Logbook – Attack Defense and resilience of R25 -039

Project ID: R25 - 039

Project Title: Data-Privacy Focused Federated Learning Framework for Industrial IoT

Student Details:

Names:	Student IDs:
Nanayakkara Y.D.T. D	IT21826368

Supervisor: Mr. Amila Seneratha

Co-Supervisor: Mr. Tharaniyawarma Kumaralingam

Date of Submission: 2025

Contents

1. Group Details

Student Details:

Names:	Student IDs:	Research Component
Nanayakkara Y.D.T. D	IT21826368	Attack Defense and Resilience
Mendis H.R.M	IT21822612	Privacy Preseravation
Weerasinghe K.M	IT21831904	Secure Aggrigation
Dissanayaka K.D.A.R. A	IT21828348	Secure Communicaiton and Protocol Enforcement

2. Project Details

Topic - Data-Privacy Focused Federated Learning Framework for Industrial IoT

Aim – To develop a product that going to full fill the research

Deliverables – Federated Learning Framework designed for industrial internet of things

This project was initiated to develop a secure and private **Federated Learning (FL) framework** specifically for **Industrial IoT (IIoT)** environments.

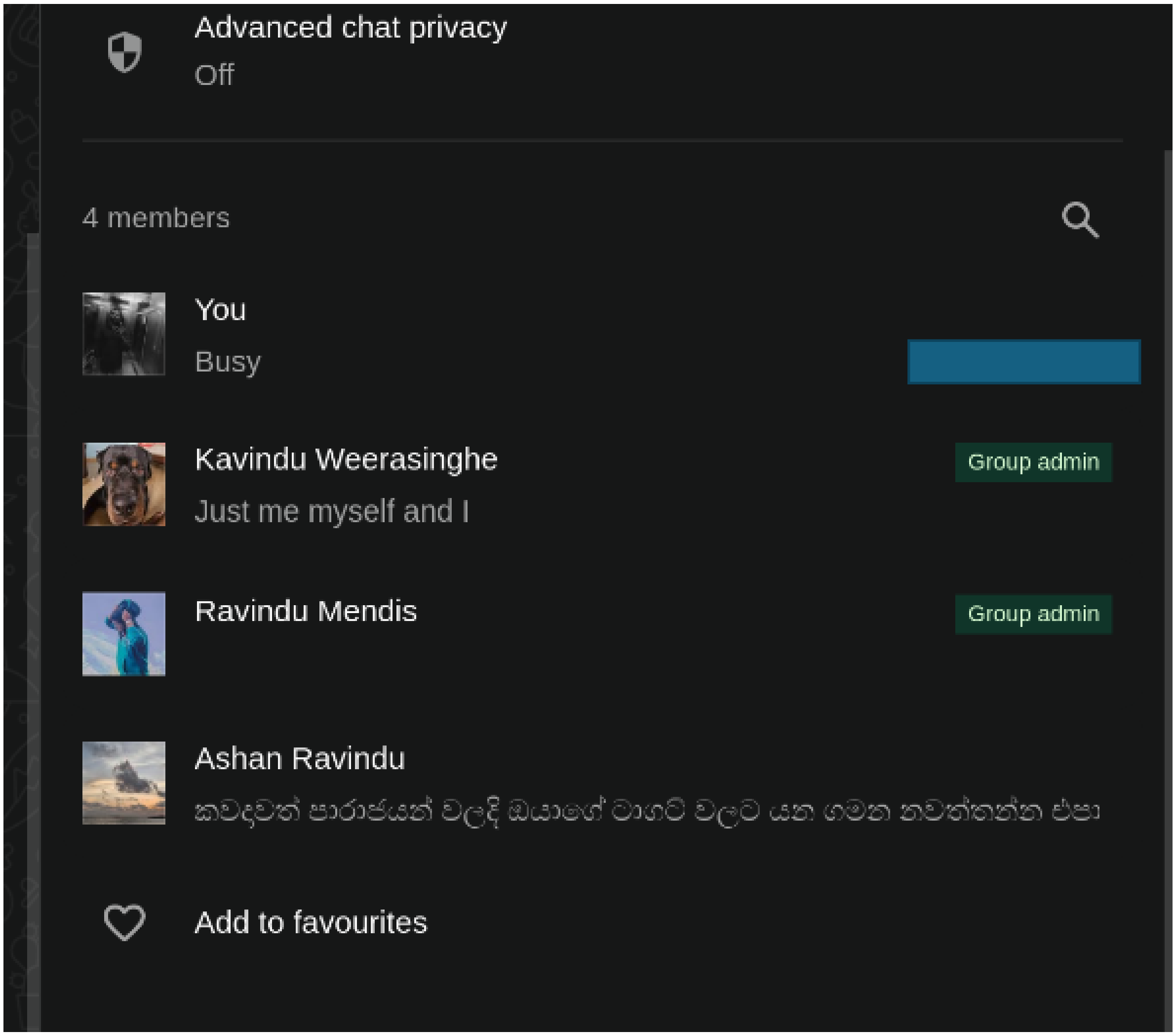
The Challenge: Traditional AI methods require centralizing sensitive factory data, which poses major **privacy risks** and clashes with the distributed nature of industrial operations. Existing FL solutions are insufficient because they fail to simultaneously provide robust security, data privacy, and efficient operation on **resource-limited IIoT devices**.

The Solution: The developed framework is a multi-layered system that provides **end-to-end protection**.

- It uses techniques like **Differential Privacy (DP)** and **Homomorphic Encryption (HE)** to guarantee data confidentiality.
- It implements a robust protocol that uses **client/server validation** to actively block cyber threats such as **Model Poisoning and Byzantine Attacks**.
- The system is optimized for **efficiency** to reduce overhead on IIoT devices.

3. Communication Methods

WhatsApp Group – Team



Advanced chat privacy
Off

4 members

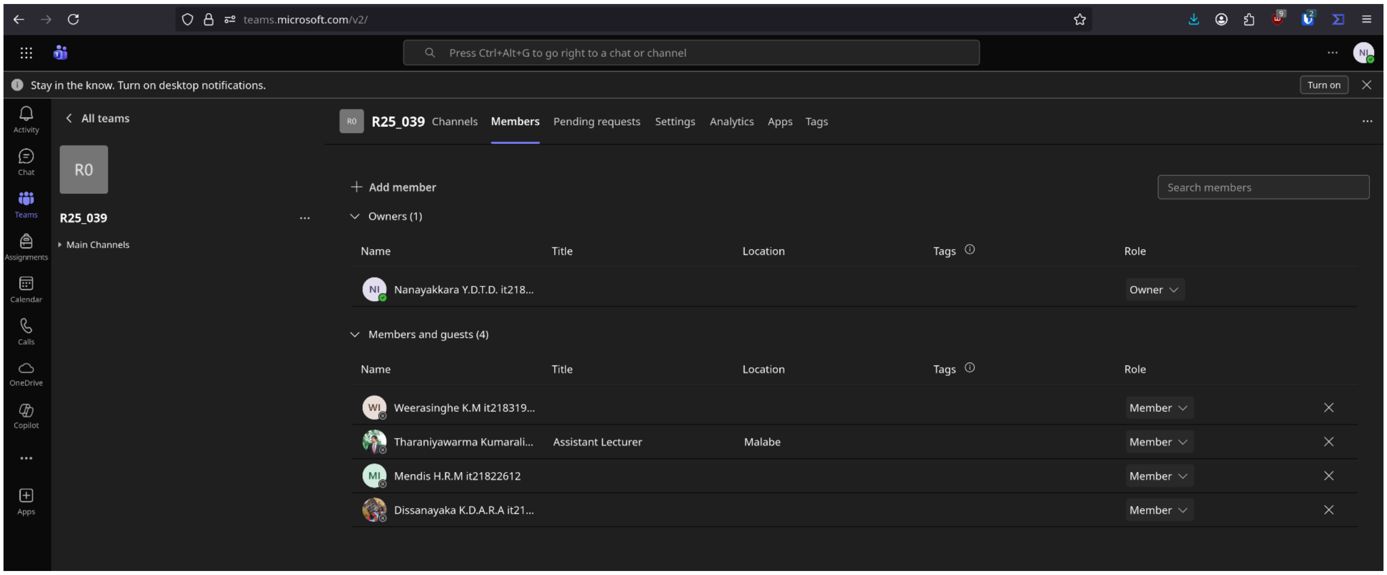
You
Busy [redacted]

Kavindu Weerasinghe — Group admin
Just me myself and I

Ravindu Mendis — Group admin

Ashan Ravindu
කවදවත් පාරාජයන් වලදී ඔයාගේ ටාගට් වලට යන ගමන නවත්තන්න එපා

Microsoft Teams - All



R25_039

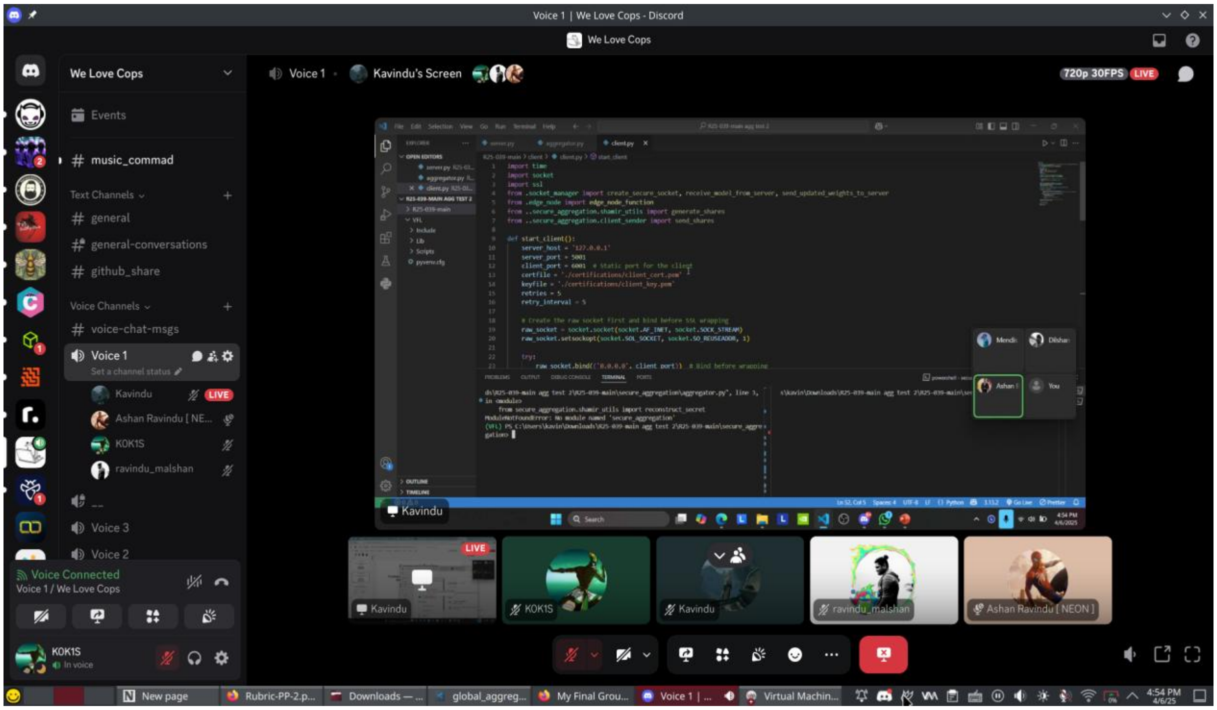
Owners (1)

Name	Title	Location	Tags	Role
Nanayakkara Y.D.T.D. it218...				Owner

Members and guests (4)

Name	Title	Location	Tags	Role
Weerasinghe K.M it218319...				Member
Tharaniyawarma Kumarali...	Assistant Lecturer	Malabe		Member
Mendis H.R.M it21822612				Member
Dissanayaka K.D.A.R.A it21...				Member

