manager initialized.
5 | 2025-09-15 01:44:48,331 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
6 | 2025-09-15 01:44:48,546 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
7 | 2025-09-15 01:44:48,993 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
8 | 2025-09-15 01:44:58,593 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
9 | 2025-09-15 01:44:58,871 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
10 | 2025-09-15 01:44:59,264 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
11 | 2025-09-15 01:44:59,264 - ADRM General - WARNING - Client 'client_3' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round.
12 | 2025-09-15 01:44:59,268 - ADRM General - WARNING - High severity anomaly for 'client_3'. Update quarantined for review.
13 | 2025-09-15 01:46:59,268 - ADRM General - INFO - Client 'client_3' unblocked. Duration expired.
14 | 2025-09-15 01:47:00,998 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
15 | 2025-09-15 01:47:01,142 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
16 | 2025-09-15 01:47:10,813 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
17 | 2025-09-15 01:47:15,912 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
18 | 2025-09-15 01:47:16,892 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
19 | 2025-09-15 01:47:16,892 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
20 | 2025-09-15 01:47:17,20,402 - ADRM General - WARNING - Client 'client_2' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round.
21 | 2025-09-15 01:47:20,404 - ADRM General - WARNING - High severity anomaly for 'client_2'. Update quarantined for review.
22 | 2025-09-15 01:49:20,401 - ADRM General - INFO - Client 'client_2' unblocked. Duration expired.
23 | 2025-09-15 01:49:21,281 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
24 | 2025-09-15 01:49:26,987 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
25 | 2025-09-15 01:49:27,367 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
26 | 2025-09-15 01:49:31,622 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
27 | 2025-09-15 01:49:31,622 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
28 | 2025-09-15 01:49:37,765 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
29 | 2025-09-15 01:49:42,688 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
30 | 2025-09-15 01:49:47,881 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
31 | 2025-09-15 01:49:47,882 - ADRM General - INFO - Challenger training buffer full. Triggering retraining.
32 | 2025-09-15 01:49:47,882 - ADRM General - INFO - Training Isolation Forest on 20 samples...
33 | 2025-09-15 01:49:48,417 - ADRM General - INFO - Training complete.
34 | 2025-09-15 01:49:48,553 - ADRM General - INFO - Model saved successfully to database/adrm_models/challenger_model.pkl
35 | 2025-09-15 01:49:48,556 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
36 | 2025-09-15 01:49:48,559 - ADRM General - WARNING - Response triggered for 'client_3'. Severity: high. Reason: Flagged as a statistical outlier compared to peers in the same round.
37 | 2025-09-15 01:49:59,137 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
38 | 2025-09-15 01:49:59,240 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
39 | 2025-09-15 01:50:04,057 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
40 | 2025-09-15 01:50:09,557 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
41 | 2025-09-15 01:50:09,775 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
42 | 2025-09-15 01:50:09,775 - ADRM General - WARNING - Client 'client_1' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round.
43 | 2025-09-15 01:50:09,775 - ADRM General - WARNING - High severity anomaly for 'client_1'. Update quarantined for review.
44 | 2025-09-15 01:52:10,322 - ADRM General - INFO - Client 'client_1' unblocked. Duration expired.
45 | 2025-09-15 01:52:10,362 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
46 | 2025-09-15 01:52:14,617 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
47 | 2025-09-15 01:52:29,129 - ADRM General - WARNING - Prediction skipped: model is not trained yet. Approving by default.
48 | 2025-09-15 01:52:29,128 - ADRM General - WARNING - Client 'client_1' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round.
49 | 2025-09-15 01:52:29,130 - ADRM General - WARNING - High severity anomaly for 'client_1'. Update quarantined for review.
50 | 2025-09-15 01:54:20,128 - ADRM General - INFO - Client 'client_1' unblocked. Duration expired.
```

## Model creation based on dataset in the current FL system

## Attack detection

```
1 | 2025-09-15 01:44:59,267 - WARNING - CROSS-CLIENT outlier detected: client_3 with Z-Score=7.43
2 | 2025-09-15 01:44:59,267 - WARNING - Response triggered for 'client_3'. Severity: high. Reason: Flagged as a statistical outlier compared to peers in the same round.
3 | 2025-09-15 01:44:59,267 - WARNING - Client 'client_3' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round. | Reputation Penalty: -25 points.
4 | 2025-09-15 01:44:59,267 - INFO - Blocklist with 1 clients saved to file.
5 | 2025-09-15 01:46:59,269 - INFO - Client 'client_3' unblocked. Duration expired.
6 | 2025-09-15 01:46:59,271 - INFO - Blocklist with 0 clients saved to file.
7 | 2025-09-15 01:47:28,403 - WARNING - CROSS-CLIENT outlier detected: client_2 with Z-Score=5.22
8 | 2025-09-15 01:47:28,401 - WARNING - Response triggered for 'client_2'. Severity: high. Reason: Flagged as a statistical outlier compared to peers in the same round.
9 | 2025-09-15 01:47:28,403 - WARNING - Client 'client_2' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round. | Reputation Penalty: -25 points.
10 | 2025-09-15 01:47:28,403 - INFO - BlockList with 1 clients saved to file.
11 | 2025-09-15 01:49:28,412 - INFO - Client 'client_2' unblocked. Duration expired.
12 | 2025-09-15 01:49:28,414 - INFO - BlockList with 0 clients saved to file.
13 | 2025-09-15 01:50:09,778 - WARNING - CROSS-CLIENT outlier detected: client_1 with Z-Score=4.38
14 | 2025-09-15 01:50:09,778 - WARNING - Response triggered for 'client_1'. Severity: high. Reason: Flagged as a statistical outlier compared to peers in the same round.
15 | 2025-09-15 01:50:09,778 - WARNING - Client 'client_1' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round. | Reputation Penalty: -25 points.
16 | 2025-09-15 01:50:09,779 - INFO - Blocklist with 1 clients saved to file.
17 | 2025-09-15 01:52:09,779 - INFO - Client 'client_1' unblocked. Duration expired.
18 | 2025-09-15 01:52:09,778 - WARNING - CROSS-CLIENT outlier detected: client_1 with Z-Score=4.98
19 | 2025-09-15 01:52:09,778 - WARNING - Response triggered for 'client_1'. Severity: high. Reason: Flagged as a statistical outlier compared to peers in the same round.
20 | 2025-09-15 01:52:09,778 - WARNING - Client 'client_1' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round. | Reputation Penalty: -25 points.
21 | 2025-09-15 01:52:29,129 - WARNING - Client 'client_1' blocked for 2 minutes. Reason: Flagged as a statistical outlier compared to peers in the same round. | Reputation Penalty: -25 points.
22 | 2025-09-15 01:52:29,129 - INFO - Blocklist with 1 clients saved to file.
23 | 2025-09-15 01:54:20,129 - INFO - Client 'client_1' unblocked. Duration expired.
24 | 2025-09-15 01:54:20,129 - INFO - Blocklist with 0 clients saved to file.
25 |
```



# Privacy Preservation

IT21822612 | Mendis H.R.M

- **BACKGROUND**

Federated Learning enables decentralized model training but remains vulnerable to inference attacks from untrusted servers. Combining **Differential Privacy (DP)** for noise and **Homomorphic Encryption (HE)** for secure communication provides a hybrid solution to protect client data.

- **RESEARCH GAP**

Existing Federated Learning methods use either Differential Privacy or Homomorphic Encryption alone, failing to provide full protection without compromising accuracy or efficiency, especially in resource-limited IIoT settings.

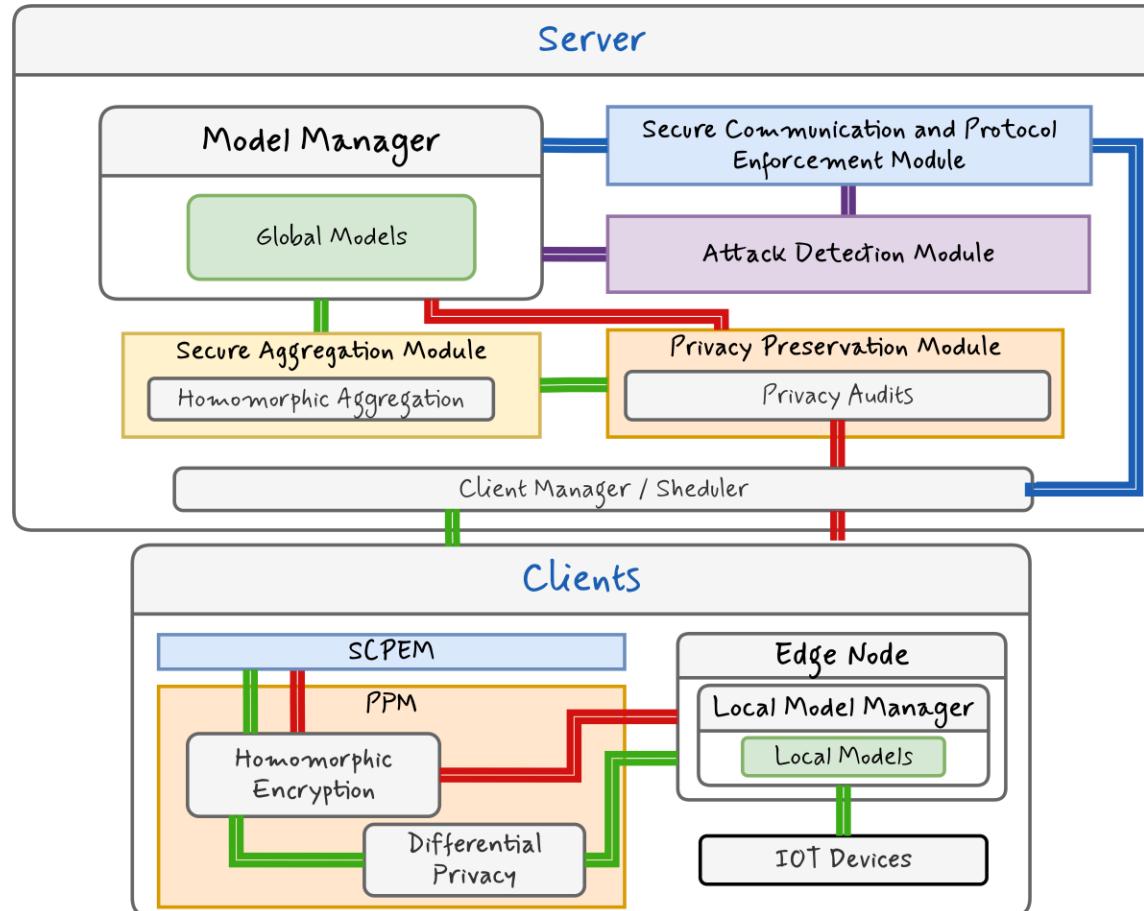
## **RESEARCH PROBLEM**

How can we design a hybrid Federated Learning framework combining Differential Privacy and Homomorphic Encryption to protect client data from inference attacks by untrusted servers while maintaining model accuracy and communication efficiency?

# SOLUTION:

- A hybrid privacy-preserving Federated Learning framework that combines **Differential Privacy (DP)** to add noise during training and **Homomorphic Encryption (HE)** to secure communication of model updates. This approach protects client data from inference attacks by untrusted servers while balancing model accuracy and communication efficiency, tailored for resource-constrained Industrial IoT environments.

# PPM Architecture



# METHODOLOGY

## Approach:

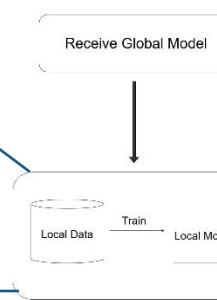
- Analyze existing FL privacy vulnerabilities.
- Combine HE and DP for enhanced privacy.
- Optimize techniques for IIoT-specific constraints.
- Validate Using real-world Datasets

## Key Techniques:

- **Homomorphic Encryption (HE):** Encrypts gradients, allowing computations on encrypted data without decrypting it. Prevents data leakage even if adversaries intercept communications.
- **Differential Privacy (DP):** Ensure that individual data points cannot be separated by adding controlled noise to gradients. Balances model accuracy with privacy

# FUNCTIONAL UNITS & IMPLEMENTATIONS (Client)

