Logbook – Secure Aggregation Module of R25 -039

Project ID: R25 - 039

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

Student Details:	
Names:	Student IDs:
Weerasinghe K.M	IT21831904

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 Resillence
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.

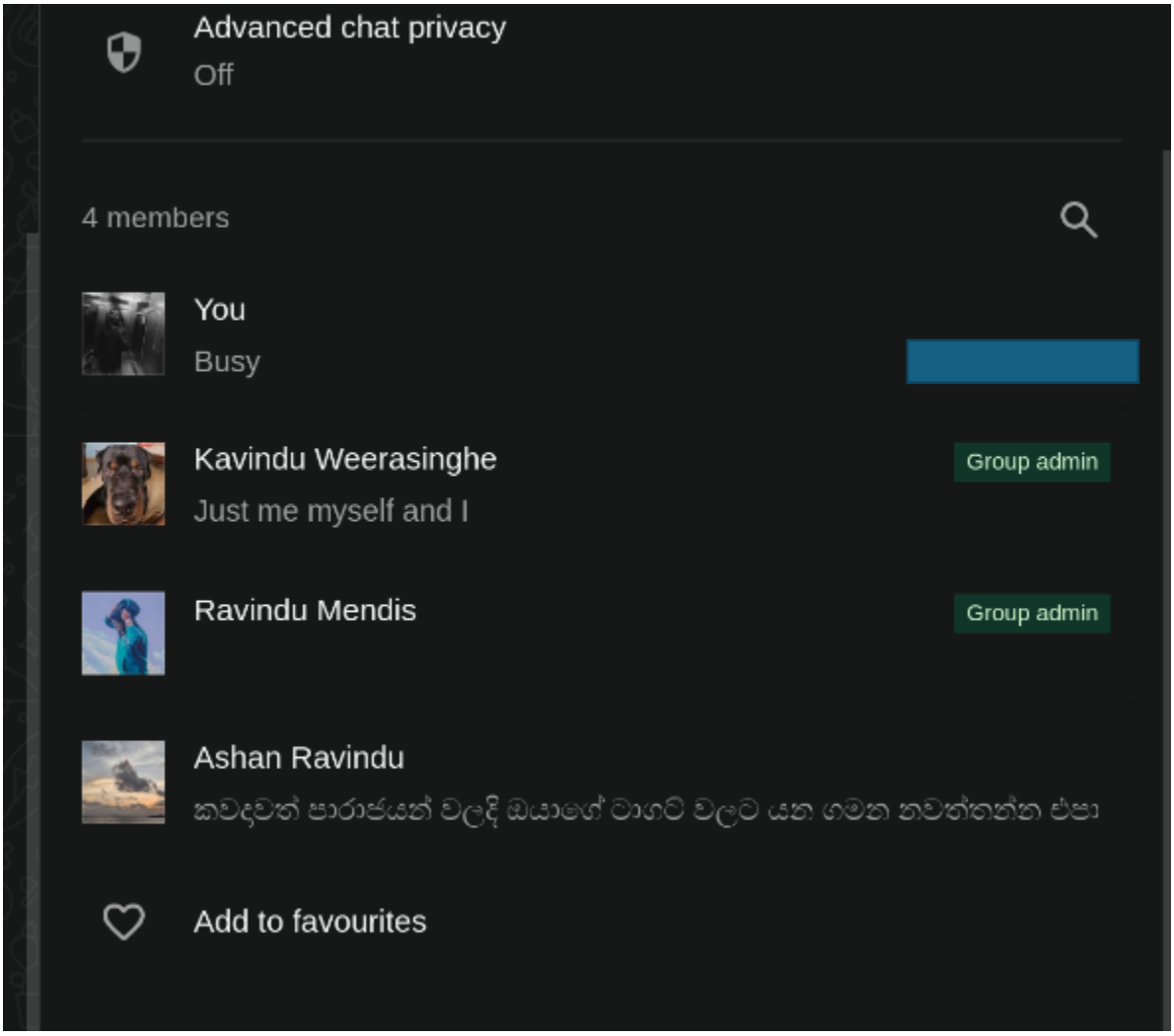
The Challenge: Traditional AI methods require centralizing sensitive factory data, which poses major **privacy risks** and clashes with the distributed nature of industrial operations. Existing FL solutions are insufficient because they fail to simultaneously provide robust security, data privacy, and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

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

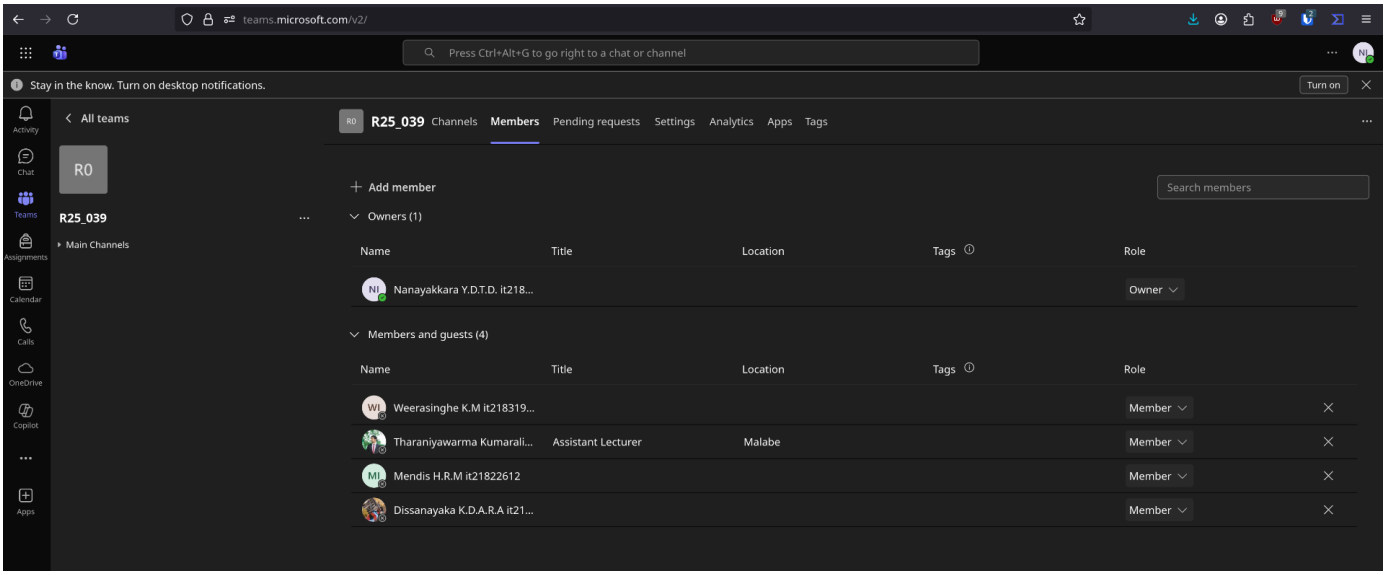
- It uses techniques like **Differential Privacy (DP)** and **Homomorphic Encryption (HE)** to guarantee data confidentiality.
- It implements a robust protocol that uses **client/server validation** to actively block cyber threats such as **Model Poisoning and Byzantine Attacks**.
- The system is optimized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