Group Meetings – Discord – Team



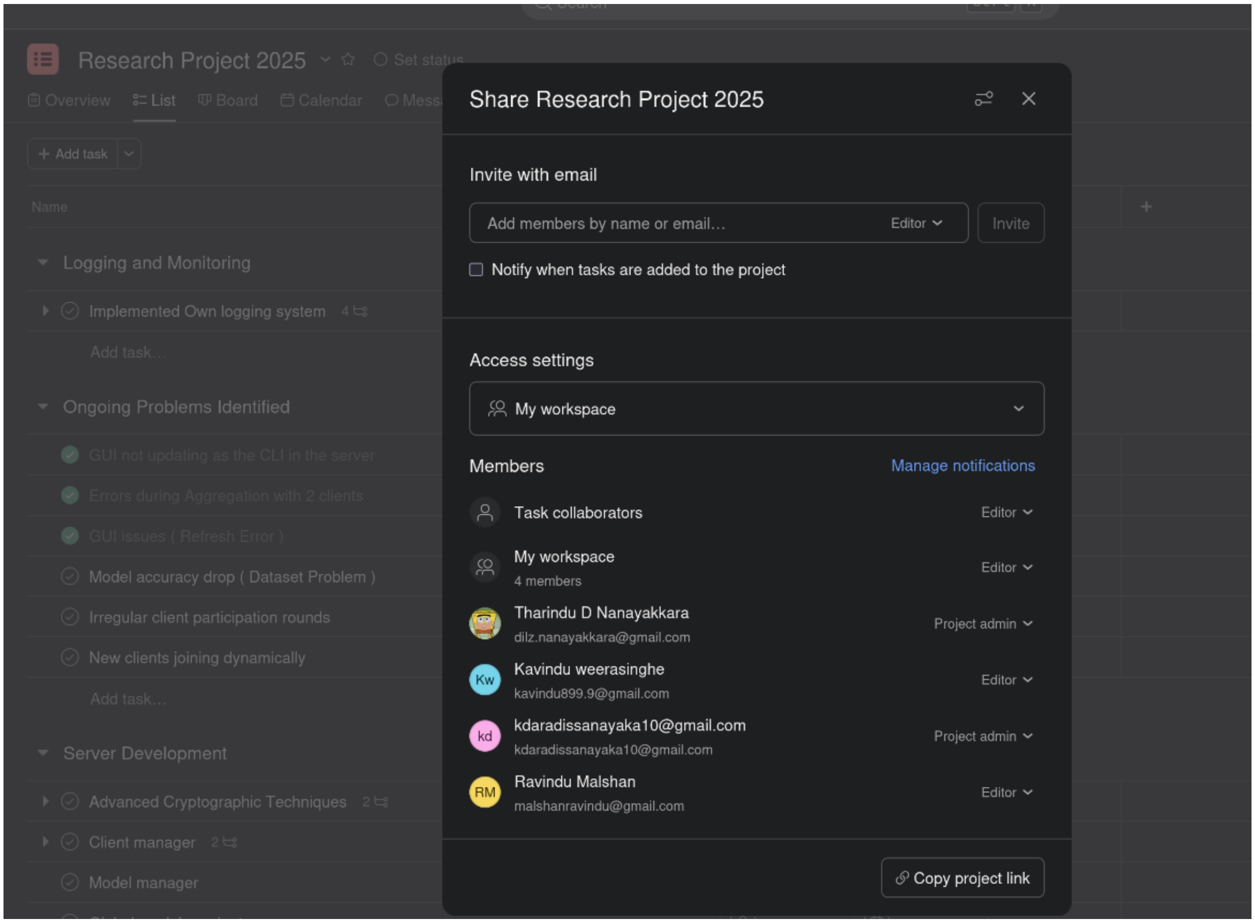
server.py
aggregator.py
client.py

R25-039-main > client > client.py > start_client

```python
import time
import socket
import ssl
from .socket_manager import create_secure_socket, receive_model_from_server, send_updated_weights_to_server
from .edge_node import edge_node_function
from ..secure_aggregation.shamir_utils import generate_shares
from ..secure_aggregation.client_sender import send_shares

def start_client():
    server_host = '127.0.0.1'
    server_port = 5001
    client_port = 6001  # Static port for the client
    certfile = './certifications/client_cert.pem'
    keyfile = './certifications/client_key.pem'
    retries = 5
    retry_interval = 5

    # Create the raw socket first and bind before SSL wrapping
    raw_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    raw_socket.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)

    try:
        raw_socket.bind(('0.0.0.0', client_port))  # Bind before wrapping
```

```
ds\R25-039-main agg test 2\R25-039-main\secure_aggregation\aggregator.py", line 3,
in <module>
    from secure_aggregation.shamir_utils import reconstruct_secret
ModuleNotFoundError: No module named 'secure_aggregation'
(VFL) PS C:\Users\kavin\Downloads\R25-039-main agg test 2\R25-039-main\secure_aggre
gation> 
```

Asana – Task Assigning – Team



Logging and Monitoring

- Implemented Own logging system 4
- Add task…

Ongoing Problems Identified

- GUI not updating as the CLI in the server
- Errors during Aggregation with 2 clients
- GUI issues (Refresh Error)
- Model accuracy drop (Dataset Problem)
- Irregular client participation rounds
- New clients joining dynamically
- Add task…

Server Development

- Advanced Cryptographic Techniques 2
- Client manager 2
- Model manager

Share Research Project 2025

Invite with email

Add members by name or email… Editor | Invite

□ Notify when tasks are added to the project

Access settings

My workspace

Members — Manage notifications

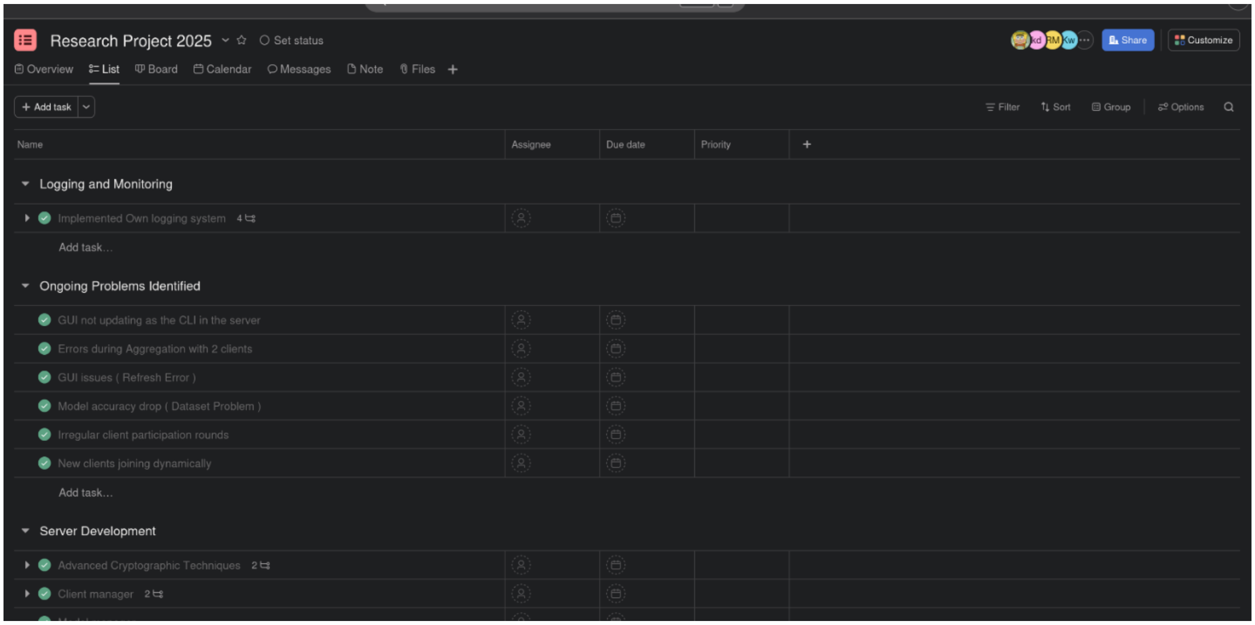
Member	Role
Task collaborators	Editor
My workspace 4 members	Editor
Tharindu D Nanayakkara dilz.nanayakkara@gmail.com	Project admin
Kavindu weerasinghe kavindu899.9@gmail.com	Editor
kdaradissanayaka10@gmail.com kdaradissanayaka10@gmail.com	Project admin
Ravindu Malshan malshanravindu@gmail.com	Editor

Copy project link

4. Meetings With Supervisors

All the meetings were conducted in person and only WhatsApp calls were taken to organize the meeting

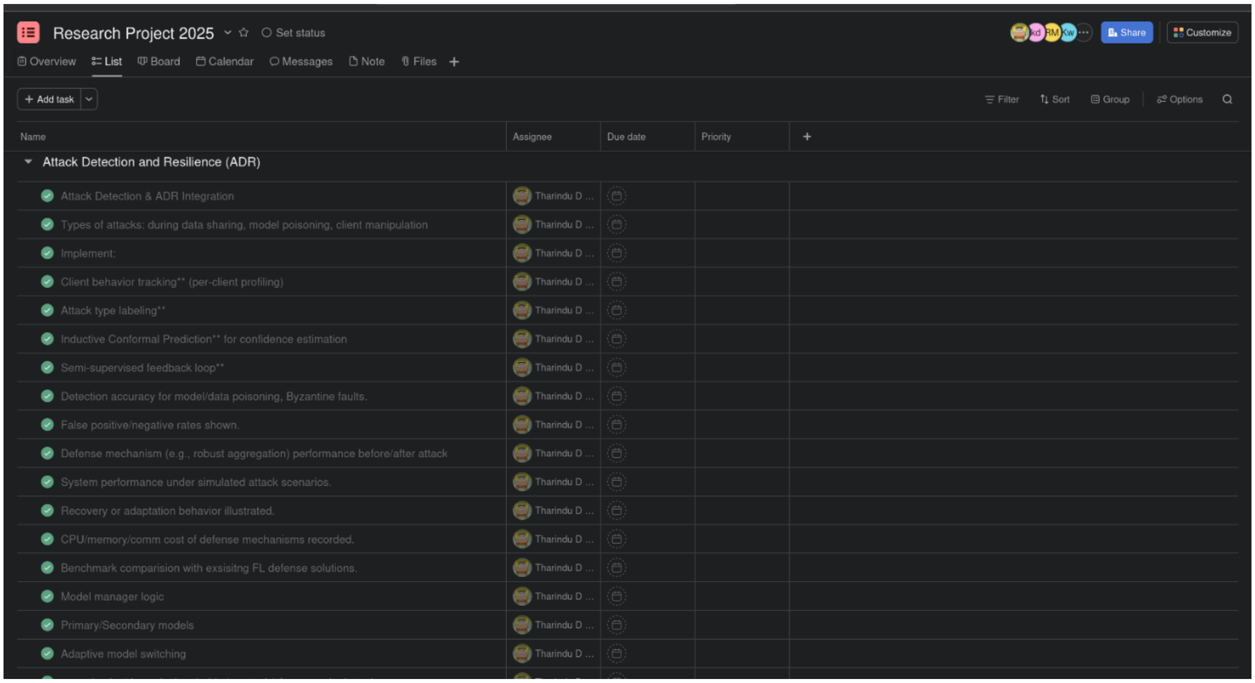
5. Task Details



Name	Assignee	Due date	Priority
Logging and Monitoring			
✓ Implemented Own logging system 4			
Add task...			
Ongoing Problems Identified			
✓ GUI not updating as the CLI in the server			
✓ Errors during Aggregation with 2 clients			
✓ GUI issues (Refresh Error)			
✓ Model accuracy drop (Dataset Problem)			
✓ Irregular client participation rounds			
✓ New clients joining dynamically			
Add task...			
Server Development			
✓ Advanced Cryptographic Techniques 2			
✓ Client manager 2			

Attack defense and resilience module was mine.

Personal task Assigning and Completion



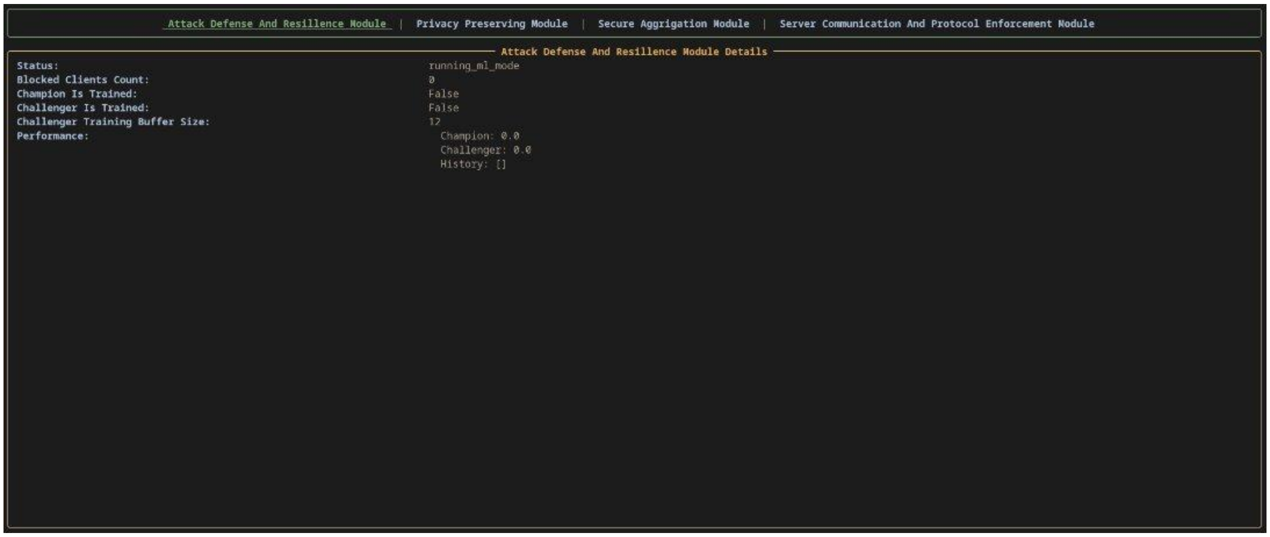
Name	Assignee	Due date	Priority
Attack Detection and Resilience (ADR)			
✓ Attack Detection & ADR Integration	Tharindu D ...		
✓ Types of attacks: during data sharing, model poisoning, client manipulation	Tharindu D ...		
✓ Implement:	Tharindu D ...		
✓ Client behavior tracking** (per-client profiling)	Tharindu D ...		
✓ Attack type labeling**	Tharindu D ...		
✓ Inductive Conformal Prediction** for confidence estimation	Tharindu D ...		
✓ Semi-supervised feedback loop**	Tharindu D ...		
✓ Detection accuracy for model/data poisoning, Byzantine faults.	Tharindu D ...		
✓ False positive/negative rates shown.	Tharindu D ...		
✓ Defense mechanism (e.g., robust aggregation) performance before/after attack	Tharindu D ...		
✓ System performance under simulated attack scenarios.	Tharindu D ...		
✓ Recovery or adaptation behavior illustrated.	Tharindu D ...		
✓ CPU/memory/comm cost of defense mechanisms recorded.	Tharindu D ...		
✓ Benchmark comparision with exsisitng FL defense solutions.	Tharindu D ...		
✓ Model manager logic	Tharindu D ...		
✓ Primary/Secondary models	Tharindu D ...		
✓ Adaptive model switching	Tharindu D ...		