```
def load_and_train_model(epochs=5):
    """Load data and train the model with the given number of epochs."""
    logging.debug("[MODEL] Loading data and starting training")
    x_train, y_train, x_test, y_test = load_data()
    model = get_model()
    model = train_local_model(model, x_train, y_train, x_test, y_test, epochs)
    logging.info("[MODEL] Training completed")
    return model, x_test, y_test
```

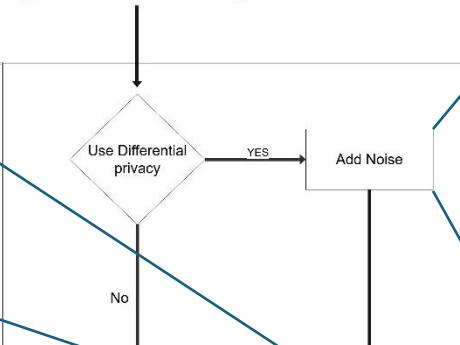


```
# Encrypt weights if HE is used
if "HE" in mode:
    enc_weights = [encrypt(w, context) for w in weights]
    comm_bytes += sum([w.numel() * w.element_size() for w in weights]) # estimate comm
    client_weights.append(enc_weights)
else:
    comm_bytes += sum([w.numel() * w.element_size() for w in weights])
    client_weights.append(weights)
```

```
# Create a TenSEAL context (CKKS scheme)
def create_context():

    context = ts.context(
        ts.SCHEME_TYPE.CKKS,
        poly_modulus_degree=16384,
        coeff_mod_bit_sizes=[60, 40, 40, 60]
    )
    context.generate_galois_keys()
    context.global_scale = 2**40
    return context

# Encrypt a tensor
def encrypt(tensor, context):
    flat = tensor.detach().cpu().flatten().tolist()
    enc = ts.ckks_vector(context, flat)
    return enc, tensor.size()
```



```
# DP functions for testing
class DifferentialPrivacyHandler:
    def __init__(self, noise_multiplier=0.2):
        """
        noise_multiplier : Controls scale of Gaussian Noise
        """
        self.noise_multiplier = noise_multiplier
        logging.debug(f"[DP INIT] Noise Multiplier set to {self.noise_multiplier}")