3. Communication Methods

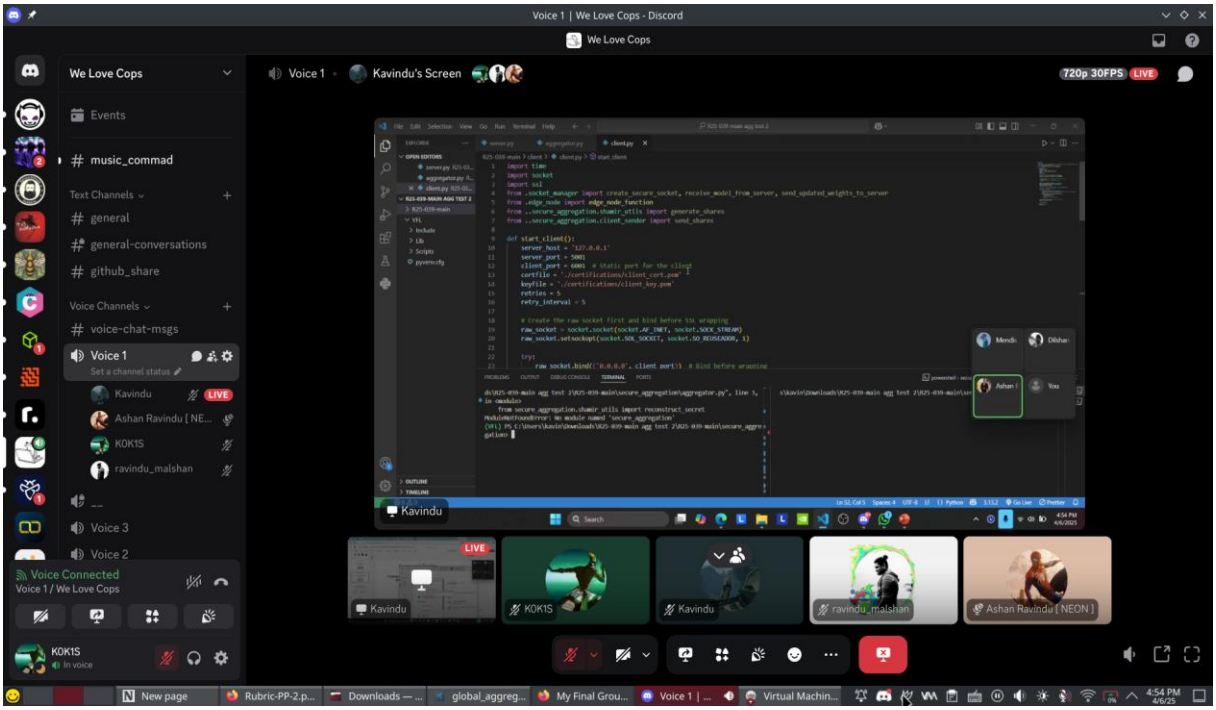
WhatsApp Group – Team



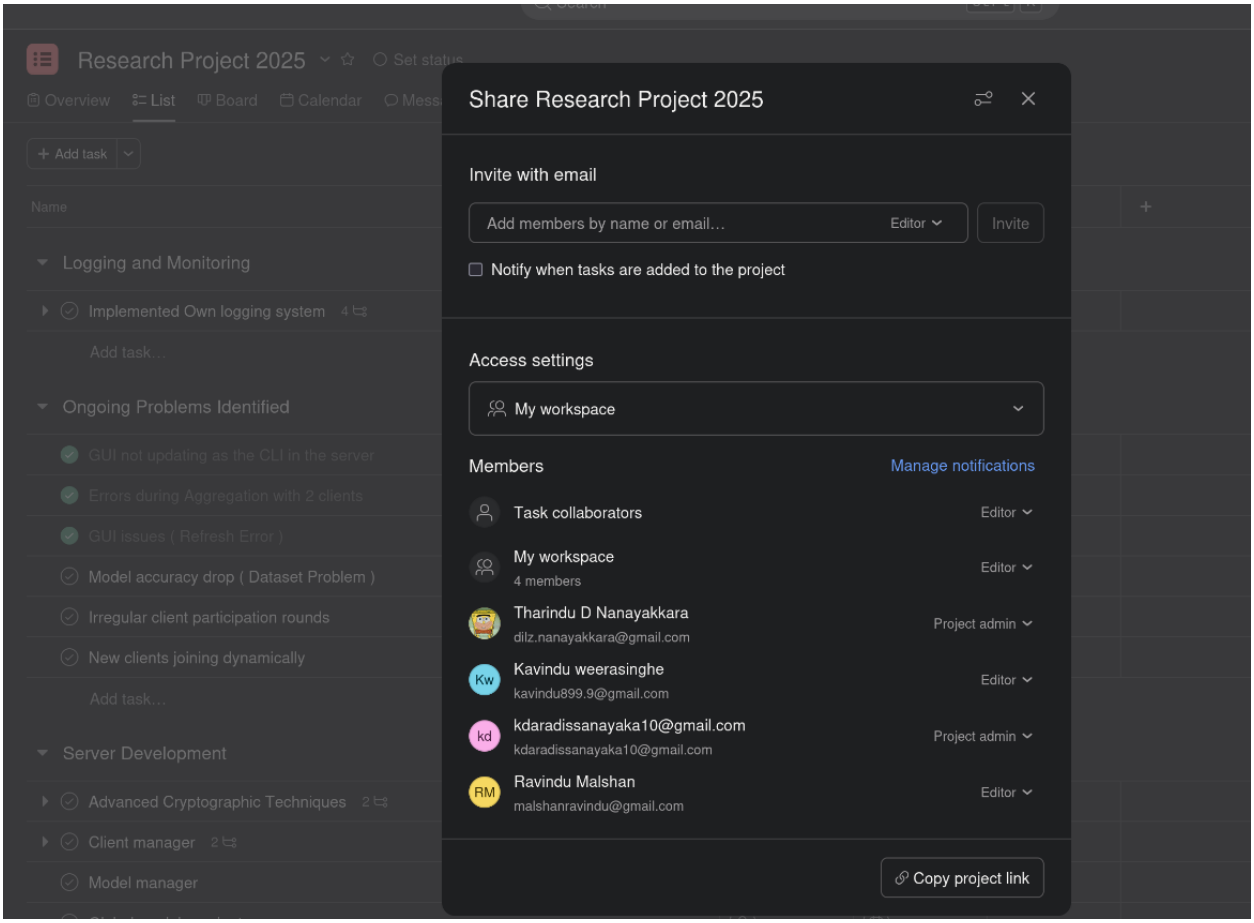
Microsoft Teams - All



Group Meetings – Discord – Team



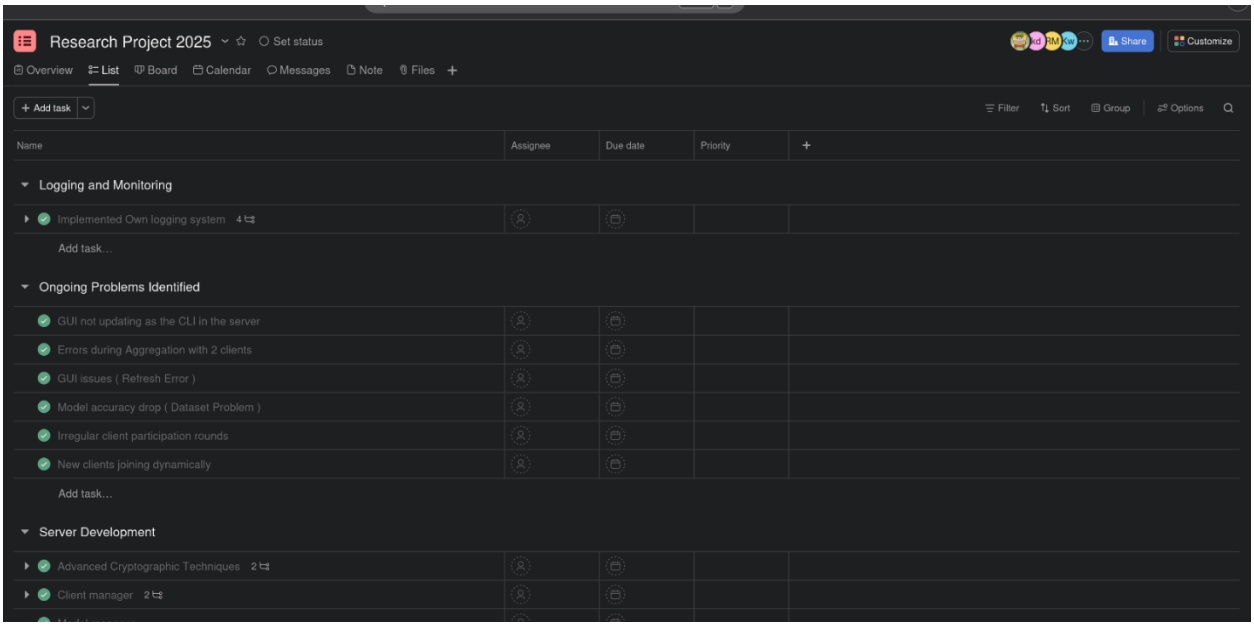
Asana – Task Assigning – Team



4. Meetings With Supervisors

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

5. Task Details



Secure Aggregation Module was mine.

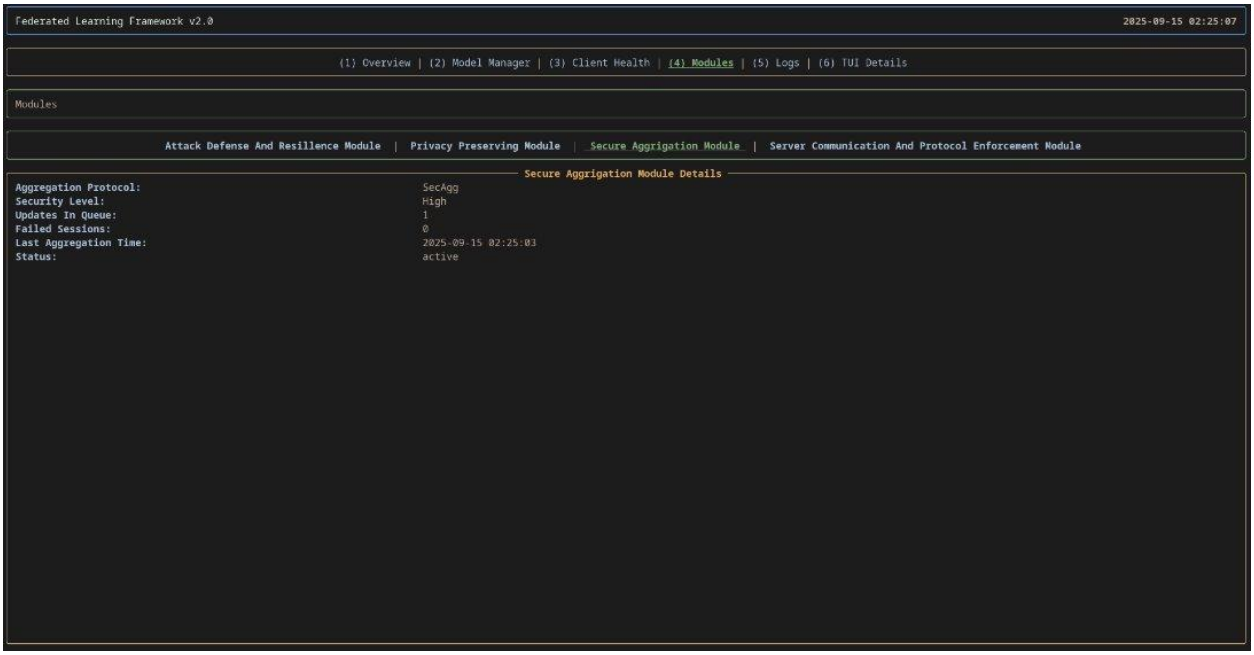
5.1 Personal task Assigning and Completion