6. System Details

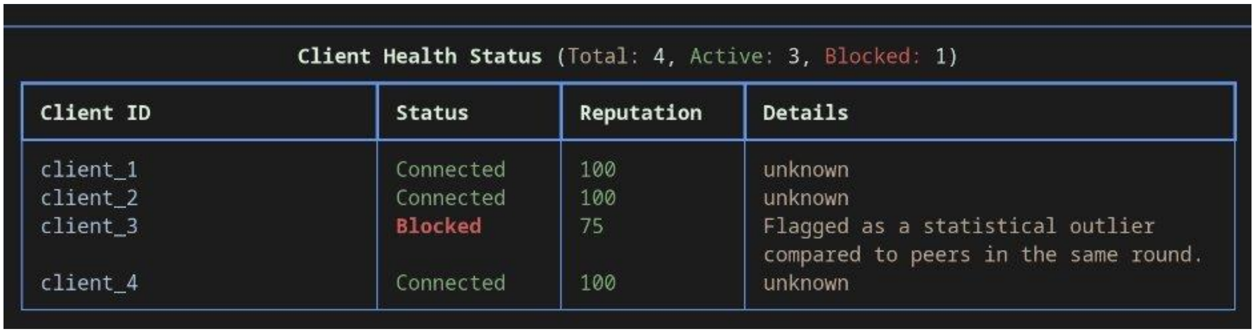
6.1 System completion status

Finished

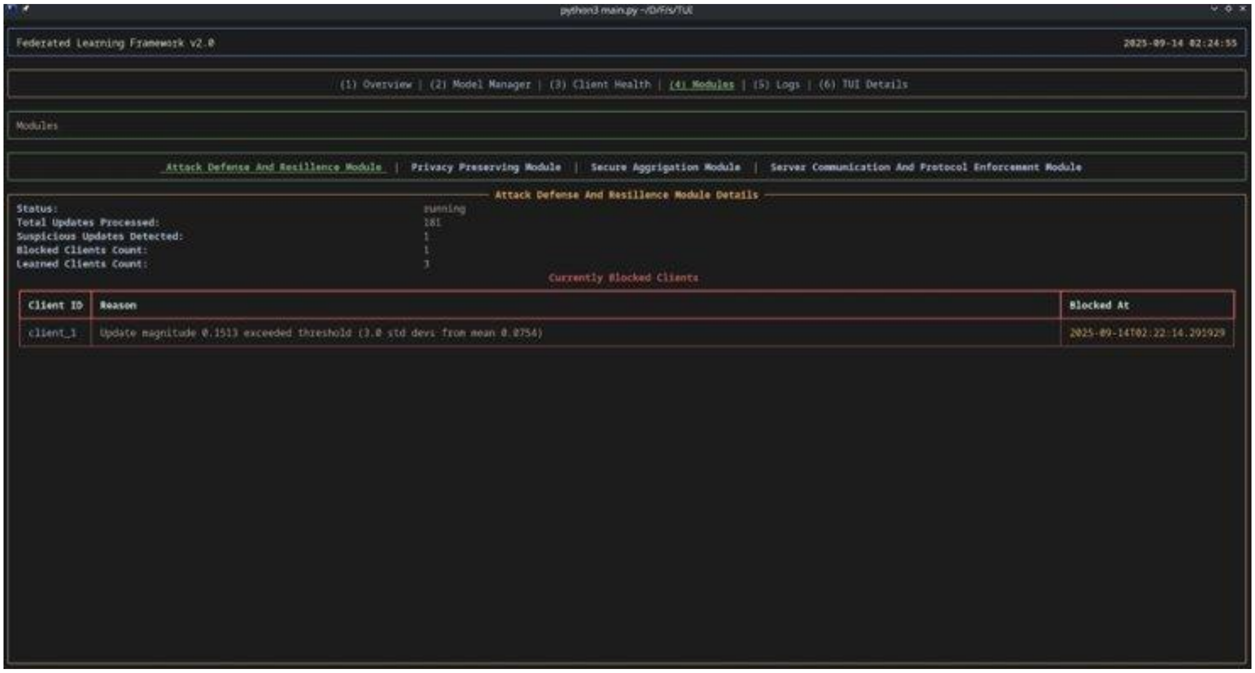
ADRM TUI


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

```
──────────────── Attack Defense And Resillence Module Details ────────────────
Status:                                      running_ml_mode
Blocked Clients Count:                       0
Champion Is Trained:                         False
Challenger Is Trained:                       False
Challenger Training Buffer Size:             12
Performance:                                   Champion: 0.0
                                               Challenger: 0.0
                                               History: []
```

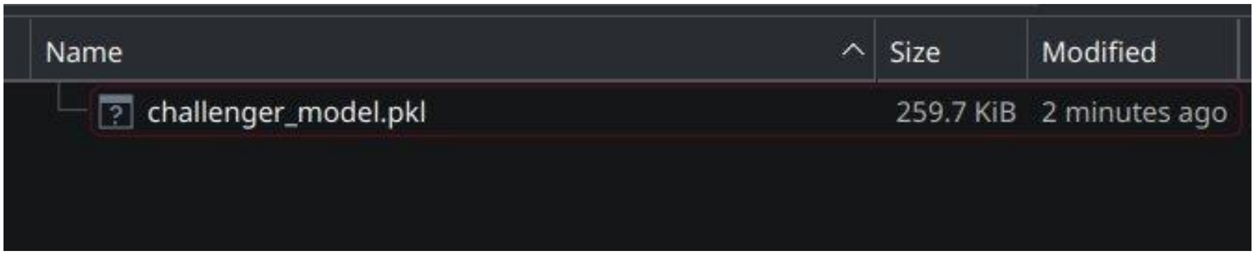


```
          Client Health Status (Total: 4, Active: 3, Blocked: 1)
┌───────────────────┬──────────┬────────────┬──────────────────────────────┐
│ Client ID         │ Status   │ Reputation │ Details                      │
├───────────────────┼──────────┼────────────┼──────────────────────────────┤
│ 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                      │
└───────────────────┴──────────┴────────────┴──────────────────────────────┘
```



```
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 Resilience Module | Privacy Preserving Module | Secure Aggrigation Module | Server Communication And Protocol Enforcement Module

─────────────────────────── Attack Defense And Resilience Module Details ───────────────────────────
Status:                                running
Total Updates Processed:               181
Suspicious Updates Detected:           1
Blocked Clients Count:                 1
Learned Clients Count:                 3
                                   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
```

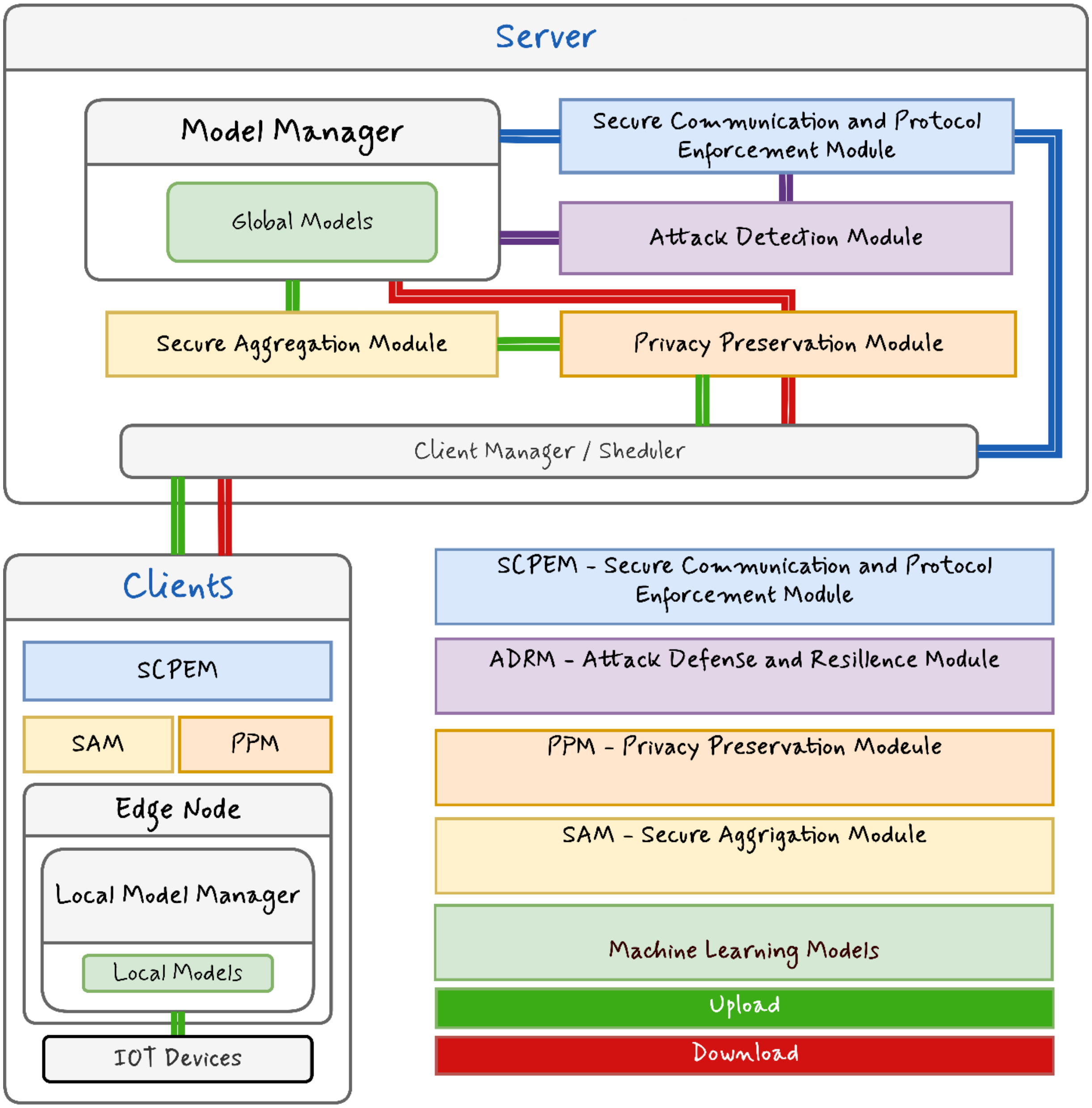
ADRM System ML model that creates when System runs.



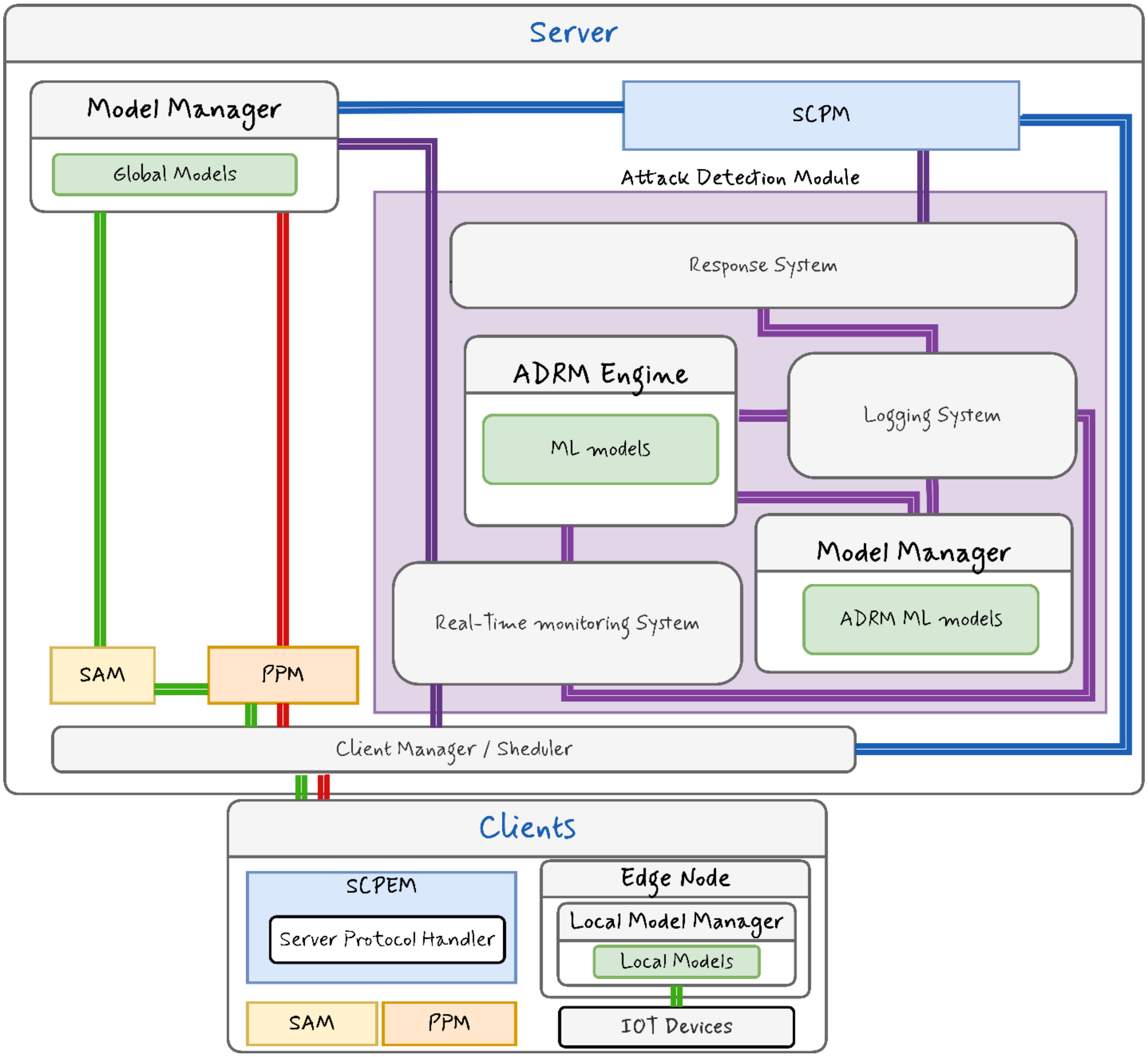
Name	Size	Modified
challenger_model.pkl	259.7 KiB	2 minutes ago