    def add_noise_to_weights(self, weights):
        """
        Add Gaussian noise to model weights
        """
        logging.debug("[DP] Starting to add noise to weights")
        noisy_weights = []
        for idx, w in enumerate(weights):
            noise = np.random.normal(loc=0.0, scale=self.noise_multiplier, size=w.shape)
            noisy_w = w + noise
            noisy_weights.append(noisy_w)
        logging.info("[DP] Successfully added noise to all model weights")
        return noisy_weights
```

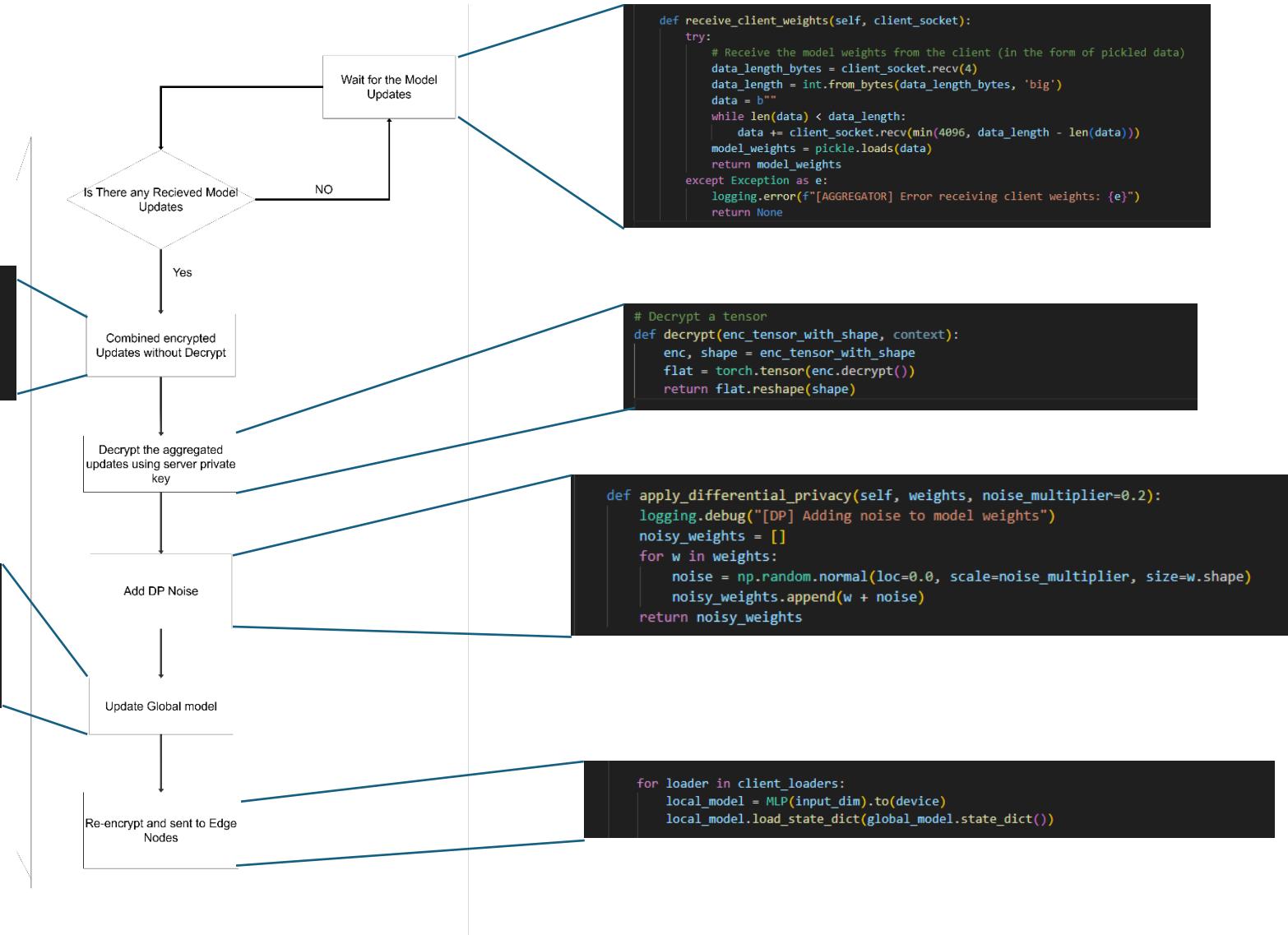
```
def send_model_weights(model):
    """
    Serialize the model weights after adding DP noise
    """
    try:
        logging.debug("[SEND] Extracting model weights")
        weights = model.get_weights()

        logging.debug("[SEND] Applying Differential Privacy to weights")
        noisy_weights = dp_handler.add_noise_to_weights(weights)

        logging.debug("[SEND] Serializing noisy weights for transmission")
        model_weights = pickle.dumps(noisy_weights)

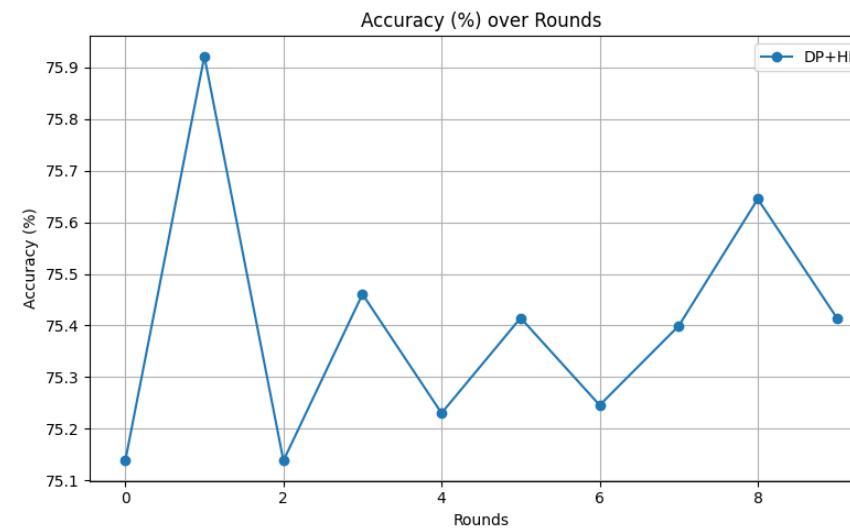
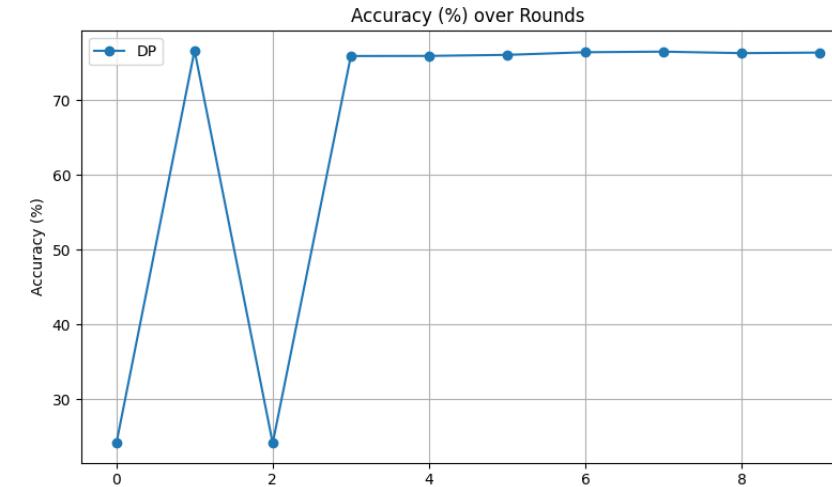
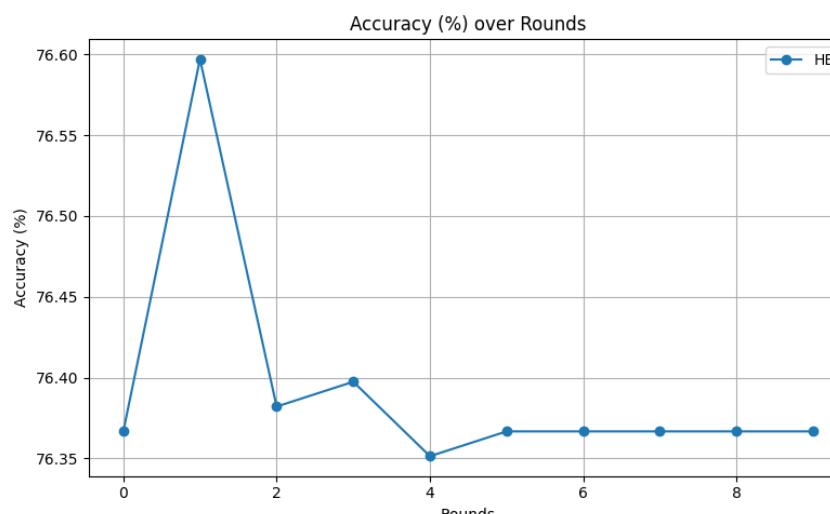
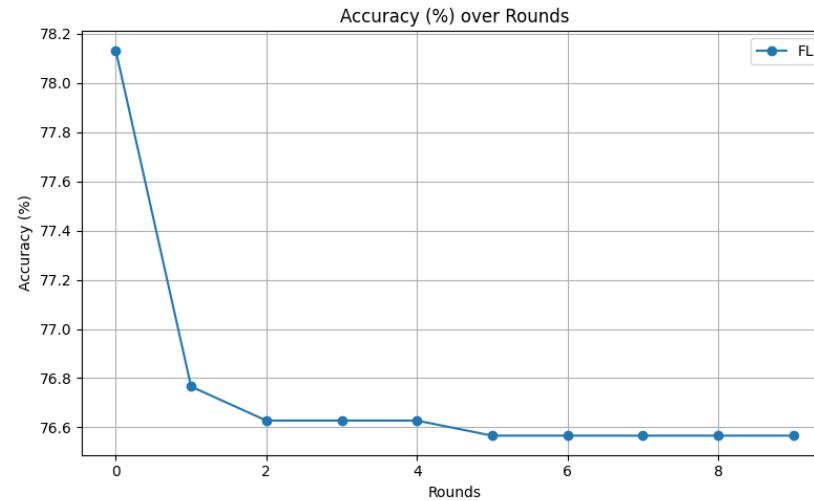
        logging.info("[SEND] Model weights successfully noise-added and serialized")
        return model_weights
    except Exception as e:
        logging.error("[SEND] Error during weight processing: {e}")
        return None
```

# FUNCTIONAL UNITS & IMPLEMENTATIONS (Server)



# PROOFS & RESULTS

- Accuracy Curves



Note: Testing was done using UCI Adult Dataset.

# PROOFS & RESULTS

## Average Accuracy over Rounds

Mode	Average Accuracy (%)	Remarks
FL	76.81	Highest accuracy because no extra privacy mechanisms are applied.
FL + DP	65.87	~11% Lower accuracy due to Differential Privacy adds <b>noise</b> to gradients to protect individuals.
FL + HE	76.39	Differential Privacy adds <b>noise</b> to gradients/weights to protect individuals. Homomorphic Encryption protects updates <b>without changing the data</b> (no noise).
FL + DP + HE	75.34	Accuracy only slightly lower than FL (~1.5% drop)

FL + DP + HE is the best choice, balancing utility and privacy. FL alone has the highest accuracy but no privacy. DP offers strong privacy with lower accuracy, while HE protects only communication. Combining DP and HE gives strong privacy with minimal accuracy loss, making it both practical and secure.

# Evidence of Completion