6. System Details

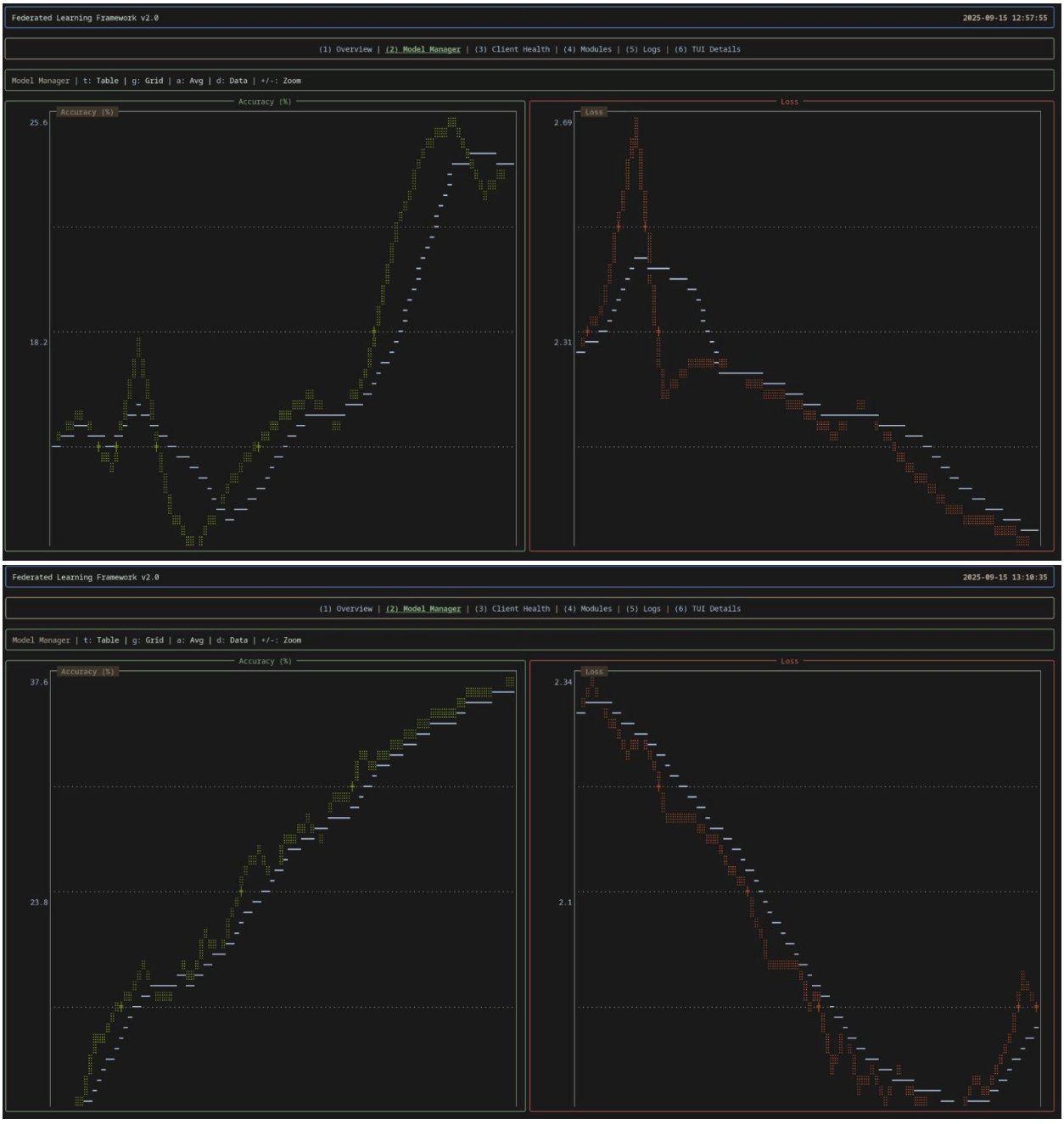
6.1 System completion status

Finished

SAM TUI

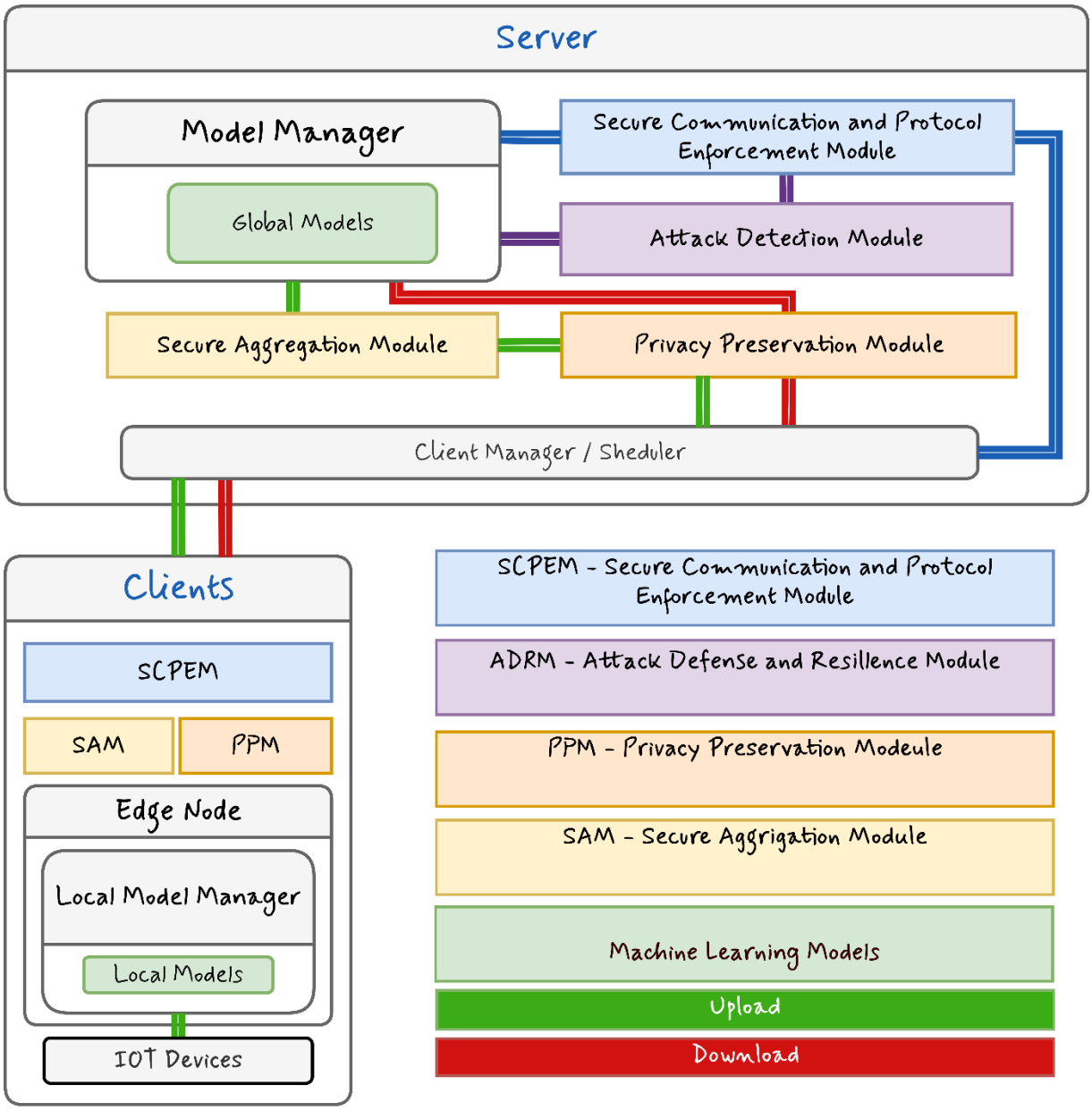


Aggregation Process server

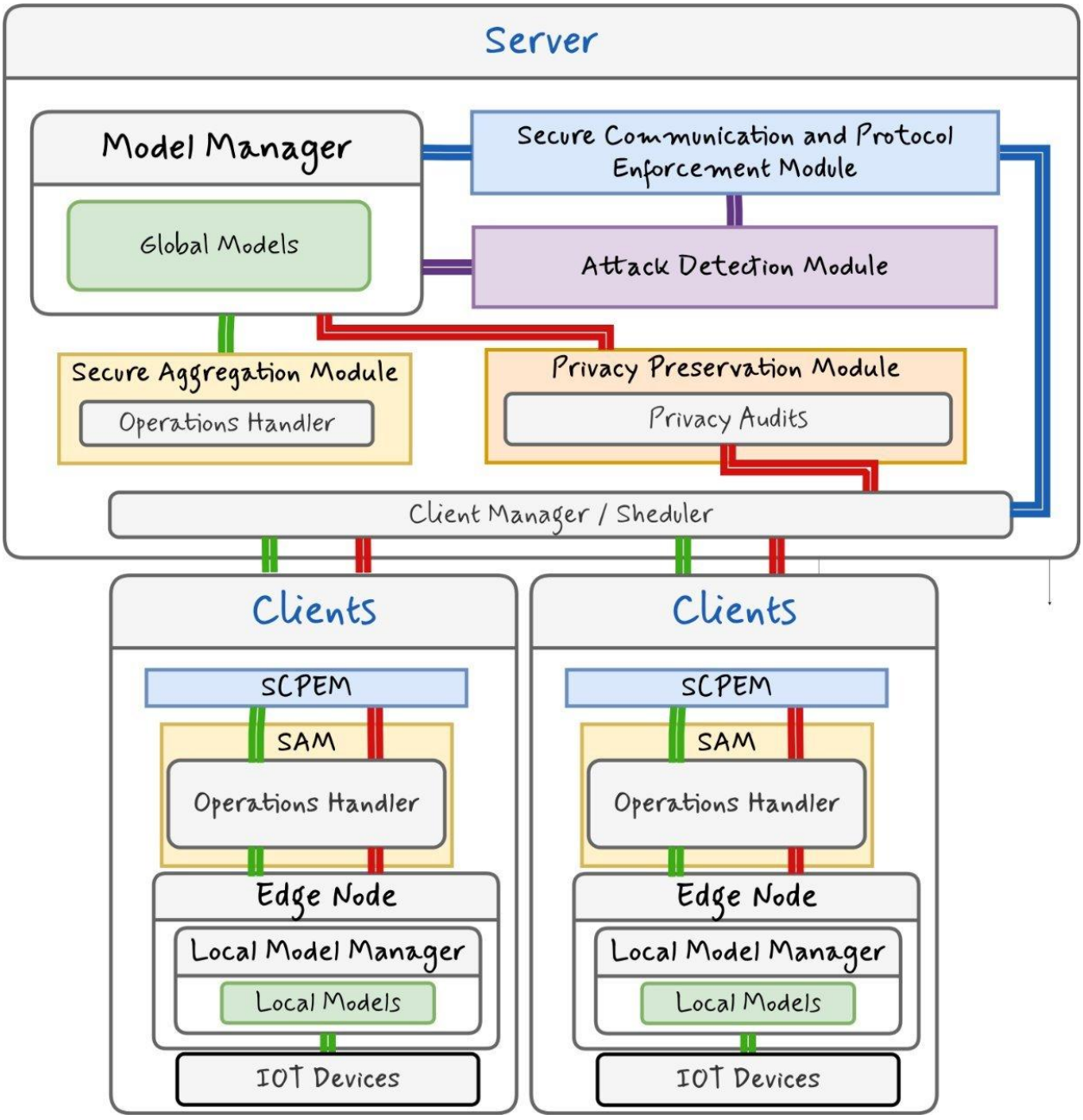


6.2 System Design

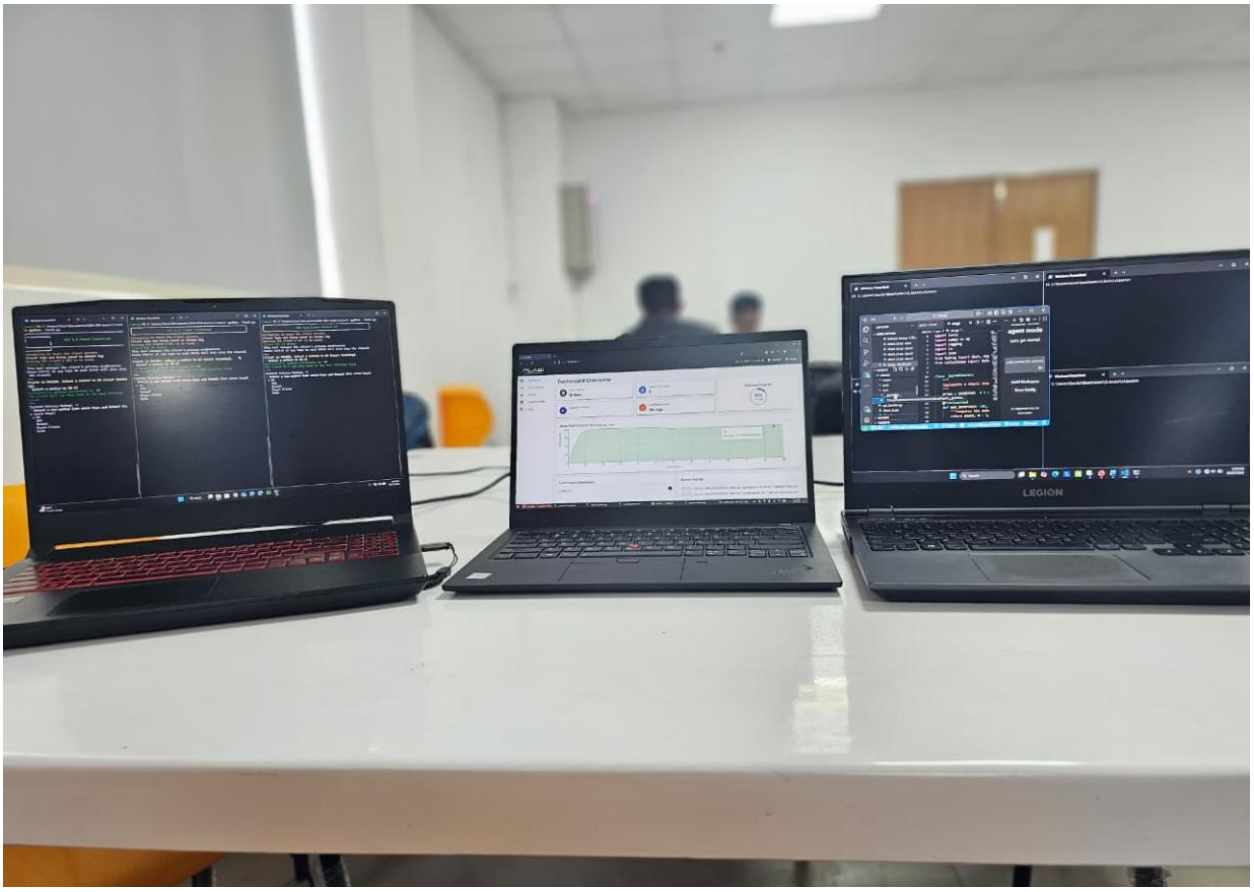
I. System Architecture



II. Module Architecture

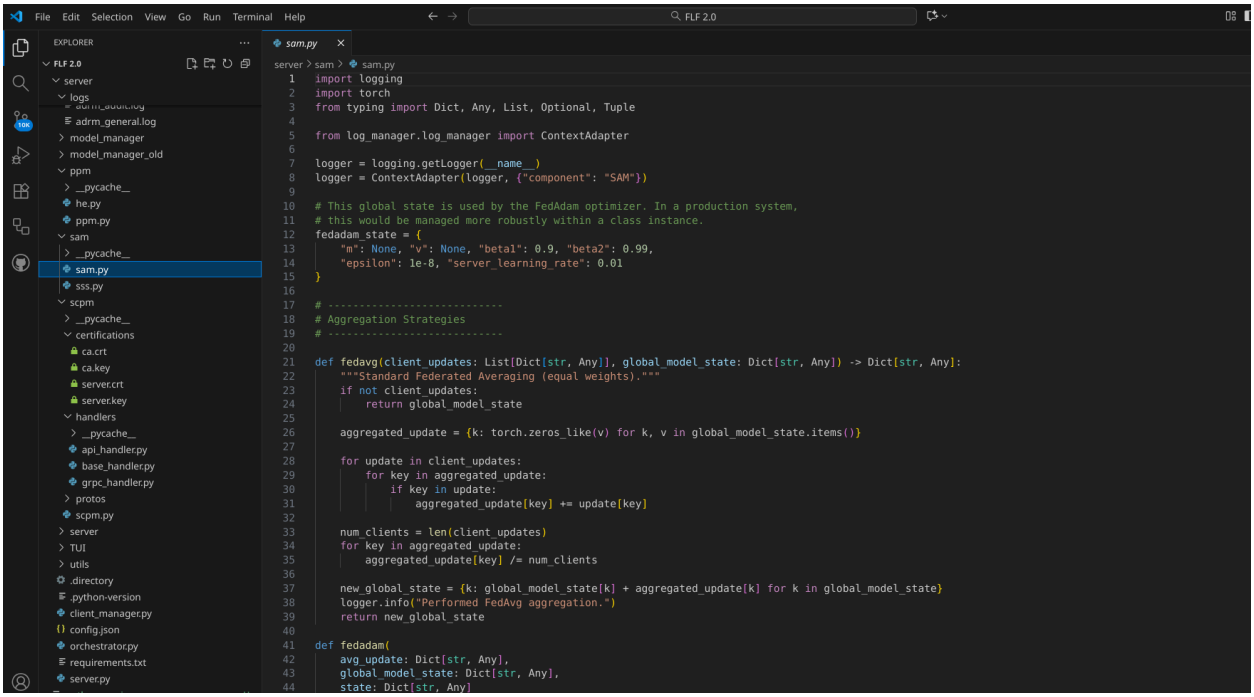


6.3 System Testing

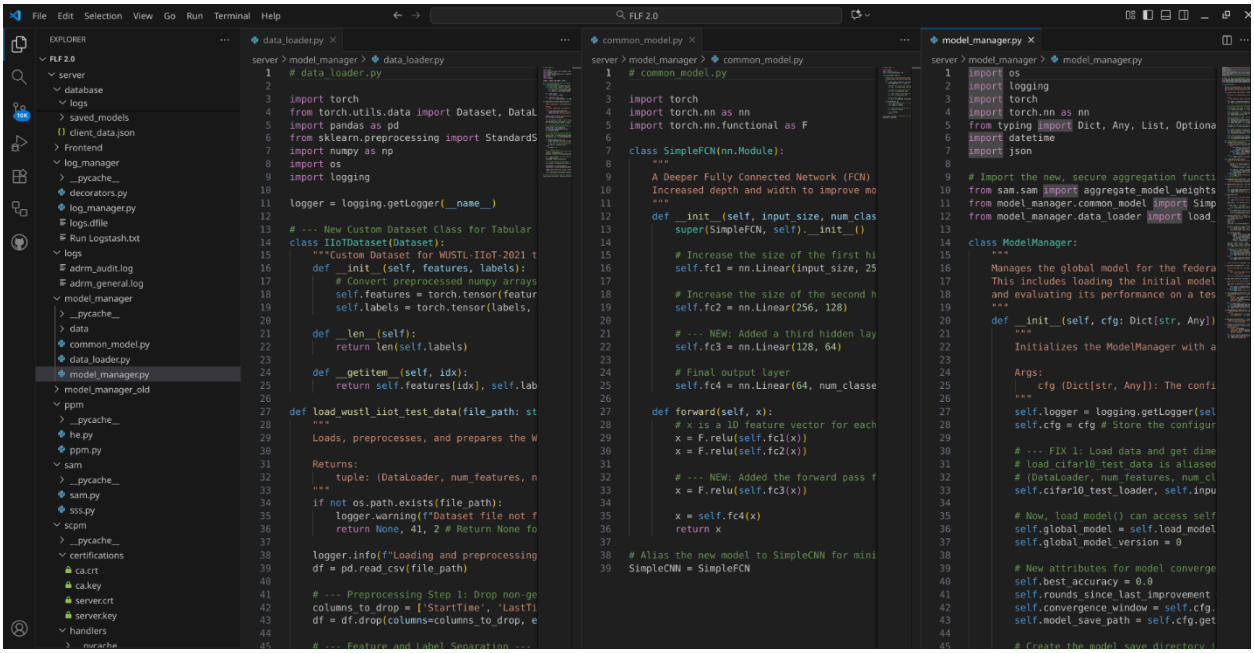


6.4 System Codes

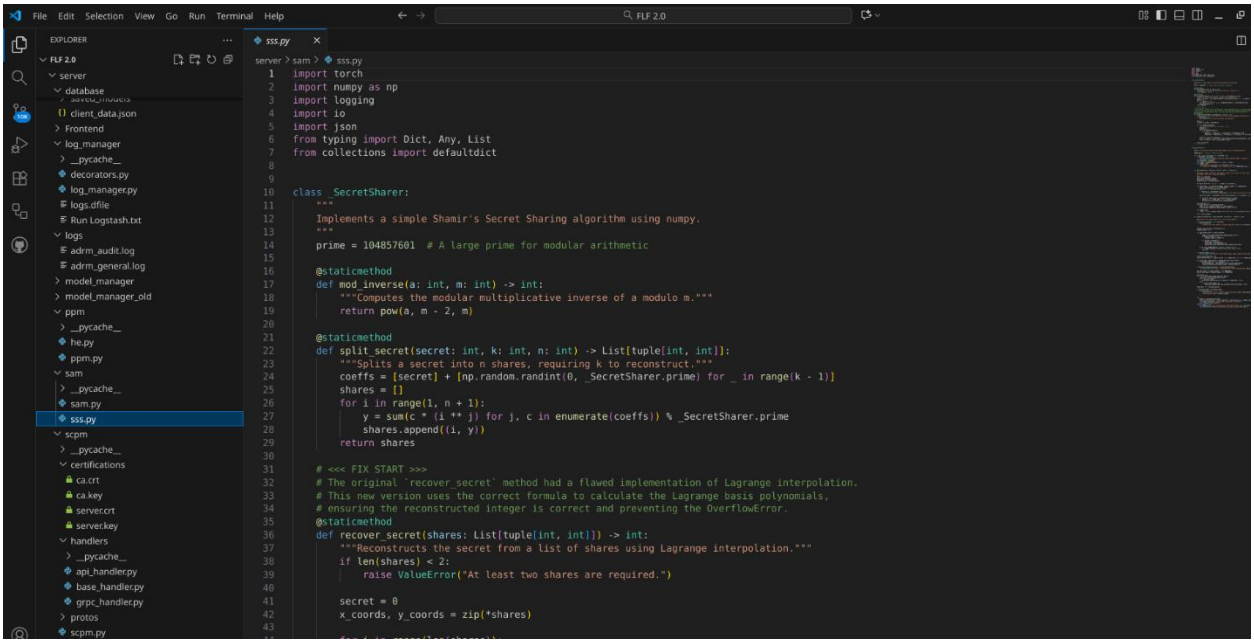
SAM – Server