6.2 System Design

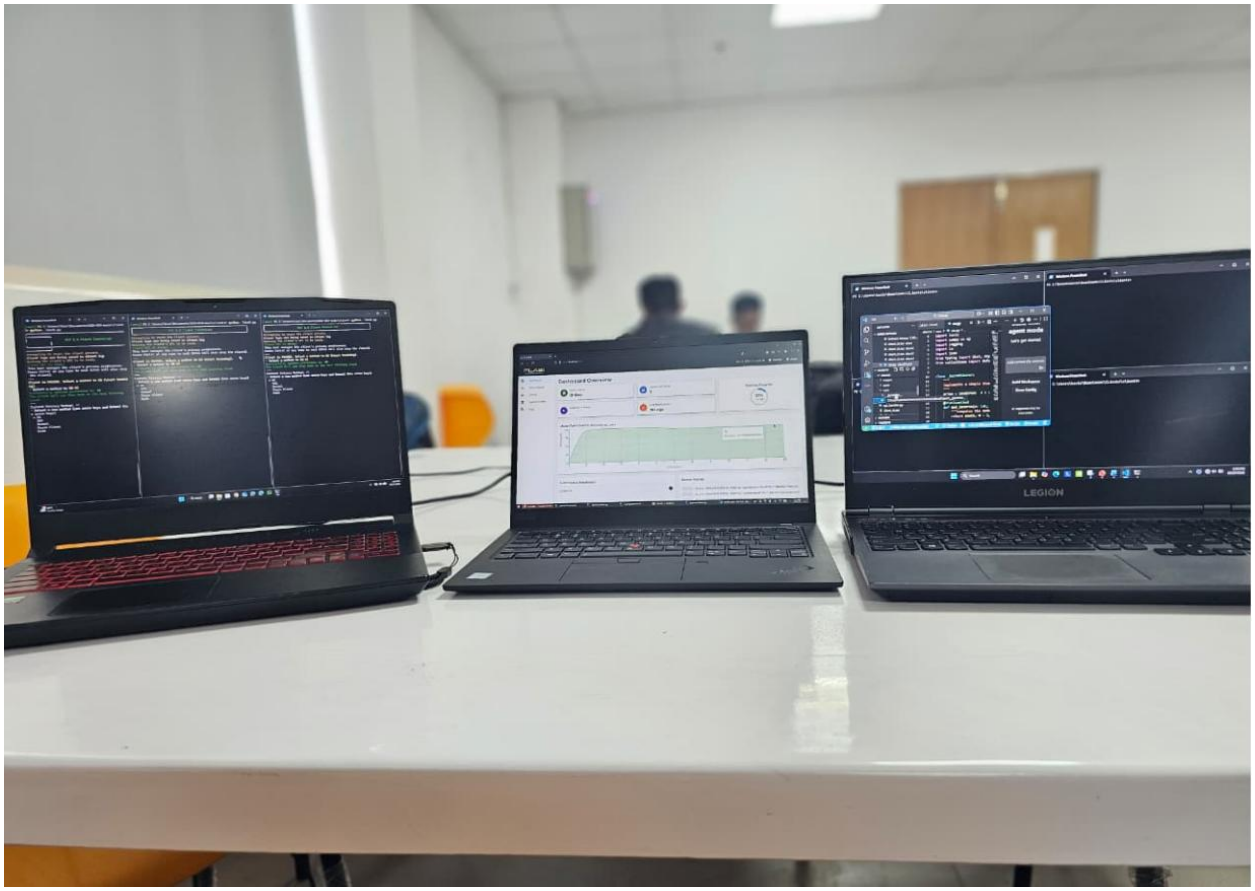
I. System Architecture


Server
Model Manager
Global Models
Secure Communication and Protocol Enforcement Module
Attack Detection Module
Secure Aggregation Module
Privacy Preservation Module
Client Manager / Shedaler
Clients
SCPEM
SAM
PPM
Edge Node
Local Model Manager
Local Models
IOT Devices
SCPEM - Secure Communication and Protocol Enforcement Module
ADRM - Attack Defense and Resillence Module
PPM - Privacy Preservation Modeule
SAM - Secure Aggrigation Module
Machine Learning Models
Upload
Download

II. Module Architecture

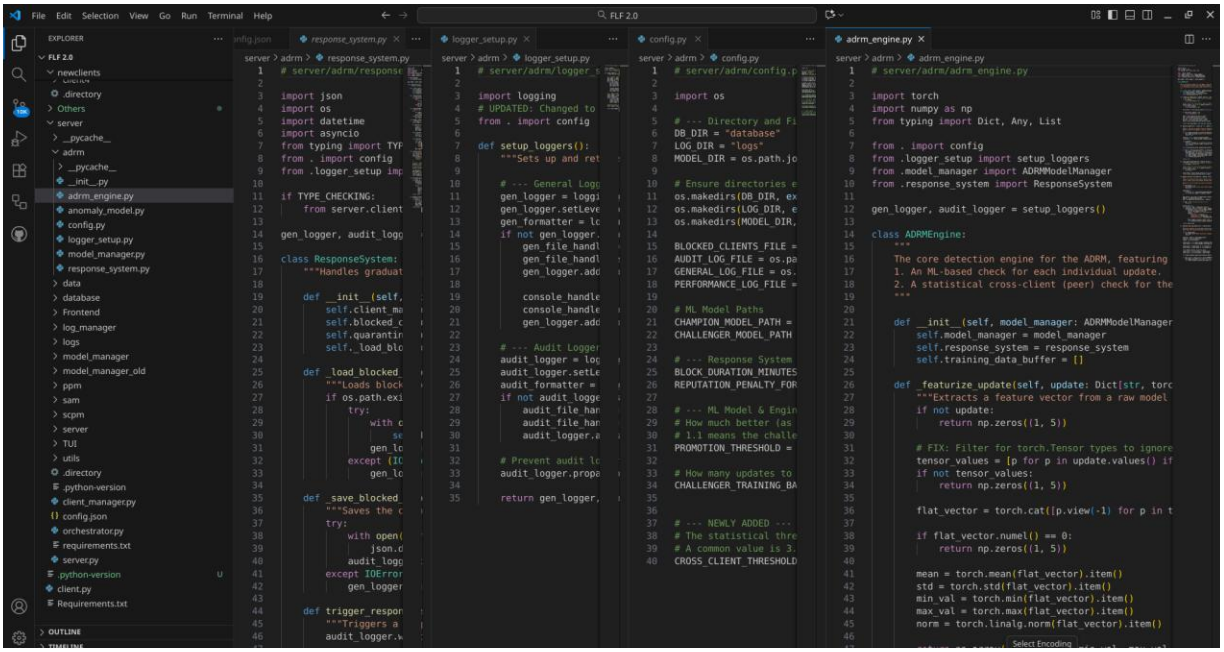


6.3 System Testing



6.4 System Codes

ADRM – Server



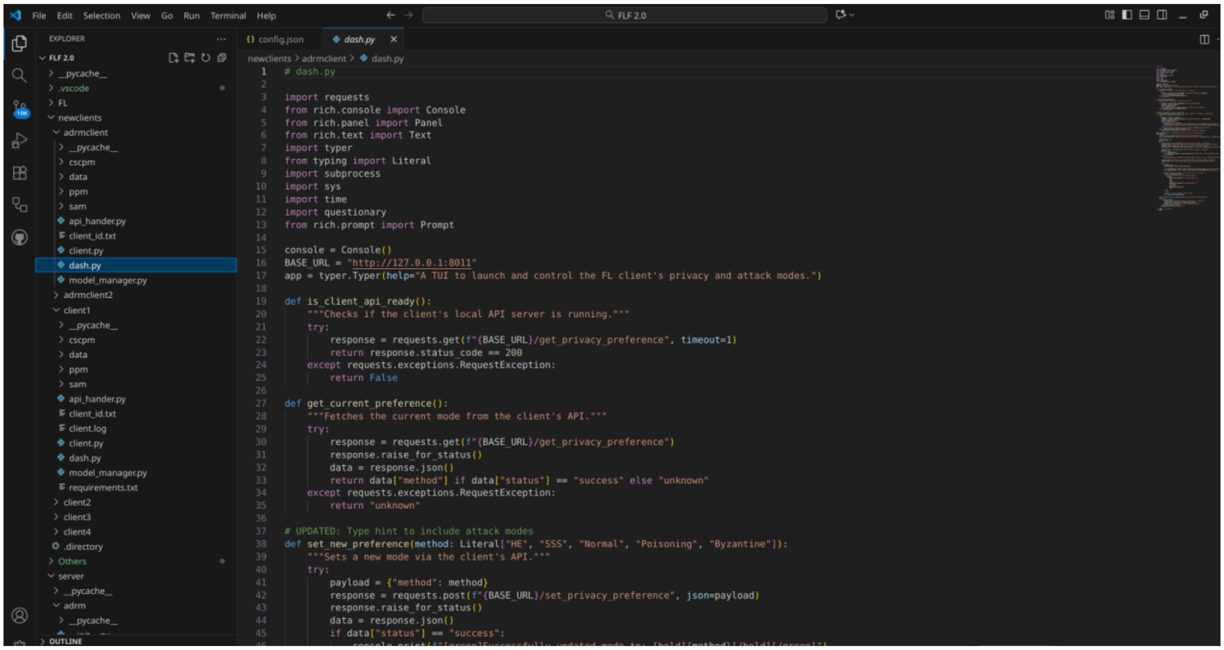
```
# server/adrm/response
 
import json
import os
import datetime
import asyncio
from typing import TYP
from . import config
from .logger_setup imp

if TYPE_CHECKING:
    from server.client

gen_logger, audit_logg

class ResponseSystem:
    """Handles graduat

    def __init__(self,
        self.client_ma
        self.blocked_c
        self.quarantin
        self._load_blo

    def _load_blocked_
        """Loads block
        if os.path.exi
            try:
                with c
                    se
                gen_lo
            except (IC
                gen_lo

    def _save_blocked_
        """Saves the c
        try:
            with open(
                json.d
            audit_logg
        except IOError
            gen_logger

    def trigger_respon
        """Triggers a
        audit_logger.w
```

```
# server/adrm/logger_s

import logging
# UPDATED: Changed to
from . import config

def setup_loggers():
    """Sets up and ret

    # --- General Logg
    gen_logger = loggi
    gen_logger.setLeve
    gen_formatter = lc
    if not gen_logger.
        gen_file_handl
        gen_file_handl
        gen_logger.add

        console_handle
        console_handle
        gen_logger.add

    # --- Audit Logger
    audit_logger = log
    audit_logger.setLe
    audit_formatter =
    if not audit_logge
        audit_file_han
        audit_file_han
        audit_logger.a

    # Prevent audit lc
    audit_logger.propa

    return gen_logger,
```

```
# server/adrm/config.p

import os

# --- Directory and Fi
DB_DIR = "database"
LOG_DIR = "logs"
MODEL_DIR = os.path.jo

# Ensure directories e
os.makedirs(DB_DIR, ex
os.makedirs(LOG_DIR, e
os.makedirs(MODEL_DIR,

BLOCKED_CLIENTS_FILE =
AUDIT_LOG_FILE = os.pa
GENERAL_LOG_FILE = os.
PERFORMANCE_LOG_FILE =

# ML Model Paths
CHAMPION_MODEL_PATH =
CHALLENGER_MODEL_PATH

# --- Response System
BLOCK_DURATION_MINUTES
REPUTATION_PENALTY_FOR

# --- ML Model & Engin
# How much better (as
# 1.1 means the challe
PROMOTION_THRESHOLD =

# How many updates to
CHALLENGER_TRAINING_BA


# --- NEWLY ADDED ---
# The statistical thre
# A common value is 3.
CROSS_CLIENT_THRESHOLD
```

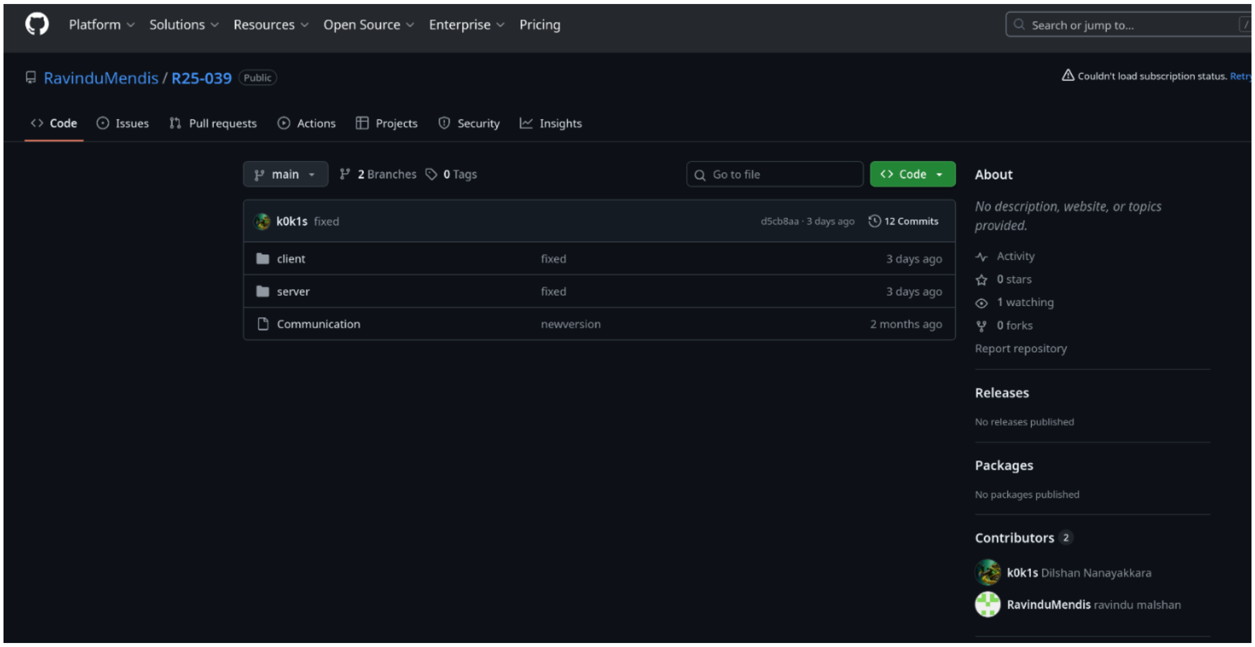
```
# server/adrm/adrm_engine.py

import torch
import numpy as np
from typing import Dict, Any, List

from . import config
from .logger_setup import setup_loggers
from .model_manager import ADRMModelManager
from .response_system import ResponseSystem

gen_logger, audit_logger = setup_loggers()

class ADRMEngine:
    """
    The core detection engine for the ADRM, featuring
    1. An ML-based check for each individual update.
    2. A statistical cross-client (peer) check for the
    """

    def __init__(self, model_manager: ADRMModelManager
        self.model_manager = model_manager
        self.response_system = response_system
        self.training_data_buffer = []

    def _featurize_update(self, update: Dict[str, torc
        """Extracts a feature vector from a raw model
        if not update:
            return np.zeros((1, 5))

        # FIX: Filter for torch.Tensor types to ignore
        tensor_values = [p for p in update.values() if
        if not tensor_values:
            return np.zeros((1, 5))

        flat_vector = torch.cat([p.view(-1) for p in t

        if flat_vector.numel() == 0:
            return np.zeros((1, 5))

        mean = torch.mean(flat_vector).item()
        std = torch.std(flat_vector).item()
        min_val = torch.min(flat_vector).item()
        max_val = torch.max(flat_vector).item()
        norm = torch.linalg.norm(flat_vector).item()
```

ADRM – Client



```
# dash.py

import requests
from rich.console import Console
from rich.panel import Panel
from rich.text import Text
import typer
from typing import Literal
import subprocess
import sys
import time
import questionary
from rich.prompt import Prompt

console = Console()
BASE_URL = "http://127.0.0.1:8011"
app = typer.Typer(help="A TUI to launch and control the FL client's privacy and attack modes.")

def is_client_api_ready():
    """Checks if the client's local API server is running."""
    try:
        response = requests.get(f"{BASE_URL}/get_privacy_preference", timeout=1)
        return response.status_code == 200
    except requests.exceptions.RequestException:
        return False

def get_current_preference():
    """Fetches the current mode from the client's API."""
    try:
        response = requests.get(f"{BASE_URL}/get_privacy_preference")
        response.raise_for_status()
        data = response.json()
        return data["method"] if data["status"] == "success" else "unknown"
    except requests.exceptions.RequestException:
        return "unknown"

# UPDATED: Type hint to include attack modes
def set_new_preference(method: Literal["HE", "SSS", "Normal", "Poisoning", "Byzantine"]):
    """Sets a new mode via the client's API."""
    try:
        payload = {"method": method}
        response = requests.post(f"{BASE_URL}/set_privacy_preference", json=payload)
        response.raise_for_status()
        data = response.json()
        if data["status"] == "success":
            console.print(f"[green]Successfully updated mode to: [bold]{method}[/bold][/green]")
```

7. GitHub Upload



RavinduMendis / R25-039 Public

⚠ Couldn't load subscription status. Retry

2 Branches 0 Tags

k0k1s fixed d5cb8aa · 3 days ago 12 Commits

client	fixed	3 days ago
server	fixed	3 days ago
Communication	newversion	2 months ago

About

No description, website, or topics provided.