```
2025-04-07 00:54:03,110 - DEBUG - [DP INIT] Noise Multiplier set to 0.2
Connected to server at 127.0.0.1:5001 from static port 6001.
2025-04-07 00:54:15,729 - INFO - Waiting to receive initial model from the server.
2025-04-07 00:54:15,733 - INFO - Expecting 670665 bytes of model data.
2025-04-07 00:54:15,738 - INFO - Successfully received 670665 bytes of model data.
2025-04-07 00:54:15,739 - INFO - [RECEIVE] Successfully deserialized model weights (bytes)
2025-04-07 00:54:15,739 - DEBUG - [MODEL] Loading data and starting training
2025-04-07 00:54:17,836 - DEBUG - [MODEL] Creating new model instance
```

```
● (venv) PS C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular> python main.py --mode FL
```

```
== Running mode: FL ==
Round 1/10 | Mode: FL | Acc: 78.13% | Comm: 215080 bytes
Round 2/10 | Mode: FL | Acc: 76.77% | Comm: 215080 bytes
Round 3/10 | Mode: FL | Acc: 76.63% | Comm: 215080 bytes
Round 4/10 | Mode: FL | Acc: 76.63% | Comm: 215080 bytes
Round 5/10 | Mode: FL | Acc: 76.63% | Comm: 215080 bytes
Round 6/10 | Mode: FL | Acc: 76.57% | Comm: 215080 bytes
Round 7/10 | Mode: FL | Acc: 76.57% | Comm: 215080 bytes
Round 8/10 | Mode: FL | Acc: 76.57% | Comm: 215080 bytes
Round 9/10 | Mode: FL | Acc: 76.57% | Comm: 215080 bytes
Round 10/10 | Mode: FL | Acc: 76.57% | Comm: 215080 bytes
```

```
● (venv) PS C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular> python main.py --mode HE
```

```
== Running mode: HE ==
Round 1/10 | Mode: HE | Acc: 76.37% | Comm: 215080 bytes
Round 2/10 | Mode: HE | Acc: 76.60% | Comm: 215080 bytes
Round 3/10 | Mode: HE | Acc: 76.38% | Comm: 215080 bytes
Round 4/10 | Mode: HE | Acc: 76.40% | Comm: 215080 bytes
Round 5/10 | Mode: HE | Acc: 76.35% | Comm: 215080 bytes
Round 6/10 | Mode: HE | Acc: 76.37% | Comm: 215080 bytes
Round 7/10 | Mode: HE | Acc: 76.37% | Comm: 215080 bytes
Round 8/10 | Mode: HE | Acc: 76.37% | Comm: 215080 bytes
Round 9/10 | Mode: HE | Acc: 76.37% | Comm: 215080 bytes
Round 10/10 | Mode: HE | Acc: 76.37% | Comm: 215080 bytes
```

```
○ (venv) PS C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular> python main.py --mode DP+HE
```

```
● (venv) PS C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular> python main.py --mode DP+HE
== Running mode: DP+HE ==
C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular\venv\Lib\site-packages\opacus\privacy_engine.py:96: UserWarning: Full backward hook is used as it allows for much faster training performance, but remember to turn it on and retrain one last time before using it.
  warnings.warn(
C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular\utils\train.py:31: UserWarning: Full backward hook is used as it allows for much faster training performance, but remember to turn it on and retrain one last time before using it.
  inputs require gradients. See https://docs.pytorch.org/docs/main/generated/torch.nn.Module.html#torch.nn.Module.loss.backward()
Round 1/10 | Mode: DP+HE | Acc: 75.14% | Comm: 215080 bytes
Round 2/10 | Mode: DP+HE | Acc: 75.92% | Comm: 215080 bytes
Round 3/10 | Mode: DP+HE | Acc: 75.14% | Comm: 215080 bytes
Round 4/10 | Mode: DP+HE | Acc: 75.46% | Comm: 215080 bytes
Round 5/10 | Mode: DP+HE | Acc: 75.23% | Comm: 215080 bytes
Round 6/10 | Mode: DP+HE | Acc: 75.41% | Comm: 215080 bytes
Round 7/10 | Mode: DP+HE | Acc: 75.25% | Comm: 215080 bytes
Round 8/10 | Mode: DP+HE | Acc: 75.48% | Comm: 215080 bytes
Round 9/10 | Mode: DP+HE | Acc: 75.64% | Comm: 215080 bytes
Round 10/10 | Mode: DP+HE | Acc: 75.41% | Comm: 215080 bytes
```