Model manager

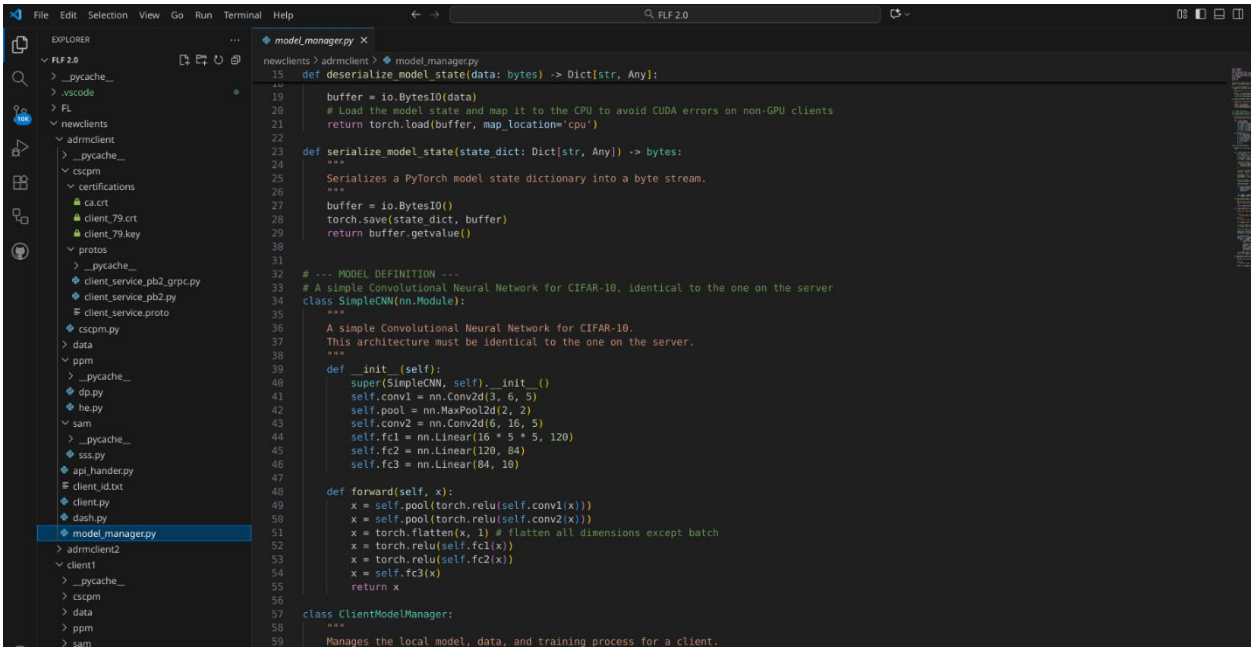


Shamir secret sharing

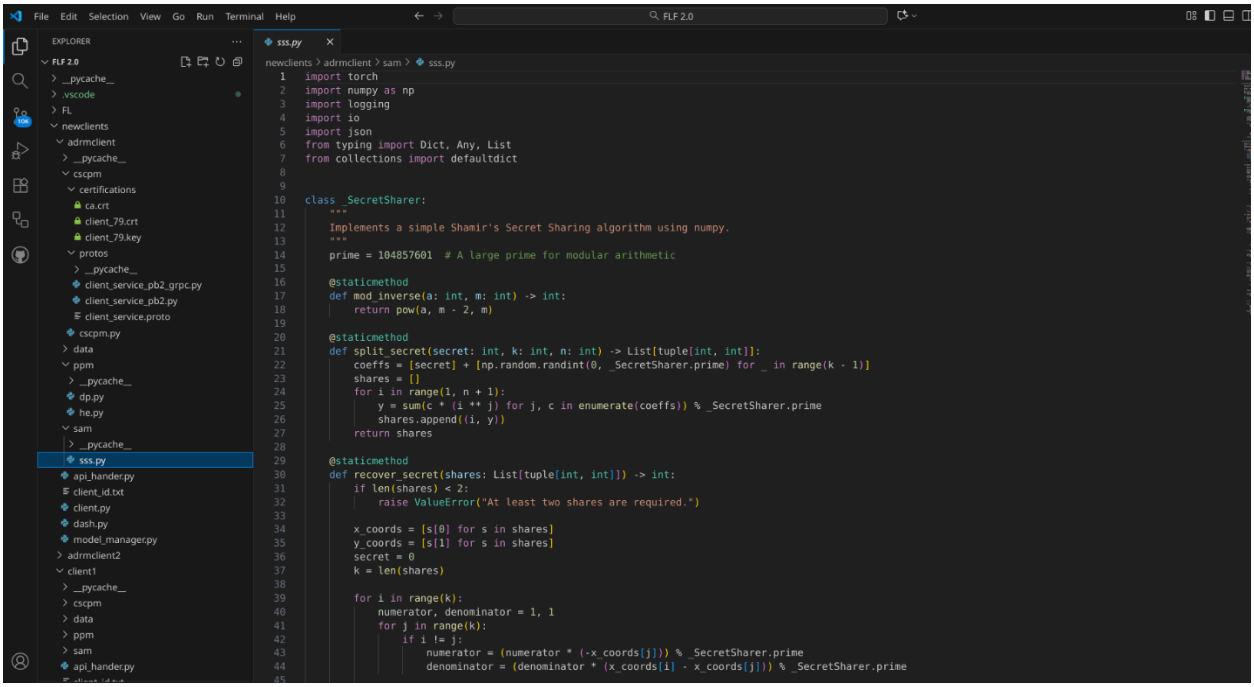


SAM – Client

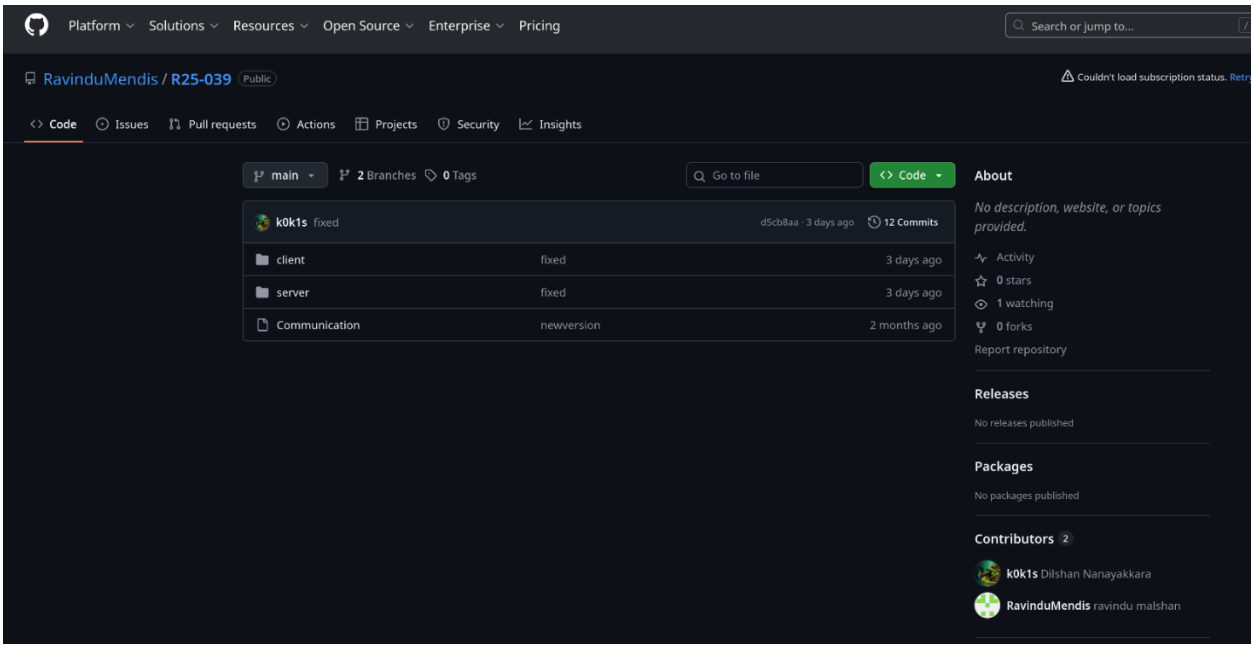
Model Manager



Sharmir secret Sharing

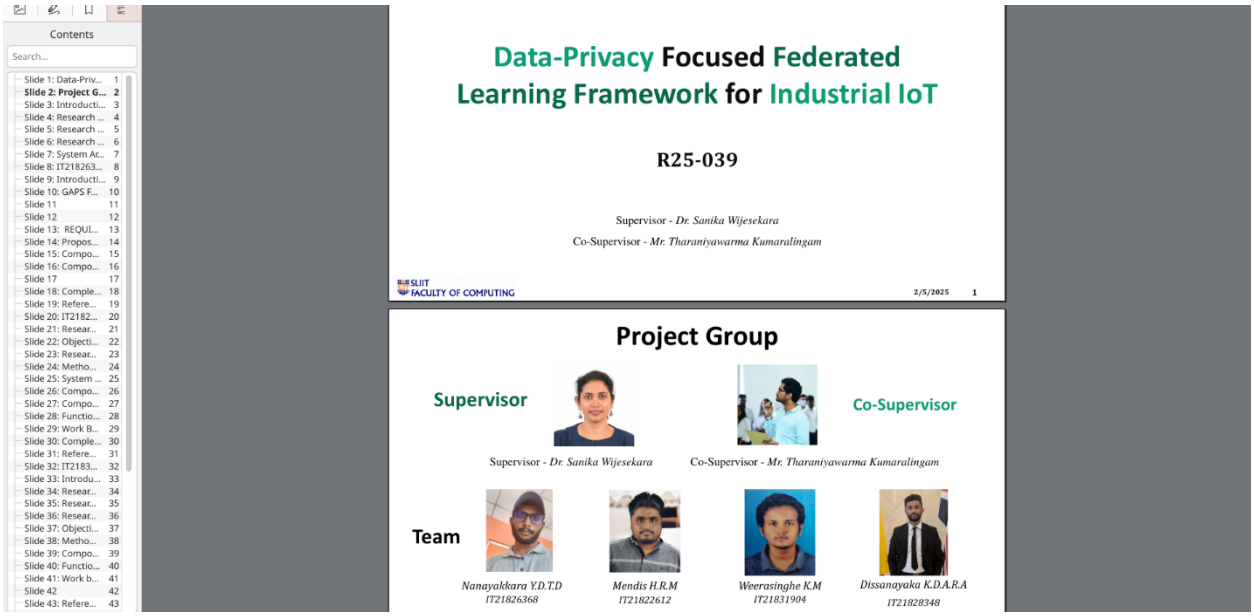

File Edit Selection View Go Run Terminal Help
FLF 2.0
EXPLORER
sss.py
newclients > adrmclient > sam > sss.py
import torch
import numpy as np
import logging
import io
import json
from typing import Dict, Any, List
from collections import defaultdict
class _SecretSharer:
"""
Implements a simple Shamir's Secret Sharing algorithm using numpy.
"""
prime = 104857601 # A large prime for modular arithmetic
@staticmethod
def mod_inverse(a: int, m: int) -> int:
return pow(a, m - 2, m)
@staticmethod
def split_secret(secret: int, k: int, n: int) -> List[tuple[int, int]]:
coeffs = [secret] + [np.random.randint(0, _SecretSharer.prime) for _ in range(k - 1)]
shares = []
for i in range(1, n + 1):
y = sum(c * (i ** j) for j, c in enumerate(coeffs)) % _SecretSharer.prime
shares.append((i, y))
return shares
@staticmethod
def recover_secret(shares: List[tuple[int, int]]) -> int:
if len(shares) < 2:
raise ValueError("At least two shares are required.")
x_coords = [s[0] for s in shares]
y_coords = [s[1] for s in shares]
secret = 0
k = len(shares)
for i in range(k):
numerator, denominator = 1, 1
for j in range(k):
if i != j:
numerator = (numerator * (-x_coords[j])) % _SecretSharer.prime
denominator = (denominator * (x_coords[i] - x_coords[j])) % _SecretSharer.prime