Activity
0 stars
1 watching
0 forks
Report repository

Releases

No releases published

Packages

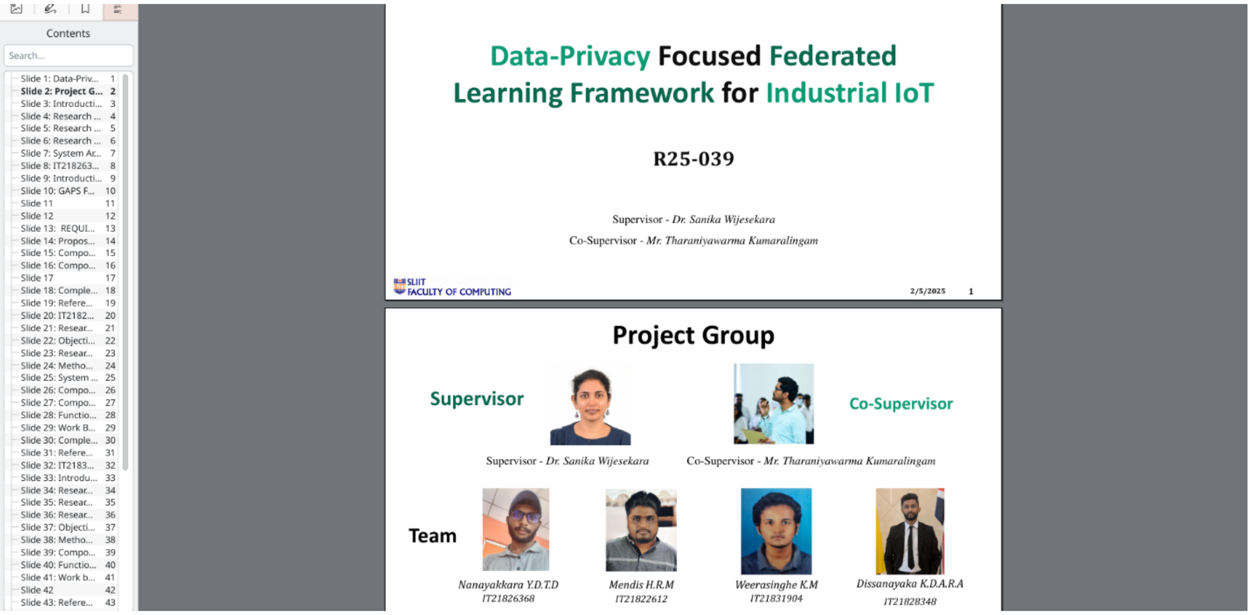
No packages published

Contributors 2

k0k1s Dilshan Nanayakkara
RavinduMendis ravindu malshan

8. Documentation

8.1 Proposal



Data-Privacy Focused Federated Learning Framework for Industrial IoT

R25-039

Supervisor - *Dr. Sanika Wijesekara*
Co-Supervisor - *Mr. Tharaniyawarma Kumaralingam*

SLIIT FACULTY OF COMPUTING

2/5/2025 1

Project Group

Supervisor

Co-Supervisor

Supervisor - *Dr. Sanika Wijesekara*
Co-Supervisor - *Mr. Tharaniyawarma Kumaralingam*

Team

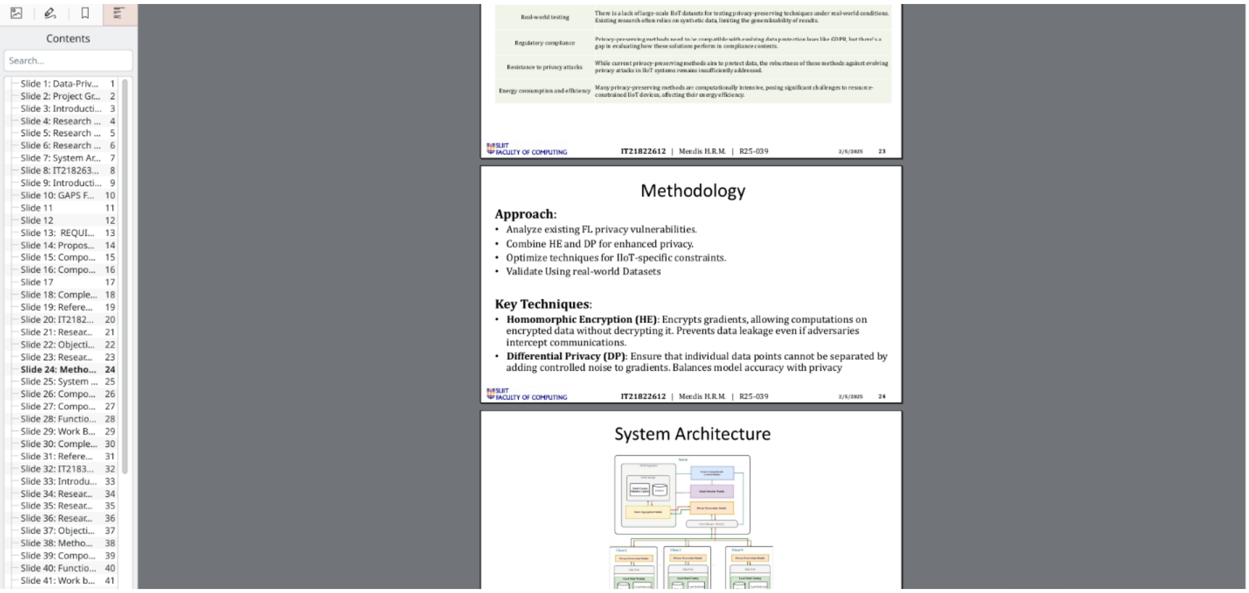
Nanayakkara Y.D.T.D
IT21826368

Mendis H.R.M
IT21822612

Weerasinghe K.M
IT21831904

Dissanayaka K.D.A.R.A
IT21828348

8.2 Presentation 1



Contents

Search...

Real-world testing	There is a lack of large-scale IIoT datasets for testing privacy-preserving techniques under real-world conditions. Existing research often relies on synthetic data, limiting the generalizability of results.
Regulatory compliance	Privacy-preserving methods need to be compatible with evolving data protection laws like GDPR, but there's a gap in evaluating how these solutions perform in compliance contexts.
Resistance to privacy attacks	While current privacy-preserving methods aim to protect data, the robustness of these methods against evolving privacy attacks in IIoT systems remains insufficiently addressed.
Energy consumption and efficiency	Many privacy-preserving methods are computationally intensive, posing significant challenges to resource-constrained IIoT devices, affecting their energy efficiency.

SLIIT FACULTY OF COMPUTING IT21822612 | Mendis H.R.M. | R25-039 2/5/2025 23

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

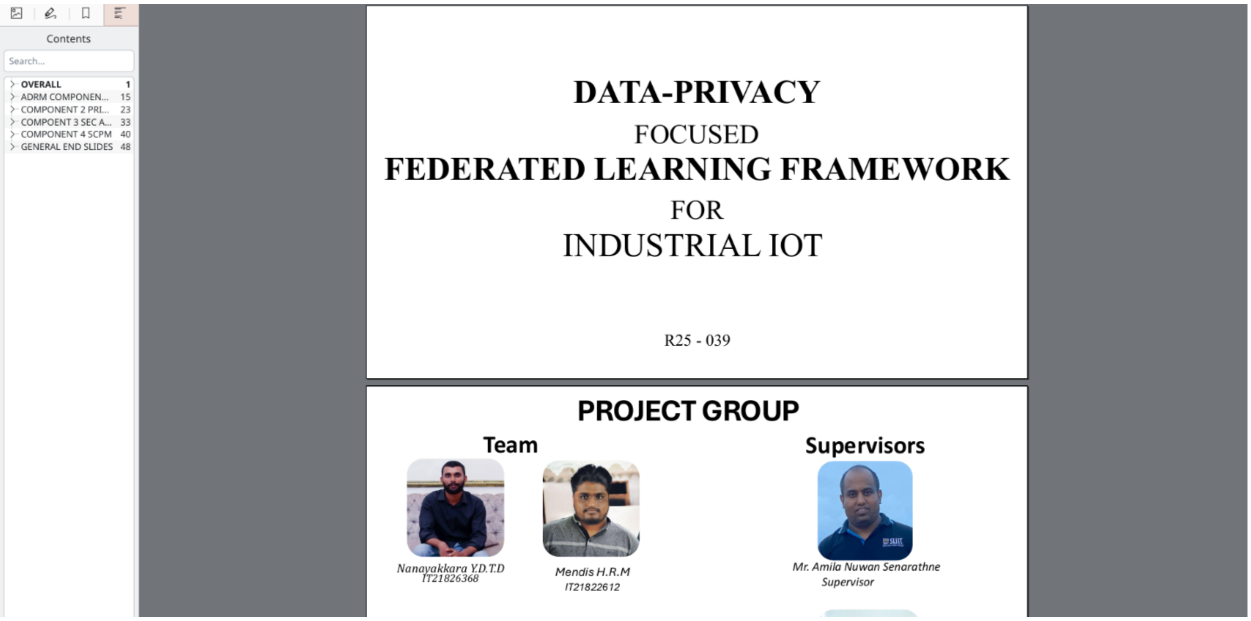
Key Techniques:

- **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

SLIIT FACULTY OF COMPUTING IT21822612 | Mendis H.R.M. | R25-039 2/5/2025 24

System Architecture

8.3 Presentation 2



Contents

Search...