```
○ (venv) PS C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular>
```

```
● (venv) PS C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular> python main.py --mode DP
== Running mode: DP ==
C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular\venv\Lib\site-packages\opacus\privacy_engine.py:96: UserWarning: Full backward hook is used as it allows for much faster training performance, but remember to turn it on and retrain one last time before using it.
  warnings.warn(
C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular\utils\train.py:31: UserWarning: Full backward hook is used as it allows for much faster training performance, but remember to turn it on and retrain one last time before using it.
  inputs require gradients. See https://docs.pytorch.org/docs/main/generated/torch.nn.Module.html#torch.nn.Module.loss.backward()
Round 1/10 | Mode: DP | Acc: 24.12% | Comm: 215080 bytes
Round 2/10 | Mode: DP | Acc: 76.64% | Comm: 215080 bytes
Round 3/10 | Mode: DP | Acc: 24.12% | Comm: 215080 bytes
Round 4/10 | Mode: DP | Acc: 75.91% | Comm: 215080 bytes
Round 5/10 | Mode: DP | Acc: 75.92% | Comm: 215080 bytes
Round 6/10 | Mode: DP | Acc: 76.06% | Comm: 215080 bytes
Round 7/10 | Mode: DP | Acc: 76.41% | Comm: 215080 bytes
Round 8/10 | Mode: DP | Acc: 76.49% | Comm: 215080 bytes
Round 9/10 | Mode: DP | Acc: 76.29% | Comm: 215080 bytes
Round 10/10 | Mode: DP | Acc: 76.37% | Comm: 215080 bytes
```

The screenshot shows the 'Privacy Preserving Module Details' section of the TUI interface. It displays the following configuration:

Module Name:	PPM
Status:	active
Epsilon:	1.0
Delta:	1e-05
He Active:	True
Description:	Privacy-Preserving Mechanism for policy auditing.



# Secure Aggregation

IT21831904 | Weerasinghe K.M

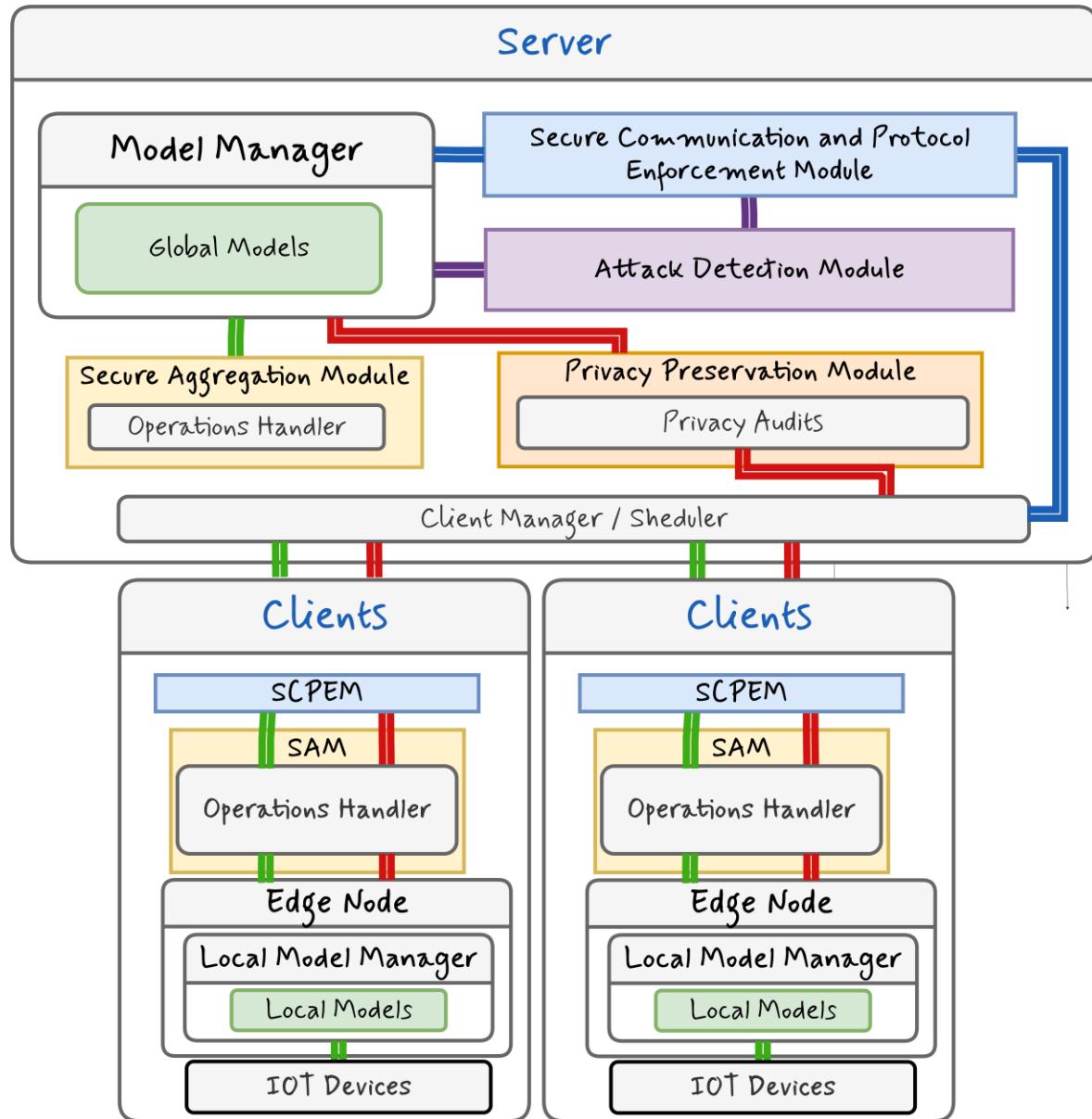
- **BACKGROUND**
  - **Main Function:** Secure aggregation ensures the server can compute an aggregate of client Updates without seeing any individual Private contribution
  - **Requirement:** It protects client data privacy during aggregation, even if the central server is curious or malicious
- **RESEARCH GAP**
  - **Limitations:** Many Secure aggregation protocols are either too heavy for resource constrained IIoT devices and some only exist in theory, and do not account for diverse IIoT environments
  - **Challenges:** They often lack robustness to network disruptions or client failures, which can cause an entire training round to collapse
- **RESEARCH PROBLEM**
  - How to design a secure Aggregation protocol that is both adaptive and robust enough for scalable IIoT deployments.

# SOLUTION:

- **Main Objective:** To aggregate client updates securely, ensuring the server learns only the final sum, not individual contributions, while being resilient to client dropouts.
- **Our approach:**
  - **Shamir's Secret Sharing (SSS):** Each client's model update is split into multiple shares. No single share reveals any information.
  - **Threshold Cryptography:** The original secret (the aggregated sum) can only be reconstructed if a minimum number of shares (the "threshold") are combined.
- **Benefits:**
  - **server Blindness:** The server cannot reconstruct any individual update.
  - **Fault Tolerance:** The aggregation succeeds even if some client failures

# Secure Aggregation Architecture

- **Client-Side Operations Handler:** Splits the local model update into encrypted shares using SSS.
- **Server-Side Operations Handler:** Receives and stores shares from all clients
- **Threshold Reconstructor:** A server function that combines shares to reconstruct the final aggregated model update once the required threshold is reached.



# **SECURE AGGREGATION PROCESS FLOW**

- Each client splits its update into  $n$  no of shares.
- Shares are distributed securely to the server.
- The server aggregates the corresponding shares from all clients.
- Once at least  $t$  clients have submitted, the server reconstructs the final aggregated update.

# SAM MODULE TUI INTERFACE

Federated Learning Framework v2.0 2025-09-15 02:25:07

(1) Overview | (2) Model Manager | (3) Client Health | (4) Modules | (5) Logs | (6) TUI Details

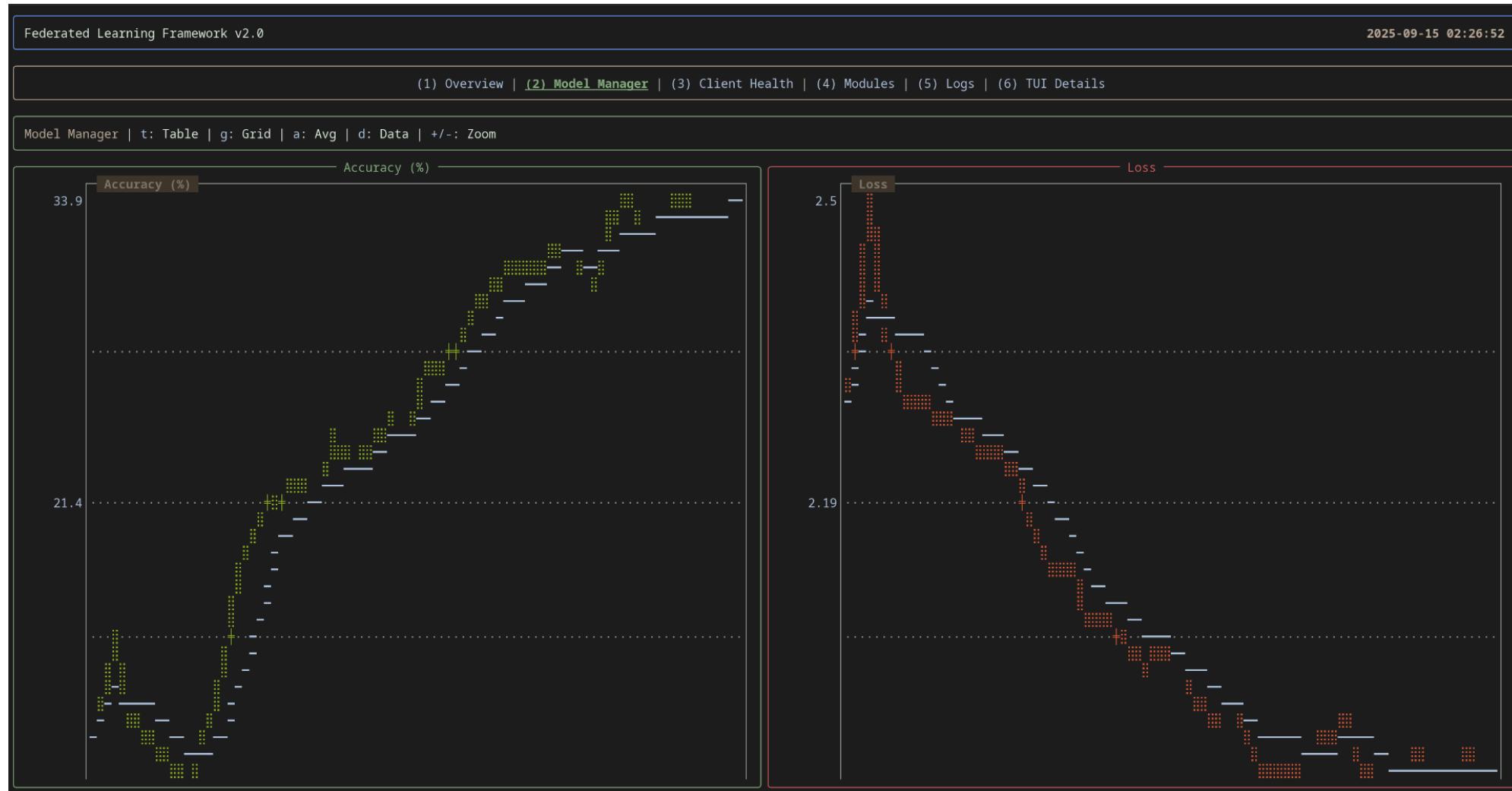
Modules

Attack Defense And Resillence Module | Privacy Preserving Module | Secure Aggrigation Module | Server Communication And Protocol Enforcement Module

Secure Aggrigation Module Details

Aggregation Protocol:	SecAgg
Security Level:	High
Updates In Queue:	1
Failed Sessions:	0
Last Aggregation Time:	2025-09-15 02:25:03
Status:	active

# AGGREGATION PROCESS





# Secure Communication and Protocol Enforcement

IT21828348 | Dissanayaka KDARA

- **BACKGROUND**

- In IIoT, communication between clients and server is a prime target for threats like eavesdropping, tampering, and MITM attacks. Standard FL focused on efficiency but lacked strong defenses. TLS provides a baseline, but its one-sided authentication leaves gaps.

- **RESEARCH GAP**

- Current solutions lack an integrated security framework for IIoT. Standard TLS often validates only the server, leaving no assurance that connected devices are legitimate. A stricter, two-way validation protocol is needed.

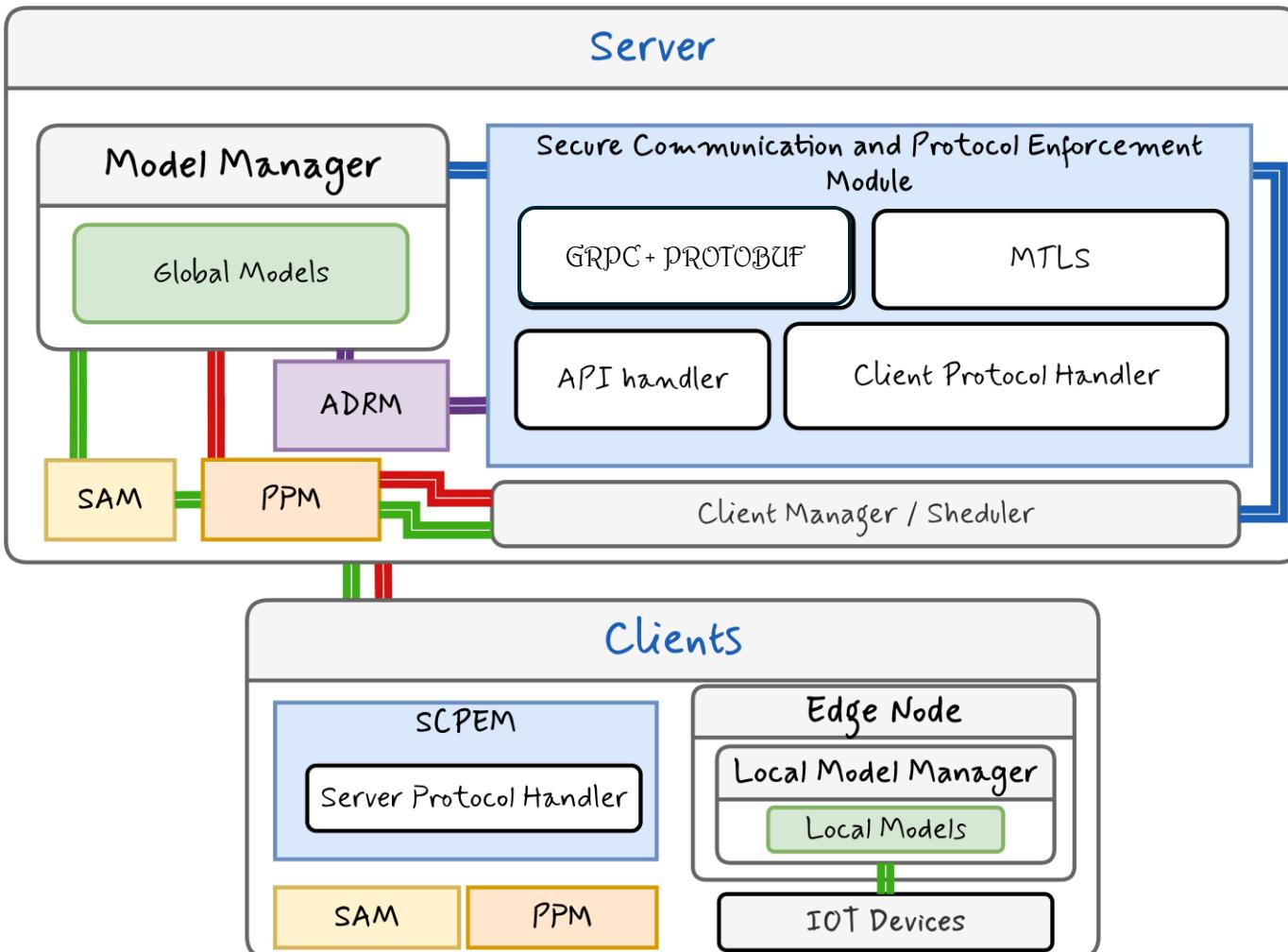
- **RESEARCH PROBLEM**