7. GitHub Upload

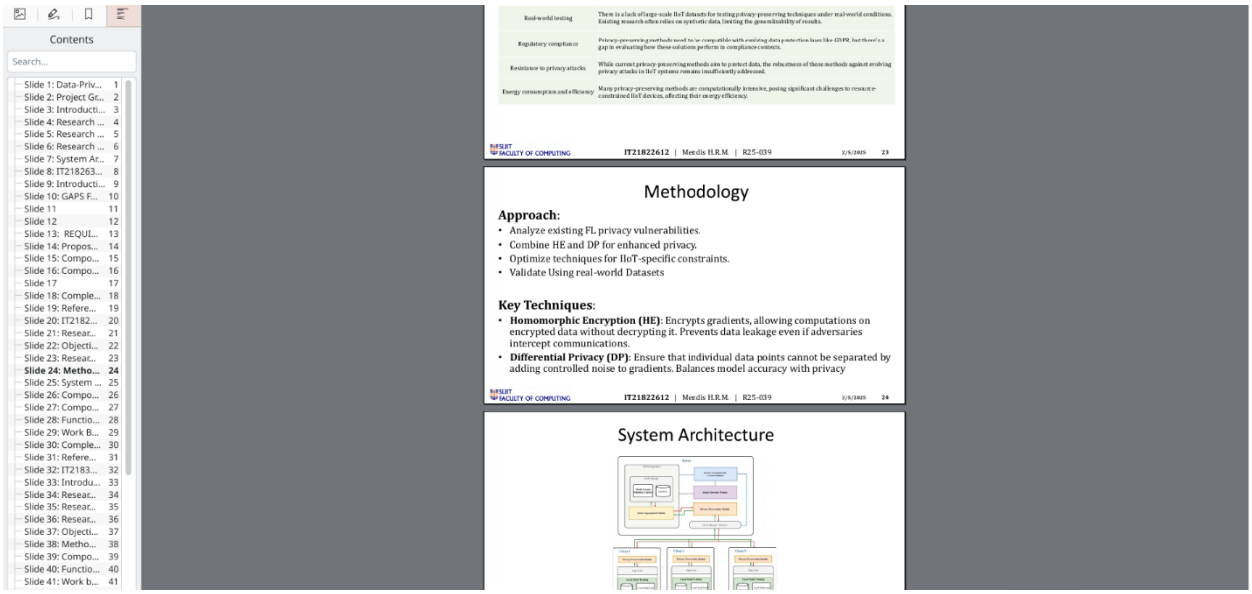


8. Documentation

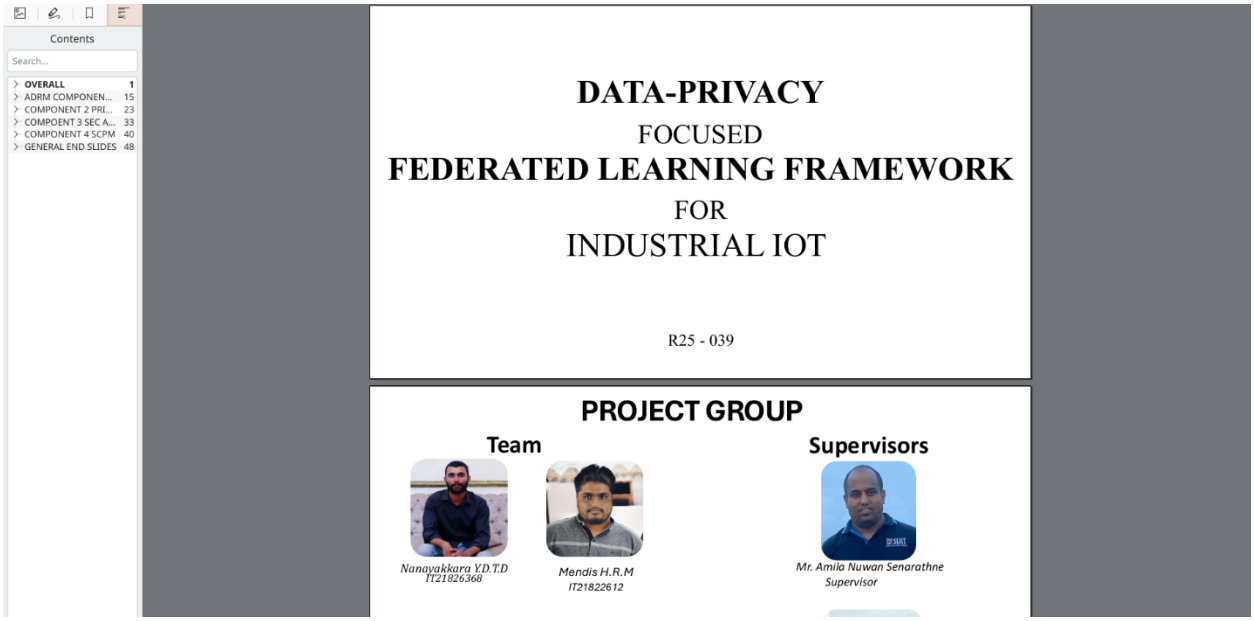
8.1 Proposal



8.2 Presentation 1



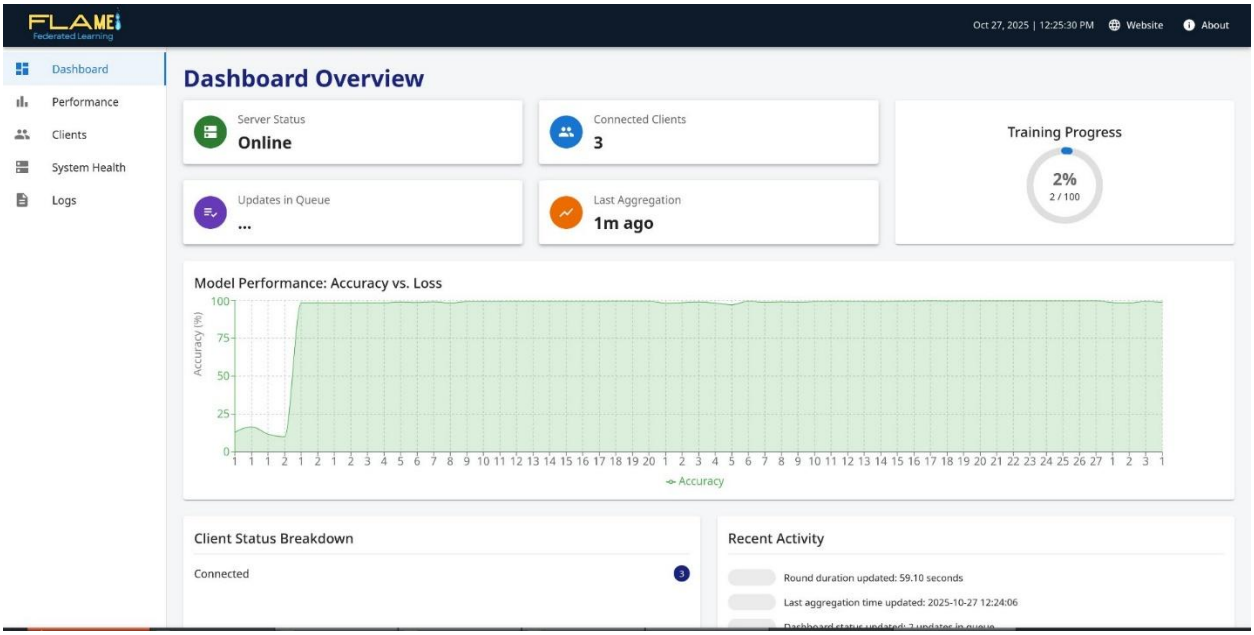
8.3 Presentation 2



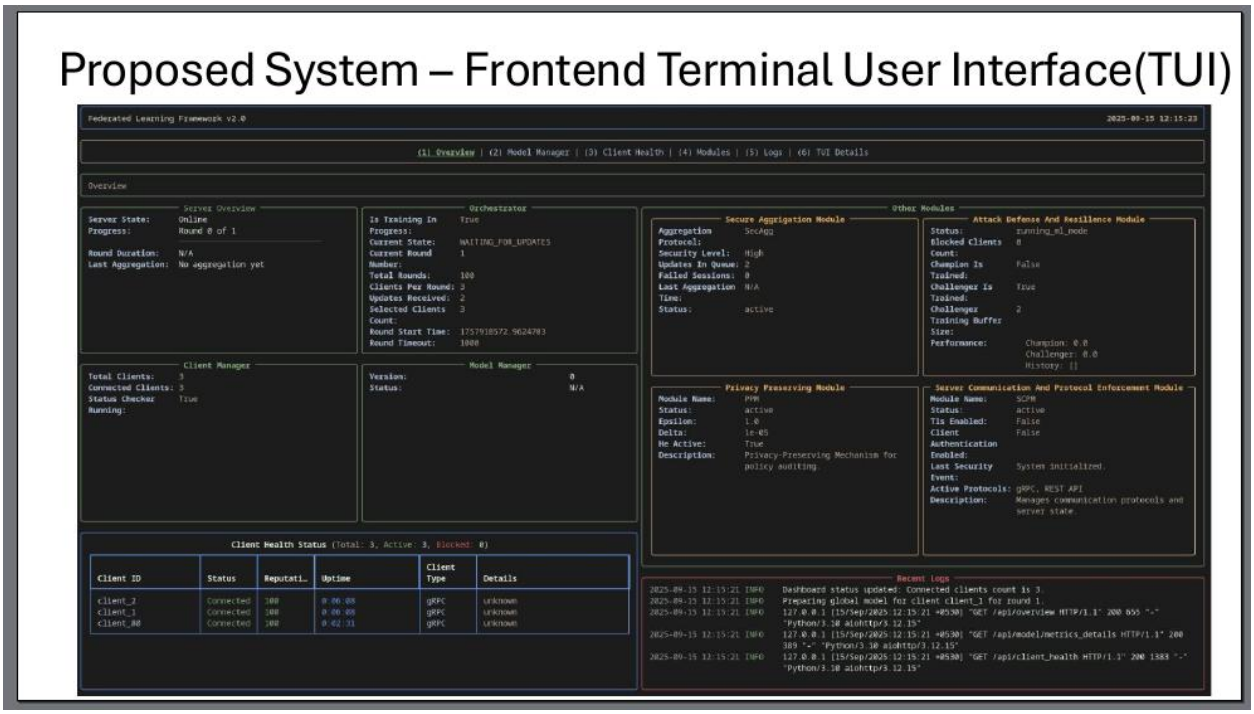
8.4 Final Presentation

8.5 Final Product

Web Portal Frontend



Terminal User interface (Frontend)



9 Research Paper

I. Conference Appetence

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

Acceptance Notification

Dear Tharindu D Nanayakkara,

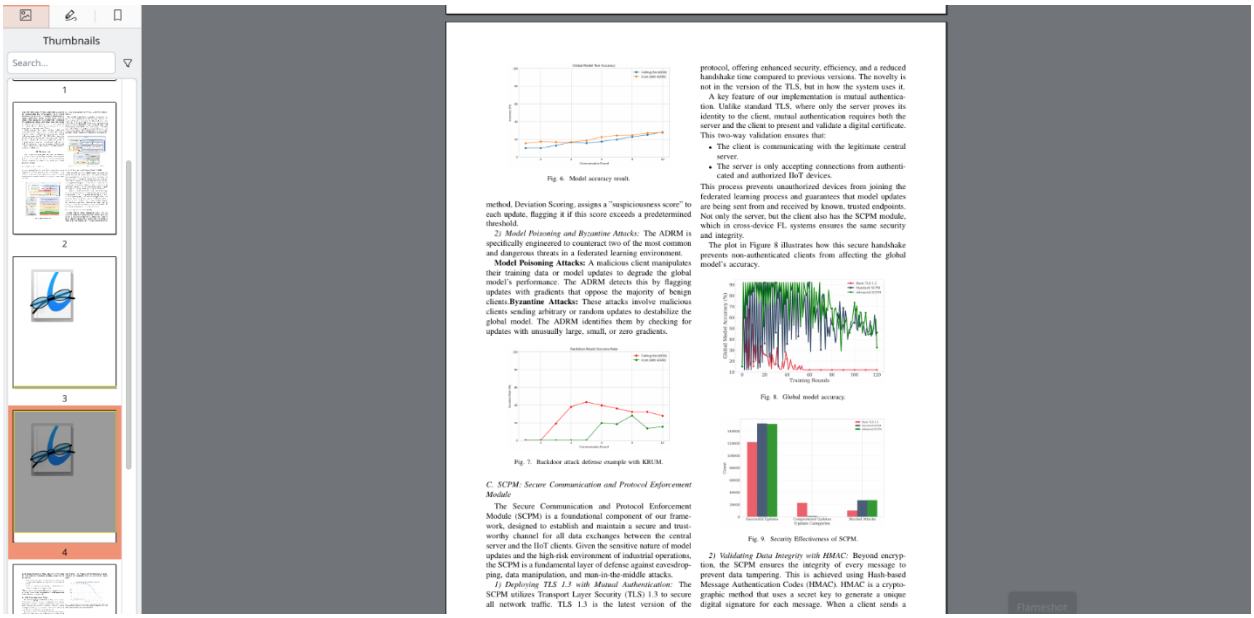
Congratulations! We are pleased to inform you that your paper has been accepted as a regular paper to be presented at the 7th International Conference on Advancements in Computing 2025.