DATA-PRIVACY

FOCUSED

FEDERATED LEARNING FRAMEWORK

FOR

INDUSTRIAL IOT

R25 - 039

PROJECT GROUP

Team

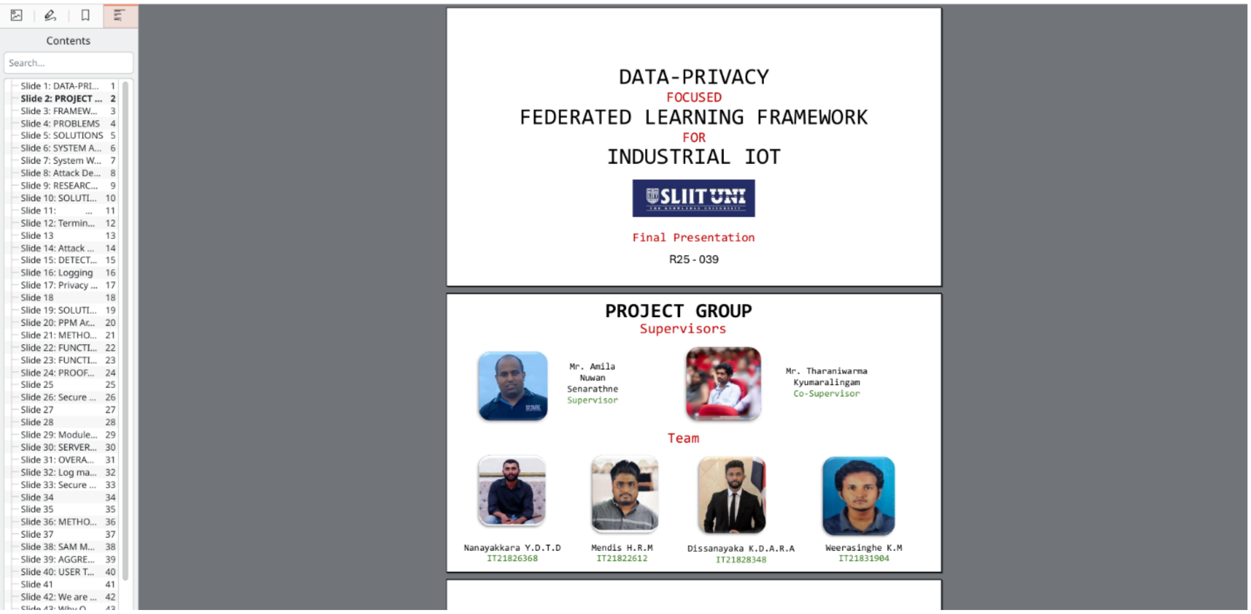
Nanayakkara Y.D.T.D
IT21826368

Mendis H.R.M
IT21822612

Supervisors

Mr. Amila Nuwan Senarathne
Supervisor

8.4 Final Presentation



DATA-PRIVACY
FOCUSED
FEDERATED LEARNING FRAMEWORK
FOR
INDUSTRIAL IOT

Final Presentation

R25 - 039

PROJECT GROUP

Supervisors

Mr. Amila Nuwan Senarathne
Supervisor

Mr. Tharaniwarma Kyumaralingam
Co-Supervisor

Team

Nanayakkara Y.D.T.D
IT21826368

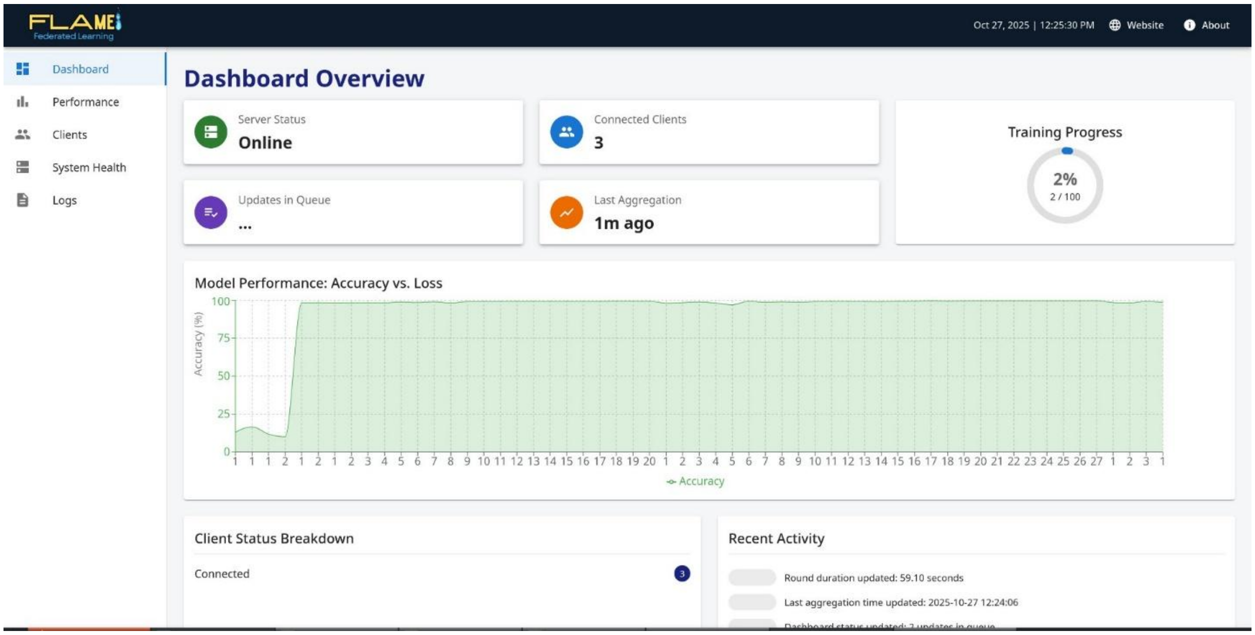
Mendis H.R.M
IT21822612

Dissanayaka K.D.A.R.A
IT21828348

Weerasinghe K.M
IT21831904

8.5 Final Product

Web Portal Frontend



Dashboard Overview

Server Status
Online

Connected Clients
3

Training Progress
2%
2 / 100

Updates in Queue
...

Last Aggregation
1m ago

Model Performance: Accuracy vs. Loss

Client Status Breakdown

Connected 3

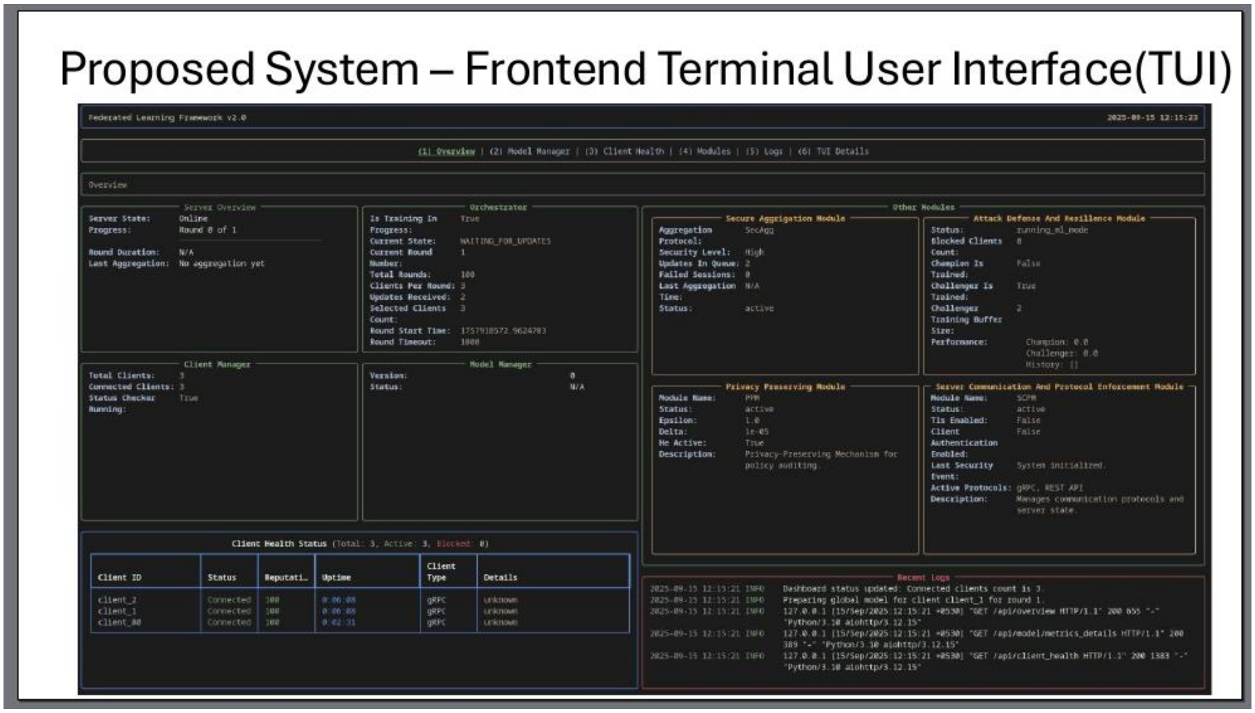
Recent Activity

Round duration updated: 59.10 seconds

Last aggregation time updated: 2025-10-27 12:24:06

Dashboard status updated: 2 updates in queue

Terminal User interface (Frontend)

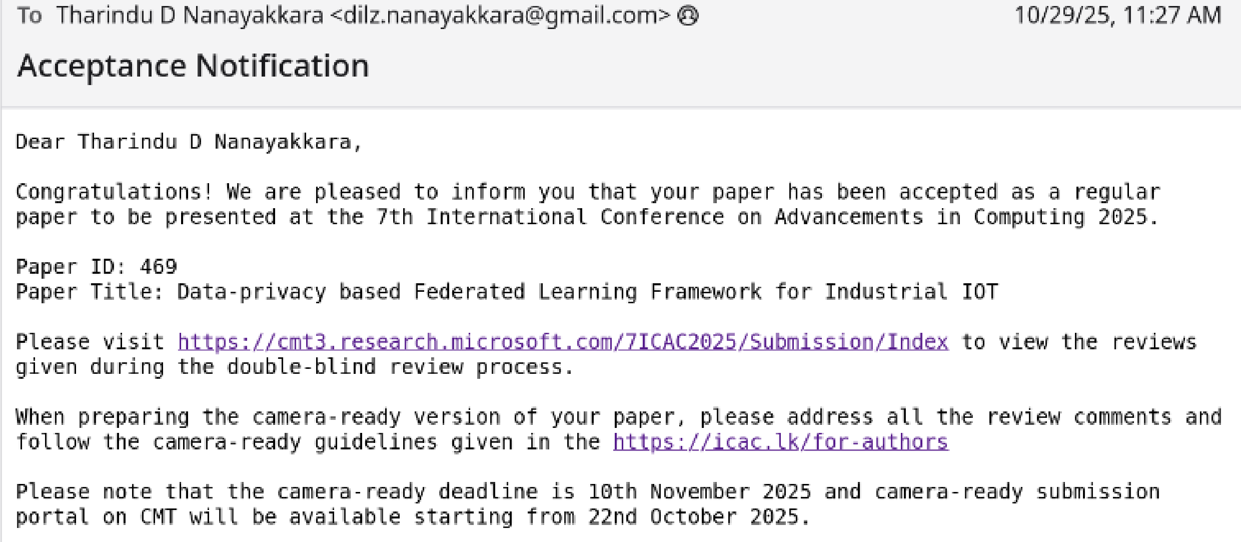


Proposed System – Frontend Terminal User Interface(TUI)

```
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      True
Progress:
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:   1757918572.9624783
Round Timeout:      1000

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

Attack Defense And Resillence 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
He 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       System initialized.
Event:
Active Protocols:   gRPC, REST API
Description:        Manages communication protocols and
                    server state.

Client Health Status (Total: 3, Active: 3, Blocked: 0)
Client ID     Status      Reputati…   Uptime     Client Type   Details
client_2      Connected   100         0:00:08    gRPC          unknown
client_1      Connected   100         0:00:08    gRPC          unknown
client_00     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"
```

8.6 Research Paper

III. Conference Appetence



To Tharindu D Nanayakkara <dilz.nanayakkara@gmail.com> 10/29/25, 11:27 AM

Acceptance Notification

Dear Tharindu D Nanayakkara,

Congratulations! We are pleased to inform you that your paper has been accepted as a regular paper to be presented at the 7th International Conference on Advancements in Computing 2025.

Paper ID: 469
Paper Title: Data-privacy based Federated Learning Framework for Industrial IOT

Please visit https://cmt3.research.microsoft.com/7ICAC2025/Submission/Index to view the reviews given during the double-blind review process.

When preparing the camera-ready version of your paper, please address all the review comments and follow the camera-ready guidelines given in the https://icac.lk/for-authors

Please note that the camera-ready deadline is 10th November 2025 and camera-ready submission portal on CMT will be available starting from 22nd October 2025.

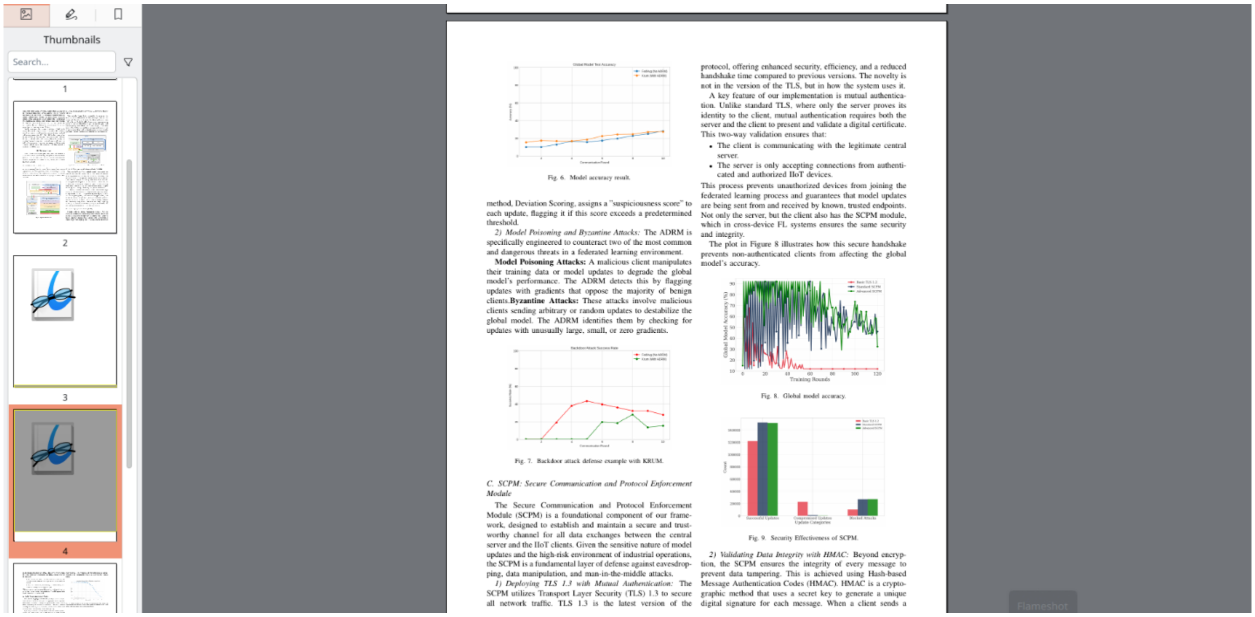


Fig. 6. Model accuracy result.

method, Deviation Scoring, assigns a "suspiciousness score" to each update, flagging it if this score exceeds a predetermined threshold.

2) Model Poisoning and Byzantine Attacks: The ADRM is specifically engineered to counteract two of the most common and dangerous threats in a federated learning environment.

Model Poisoning Attacks: A malicious client manipulates their training data or model updates to degrade the global model's performance. The ADRM detects this by flagging updates with gradients that oppose the majority of benign clients.**Byzantine Attacks:** These attacks involve malicious clients sending arbitrary or random updates to destabilize the global model. The ADRM identifies them by checking for updates with unusually large, small, or zero gradients.

Fig. 7. Backdoor attack defense example with KRUM.

C. SCPM: Secure Communication and Protocol Enforcement Module

The Secure Communication and Protocol Enforcement Module (SCPM) is a foundational component of our framework, designed to establish and maintain a secure and trustworthy channel for all data exchanges between the central server and the IIoT clients. Given the sensitive nature of model updates and the high-risk environment of industrial operations, the SCPM is a fundamental layer of defense against eavesdropping, data manipulation, and man-in-the-middle attacks.

1) Deploying TLS 1.3 with Mutual Authentication: The SCPM utilizes Transport Layer Security (TLS) 1.3 to secure all network traffic. TLS 1.3 is the latest version of the protocol, offering enhanced security, efficiency, and a reduced handshake time compared to previous versions. The novelty is not in the version of the TLS, but in how the system uses it.

A key feature of our implementation is mutual authentication. Unlike standard TLS, where only the server proves its identity to the client, mutual authentication requires both the server and the client to present and validate a digital certificate. This two-way validation ensures that:

- The client is communicating with the legitimate central server.
- The server is only accepting connections from authenticated and authorized IIoT devices.

This process prevents unauthorized devices from joining the federated learning process and guarantees that model updates are being sent from and received by known, trusted endpoints. Not only the server, but the client also has the SCPM module, which in cross-device FL systems ensures the same security and integrity.