- Insecure FL channels risk unauthorized access, tampered updates, fake servers, and undetected data changes.

# **SOLUTION:**

- Implement a secure communication protocol that ensures only authorized IIoT devices can participate, protects model updates from tampering, verifies the legitimacy of the server, and adds integrity checks beyond encryption to guarantee unaltered data.

# Module Architecture



# SERVER COMPONENTS

- **Model Manager:** Distributes and updates the global model.
- **SCPEM:** Secure channel using mTLS (two-way authentication) + HMAC for integrity.
- **Client Manager/Scheduler:** Selects and manages participating clients.

# OVERALL WORKFLOW

- Server selects clients for training.
- Global model sent via **SCPEM** (secure channel).
- Clients train locally on IoT data.
- Updates protected using **PPM & SAM**.
- Protected updates sent back via **SCPM**.
- Server validates updates with **ADRM**.
- **SAM** aggregates updates securely.
- **Model Manager** updates global model.
- Cycle repeats.

# SCPM Architecture

Federated Learning Framework v2.0

2025-09-15 02:25:36

(1) Overview | (2) Model Manager | (3) Client Health | (4) Modules | (5) Logs | (6) TUI Details

Modules

Attack Defense And Resillence Module | Privacy Preserving Module | Secure Aggrigation Module | Server Communication And Protocol Enforcement Module

Module Name: SCPM  
Status: active  
Tls Enabled: False  
Client Authentication Enabled: False  
Last Security Event: System initialized.  
Active Protocols: gRPC, REST API  
Description: Manages communication protocols and server state.

Server Communication And Protocol Enforcement Module Details

Img 1: SCPM TUI frontned

# Log manager

Federated Learning Framework v2.0 2025-09-15 02:39:31

(1) Overview | (2) Model Manager | (3) Client Health | (4) Modules | (5) Logs | (6) TUI Details

Logs

Level: ALL Search: None f: Filter Level | s: Search | r: Reset

Recent Logs

Timestamp	Level	Logger	Message
2025-09-15 02:39:13,177	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/logs HTTP/1.1" 200 54505 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,178	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/status HTTP/1.1" 200 1988 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,179	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/module_status/mm HTTP/1.1" 200 405 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,180	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/module_status/sam HTTP/1.1" 200 365 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,181	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/module_status/adm HTTP/1.1" 200 417 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,181	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/module_status/ppm HTTP/1.1" 200 353 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,182	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/module_status/scpm HTTP/1.1" 200 453 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,183	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:13 +0530] "GET /api/module_status/orchestrator HTTP/1.1" 200 485 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:13,264	INFO	ServerControlPlaneManager	Dashboard status updated: Connected clients count is 4.
2025-09-15 02:39:13,266	WARNING	Orchestrator	Denied model request from client_2. Orchestrator state is 'PAUSED_INSUFFICIENT_CLIENTS'.
2025-09-15 02:39:15,257	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:15 +0530] "GET /api/overview HTTP/1.1" 200 680 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:15,258	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:15 +0530] "GET /api/model/metrics_details HTTP/1.1" 200 6890 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:15,259	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:15 +0530] "GET /api/client_health HTTP/1.1" 200 1769 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:15,267	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:15 +0530] "GET /api/logs HTTP/1.1" 200 54016 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:15,268	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:15 +0530] "GET /api/status HTTP/1.1" 200 1988 "-" "Python/3.10 aiohttp/3.12.15"
2025-09-15 02:39:15,268	INFO	aiohttp.access	127.0.0.1 [15/Sep/2025:02:39:15 +0530] "GET /api/module_status/mm HTTP/1.1" 200 405 "-" "Python/3.10 aiohttp/3.12.15"

Img 2 : logging and monitoring of overall system

# TECHNOLOGIES

- BACKEND
  - Python
  - Asyncio
- COMMUNICATION
  - GRPC
  - Protocol buffers
  - AIOHTTP
  - AIOHTTP-CORS
- ML & DATA PROCESSING
  - PyTorch
  - Torch Vision
  - NumPy
- CRYPTOGRAPHY & SECURITY
  - PyCryptodrome
  - Secret-sharing
  - X.509 Certificates
- FRONTEND & VALIDATION
  - Rich
  - Prompt Toolkit
- LOGGING AND MONITORING
  - Python-JSON-Logger
  - Logstash

# Commercialization

## Target Industries



*Manufacturing*



*Energy*



*Healthcare*



*Automobile*

- Our product includes **4 modular components** that can be easily integrated into **any Federated Learning system** both **existing and new** to enhance **data privacy**.

**Business Models**

As a PaaS Model or Enterprise Solutions.

# Demonstration

# Clients – Running Methods

## FLF 2.0 Client Controller