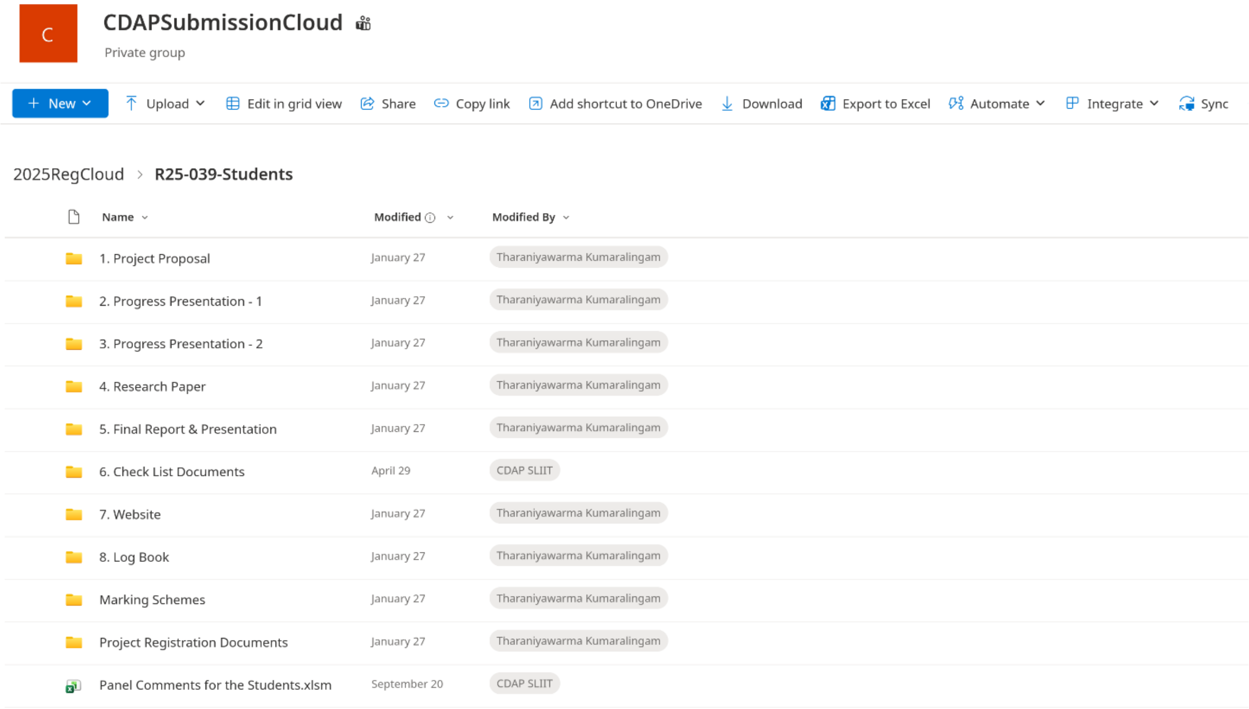
The plot in Figure 8 illustrates how this secure handshake prevents non-authenticated clients from affecting the global model's accuracy.

Fig. 8. Global model accuracy.

Fig. 9. Security Effectiveness of SCPM.

2) Validating Data Integrity with HMAC: Beyond encryption, the SCPM ensures the integrity of every message to prevent data tampering. This is achieved using Hash-based Message Authentication Codes (HMAC). HMAC is a cryptographic method that uses a secret key to generate a unique digital signature for each message. When a client sends a

9. CDAP upload



CDAPSubmissionCloud

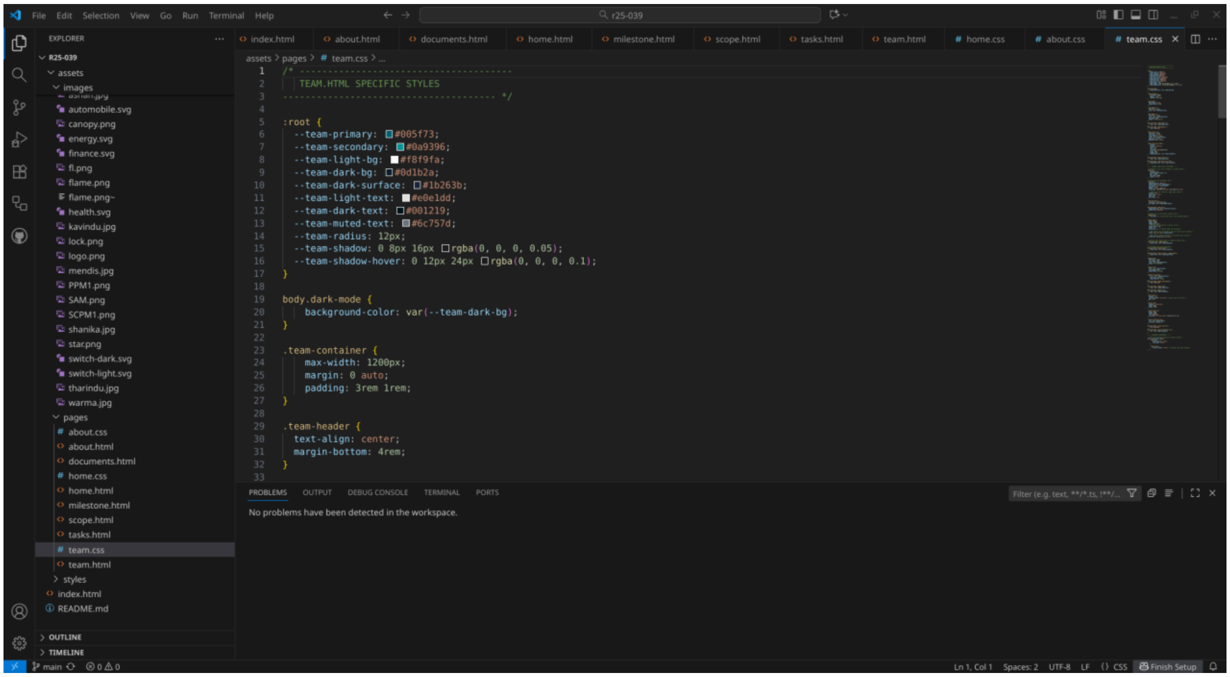
Private group

2025RegCloud > **R25-039-Students**

Name	Modified	Modified By
1. Project Proposal	January 27	Tharaniyawarma Kumaralingam
2. Progress Presentation - 1	January 27	Tharaniyawarma Kumaralingam
3. Progress Presentation - 2	January 27	Tharaniyawarma Kumaralingam
4. Research Paper	January 27	Tharaniyawarma Kumaralingam
5. Final Report & Presentation	January 27	Tharaniyawarma Kumaralingam
6. Check List Documents	April 29	CDAP SLIIT
7. Website	January 27	Tharaniyawarma Kumaralingam
8. Log Book	January 27	Tharaniyawarma Kumaralingam
Marking Schemes	January 27	Tharaniyawarma Kumaralingam
Project Registration Documents	January 27	Tharaniyawarma Kumaralingam
Panel Comments for the Students.xlsm	September 20	CDAP SLIIT

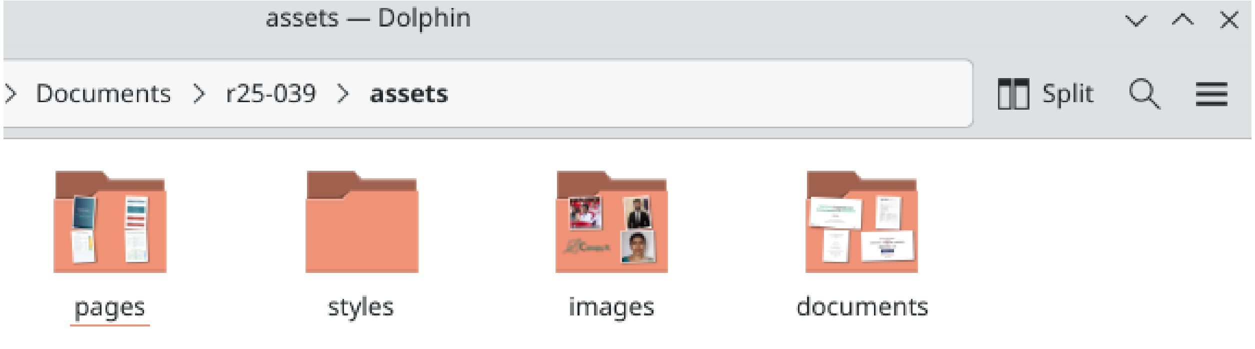
10.Website

10.1Development



```css
/* ------------------------------------
   TEAM.HTML SPECIFIC STYLES
------------------------------------ */

:root {
  --team-primary: #005f73;
  --team-secondary: #0a9396;
  --team-light-bg: #f8f9fa;
  --team-dark-bg: #0d1b2a;
  --team-dark-surface: #1b263b;
  --team-light-text: #e0e1dd;
  --team-dark-text: #001219;
  --team-muted-text: #6c757d;
  --team-radius: 12px;
  --team-shadow: 0 8px 16px rgba(0, 0, 0, 0.05);
  --team-shadow-hover: 0 12px 24px rgba(0, 0, 0, 0.1);
}

body.dark-mode {
    background-color: var(--team-dark-bg);
}

.team-container {
    max-width: 1200px;
    margin: 0 auto;
    padding: 3rem 1rem;
}

.team-header {
  text-align: center;
  margin-bottom: 4rem;
}

```

No problems have been detected in the workspace.



assets — Dolphin

> Documents > r25-039 > **assets**

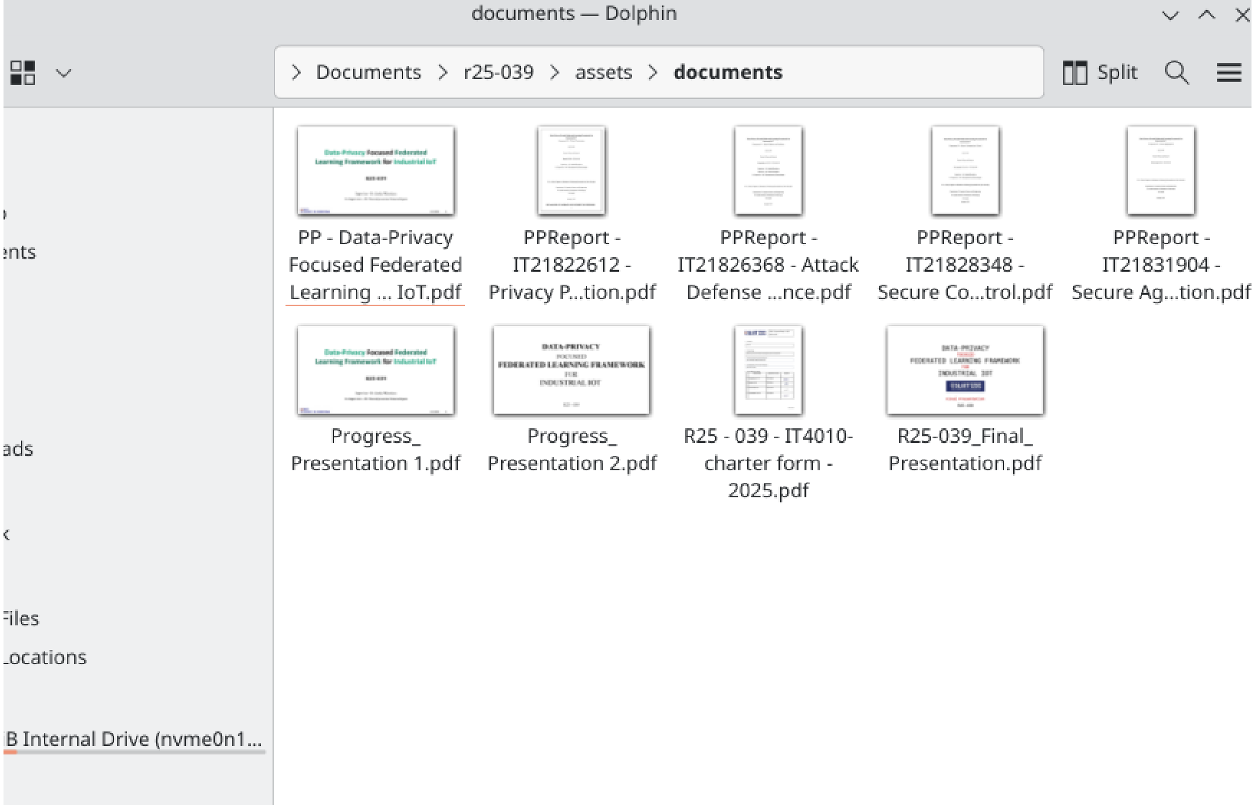
Split

pages

styles

images

documents



documents — Dolphin

> Documents > r25-039 > assets > **documents**

Split

PP - Data-Privacy Focused Federated Learning ... IoT.pdf

PPReport - IT21822612 - Privacy P...tion.pdf

PPReport - IT21826368 - Attack Defense ...nce.pdf

PPReport - IT21828348 - Secure Co...trol.pdf

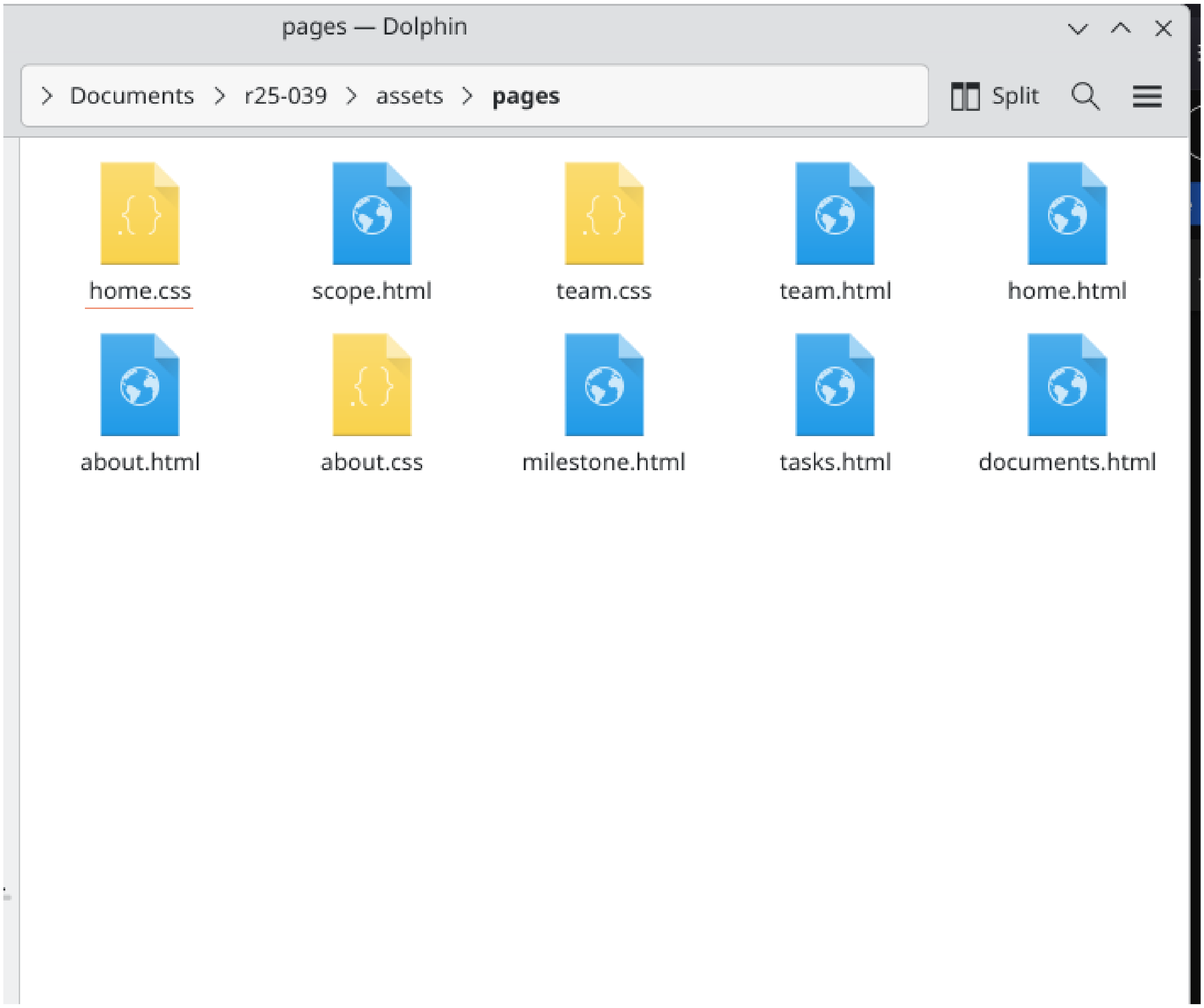
PPReport - IT21831904 - Secure Ag...tion.pdf

Progress_ Presentation 1.pdf

Progress_ Presentation 2.pdf

R25 - 039 - IT4010- charter form - 2025.pdf

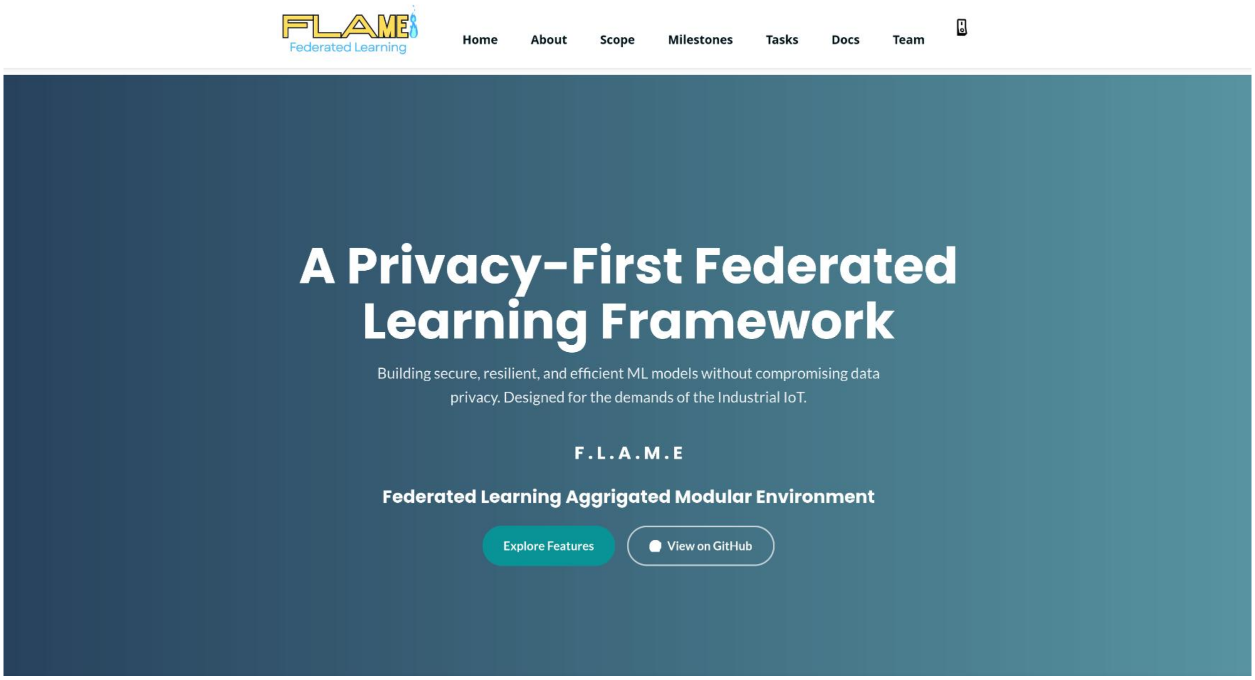
R25-039_Final_ Presentation.pdf



Documents > r25-039 > assets > pages

home.css
scope.html
team.css
team.html
home.html
about.html
about.css
milestone.html
tasks.html
documents.html

10.2 Finalize



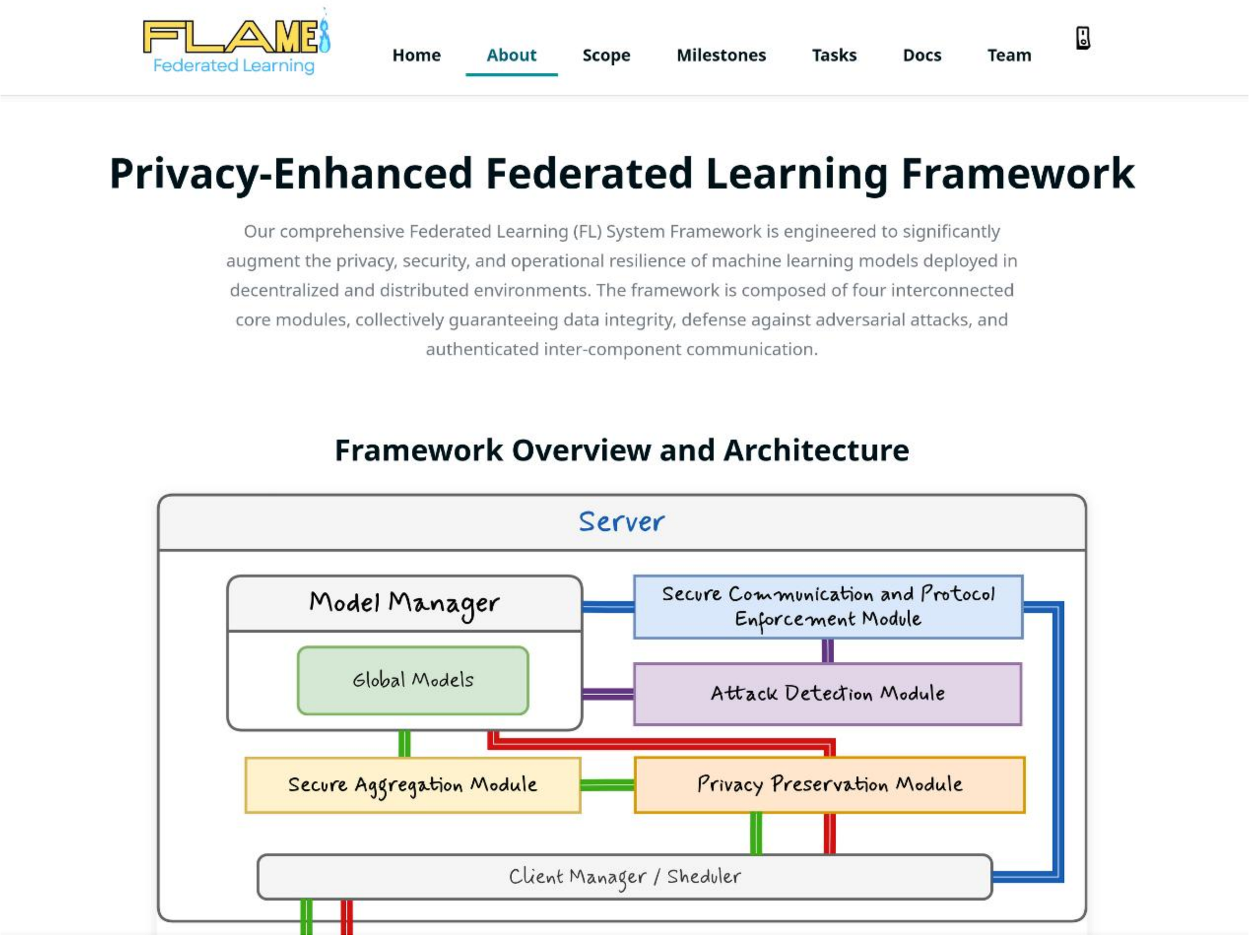
Home About Scope Milestones Tasks Docs Team

A Privacy-First Federated Learning Framework

Building secure, resilient, and efficient ML models without compromising data privacy. Designed for the demands of the Industrial IoT.

F.L.A.M.E

Federated Learning Aggrigated Modular Environment



FLAME Federated Learning

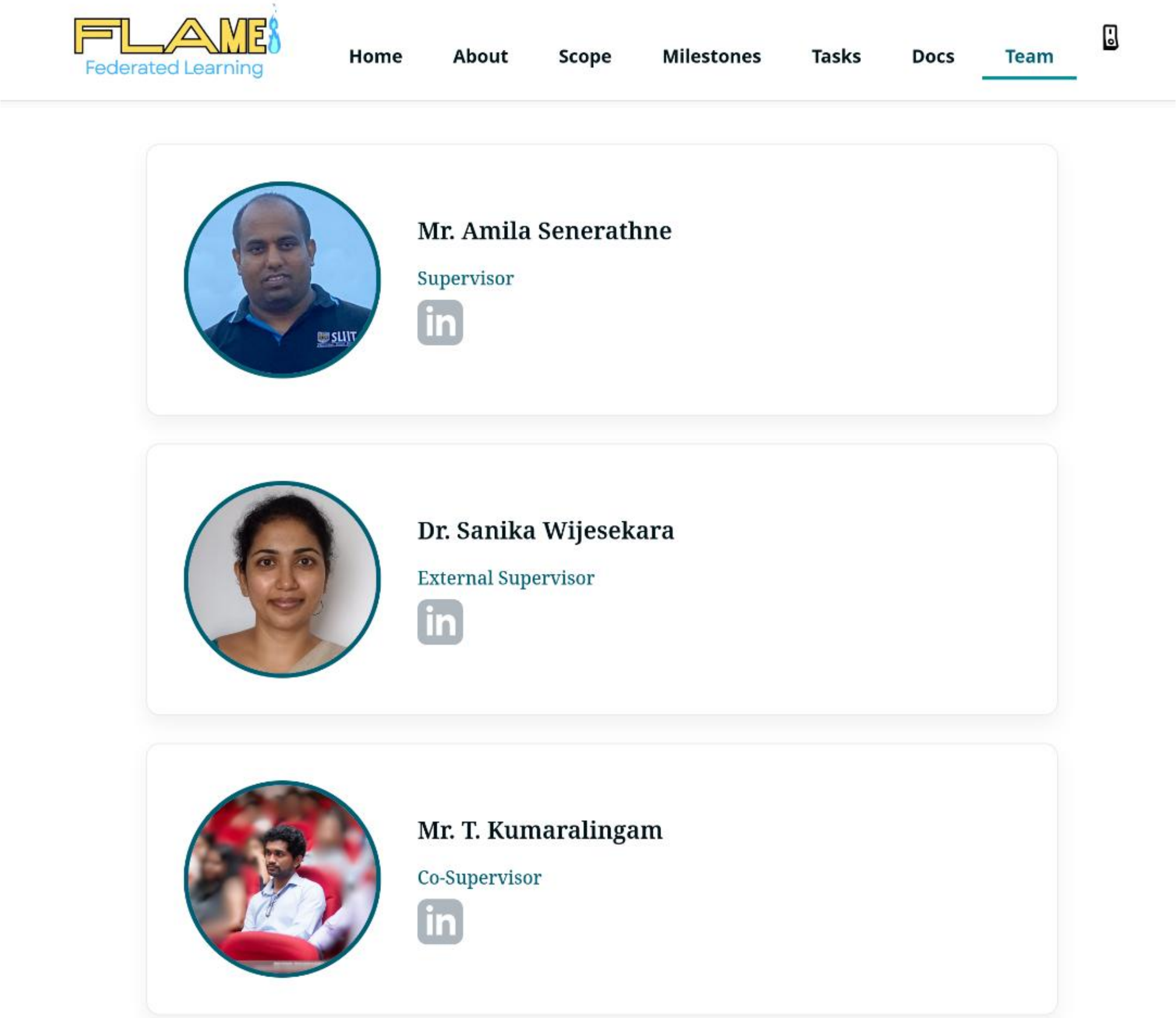
Home About Scope Milestones Tasks Docs Team

Privacy-Enhanced Federated Learning Framework

Our comprehensive Federated Learning (FL) System Framework is engineered to significantly augment the privacy, security, and operational resilience of machine learning models deployed in decentralized and distributed environments. The framework is composed of four interconnected core modules, collectively guaranteeing data integrity, defense against adversarial attacks, and authenticated inter-component communication.

Framework Overview and Architecture

Server
Model Manager
Global Models
Secure Communication and Protocol Enforcement Module
Attack Detection Module
Secure Aggregation Module
Privacy Preservation Module
Client Manager / Sheduler



Mr. Amila Senerathne

Supervisor

Dr. Sanika Wijesekara

External Supervisor

Mr. T. Kumaralingam

Co-Supervisor