```
Attempting to start the client process...
Client logs are being saved to client.log
Waiting for client's API to be ready...
Client API is ready!
This tool manages the client's privacy preferences.
Press Ctrl+C at any time to exit (this will also
stop the client).
...
Client is PAUSED. Select a method to GO (start
training).
? Select a method to GO HE
Successfully updated preference to: HE
The client will use this mode on its next training
round.
...
Current Privacy Method: HE
? Select a new method (use arrow keys and Enter) (U
se arrow keys)
» HE
  SSS
  Normal
  Pause Client
  Exit
```

## FLF 2.0 Client Controller

```
Attempting to start the client process...
Client logs are being saved to client.log
Waiting for client's API to be ready...
Client API is ready!
This tool manages the client's privacy preferences.
Press Ctrl+C at any time to exit (this will also
stop the client).
...
Client is PAUSED. Select a method to GO (start
training).
? Select a method to GO SSS
Successfully updated preference to: SSS
The client will use this mode on its next training
round.
...
Current Privacy Method: SSS
? Select a new method (use arrow keys and Enter) (U
se arrow keys)
» HE
  SSS
  Normal
  Pause Client
  Exit
```

## FLF 2.0 Client Controller

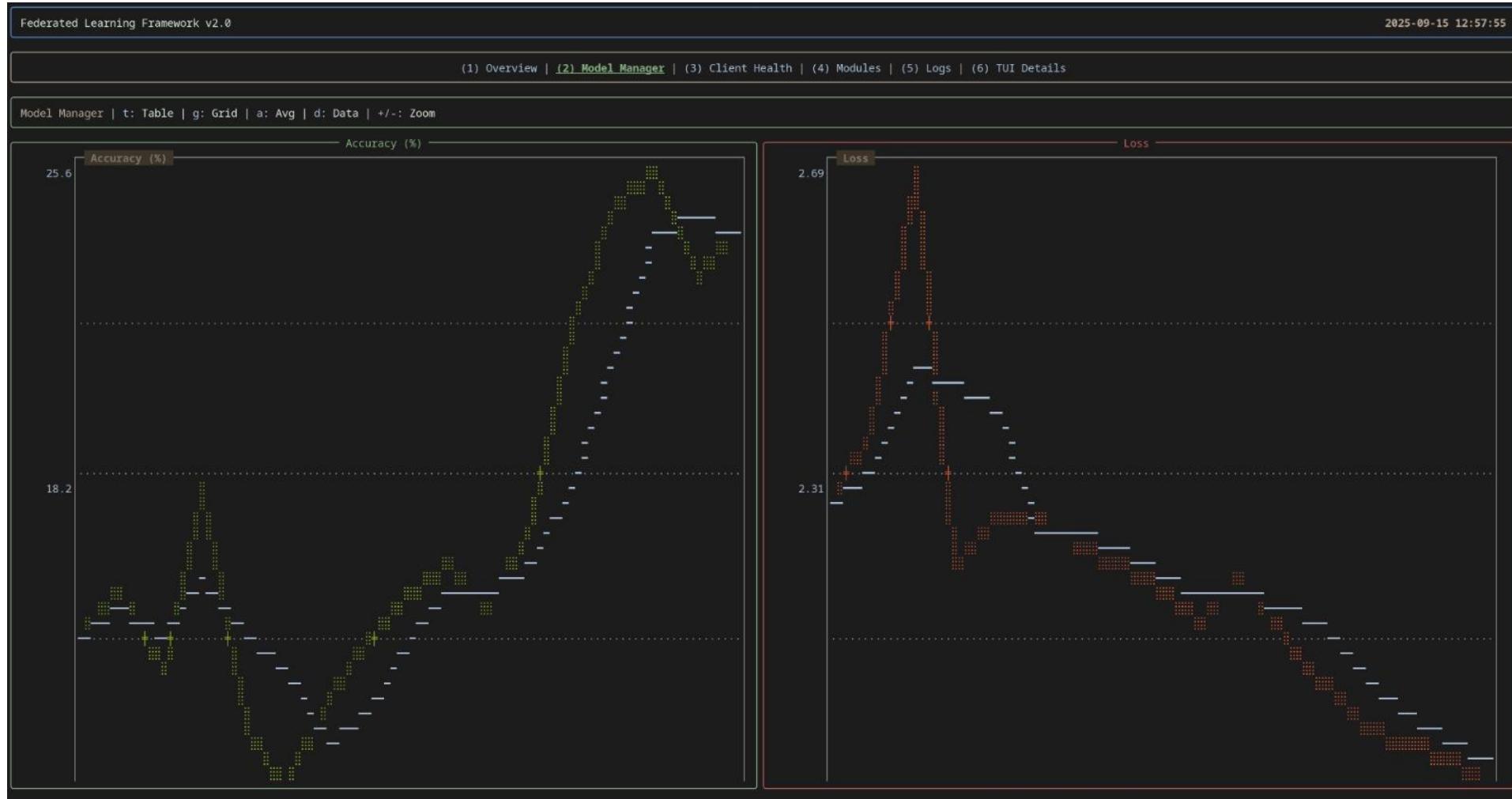
```
Attempting to start the client process...
Client logs are being saved to client.log
Waiting for client's API to be ready...
Client API is ready!
This tool manages the client's privacy preferences.
Press Ctrl+C at any time to exit (this will also
stop the client).
...
Client is PAUSED. Select a method to GO (start
training).
? Select a method to GO Normal
Successfully updated preference to: Normal
The client will use this mode on its next training
round.
...
Current Privacy Method: Normal
? Select a new method (use arrow keys and Enter) (U
se arrow keys)
» HE
  SSS
  Normal
  Pause Client
  Exit
```

Method 2 – HE + DP method

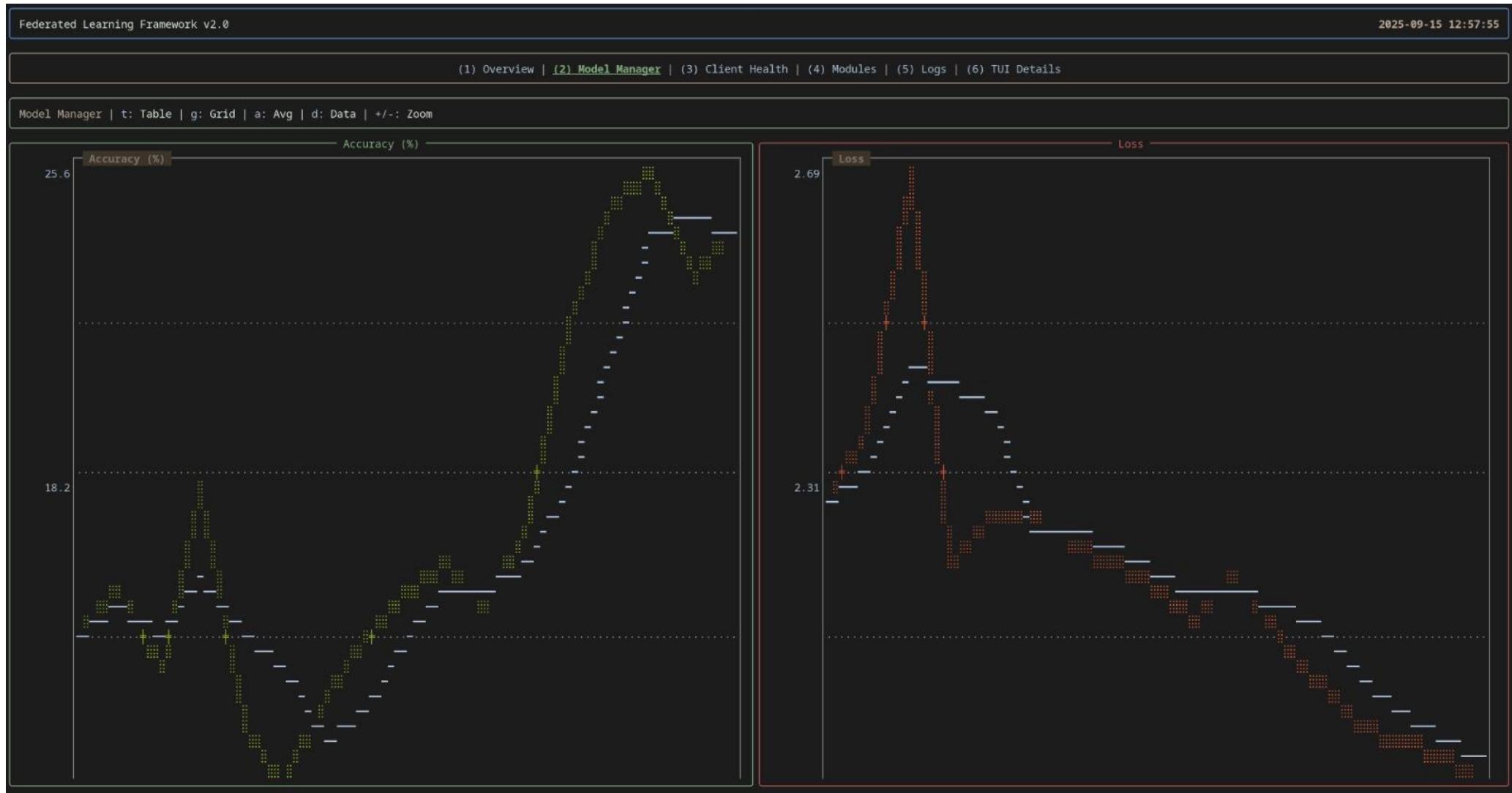
Method 3 – SSS+TH method

Method 1 – Traditional method

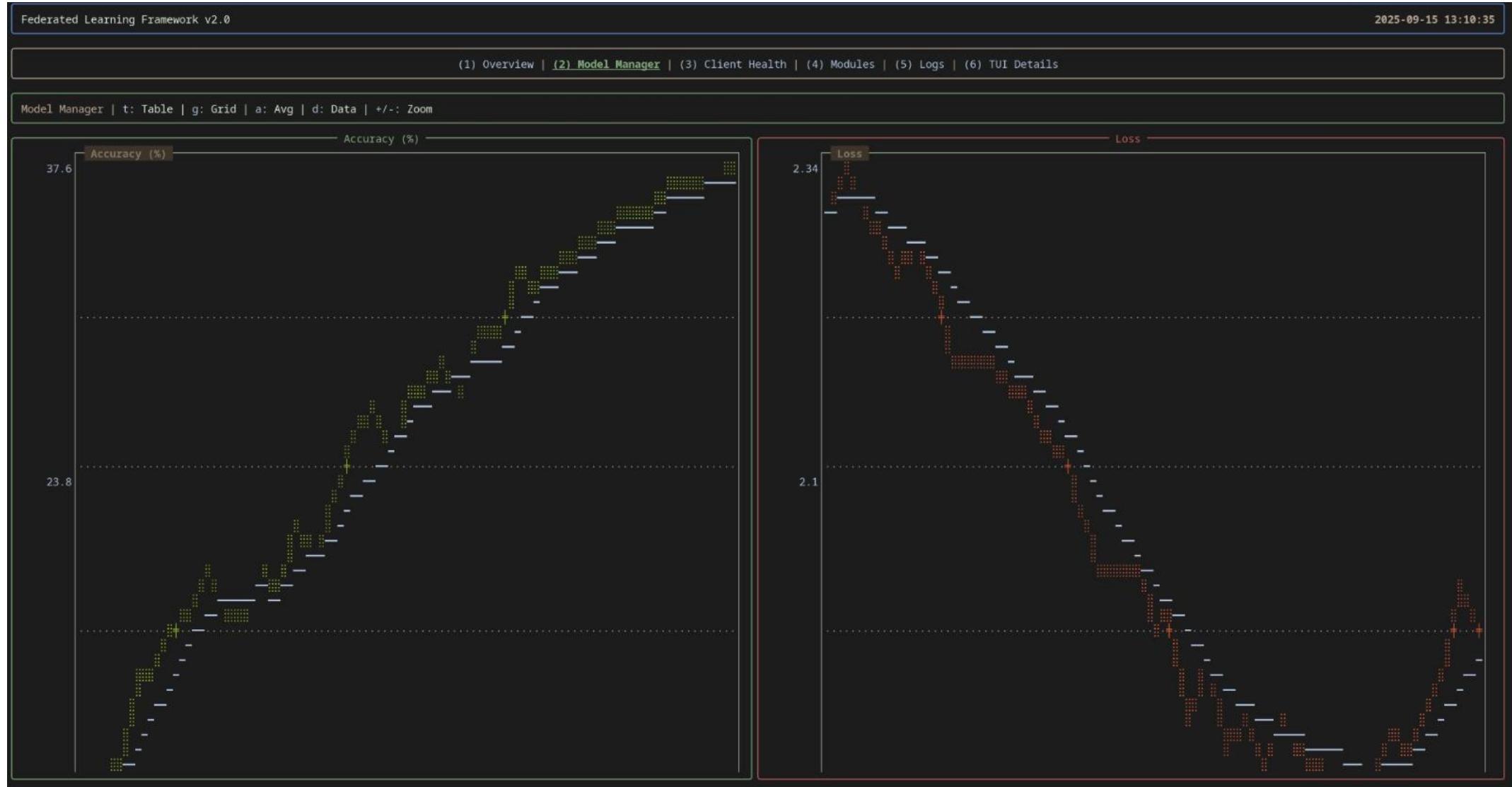
# Method 1 – Normal FL method



# Method 2 – HE + DP FL method



# Method 3 – SSS + TC FL method



# THE END

Thank You