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

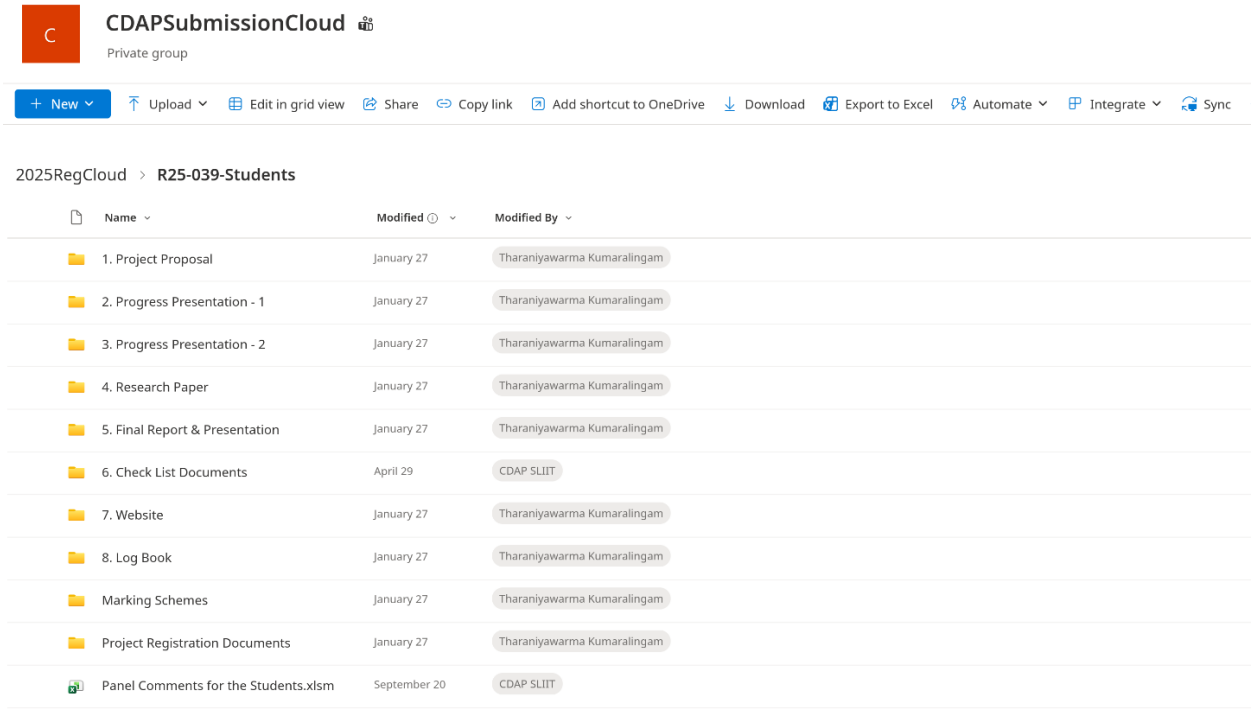
Please visit https://cmt3.research.microsoft.com/7ICAC2025/Submission/Index to view the reviews given during the double-blind review process.

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.

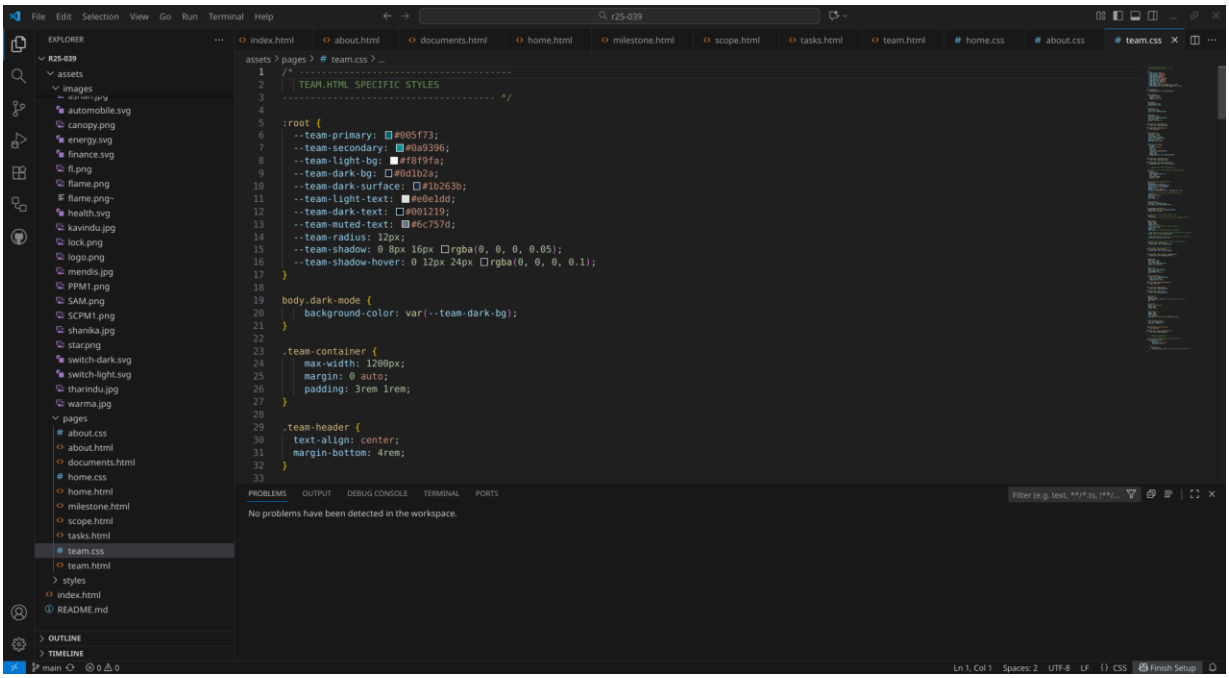


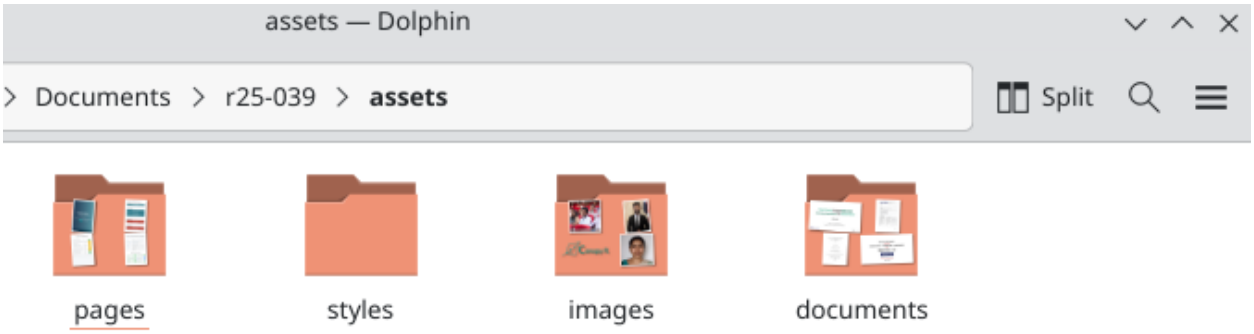
9. CDAP upload

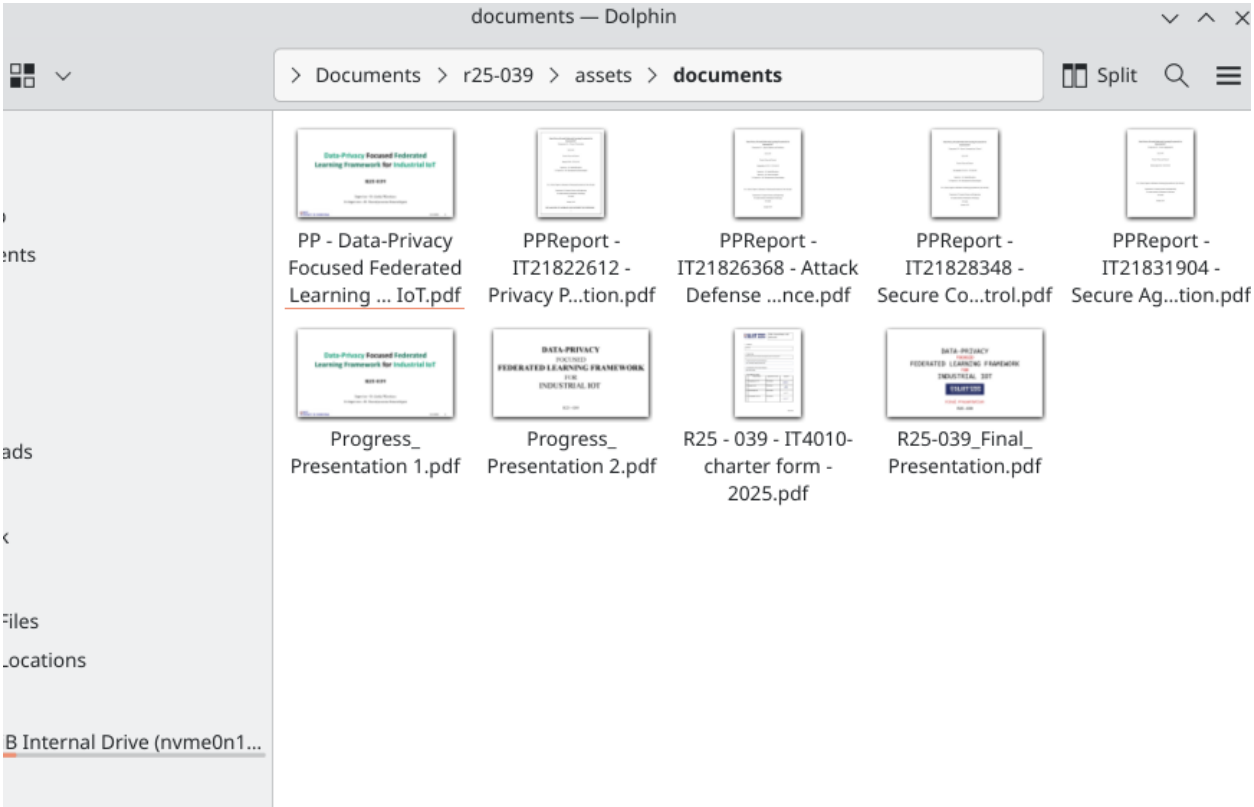


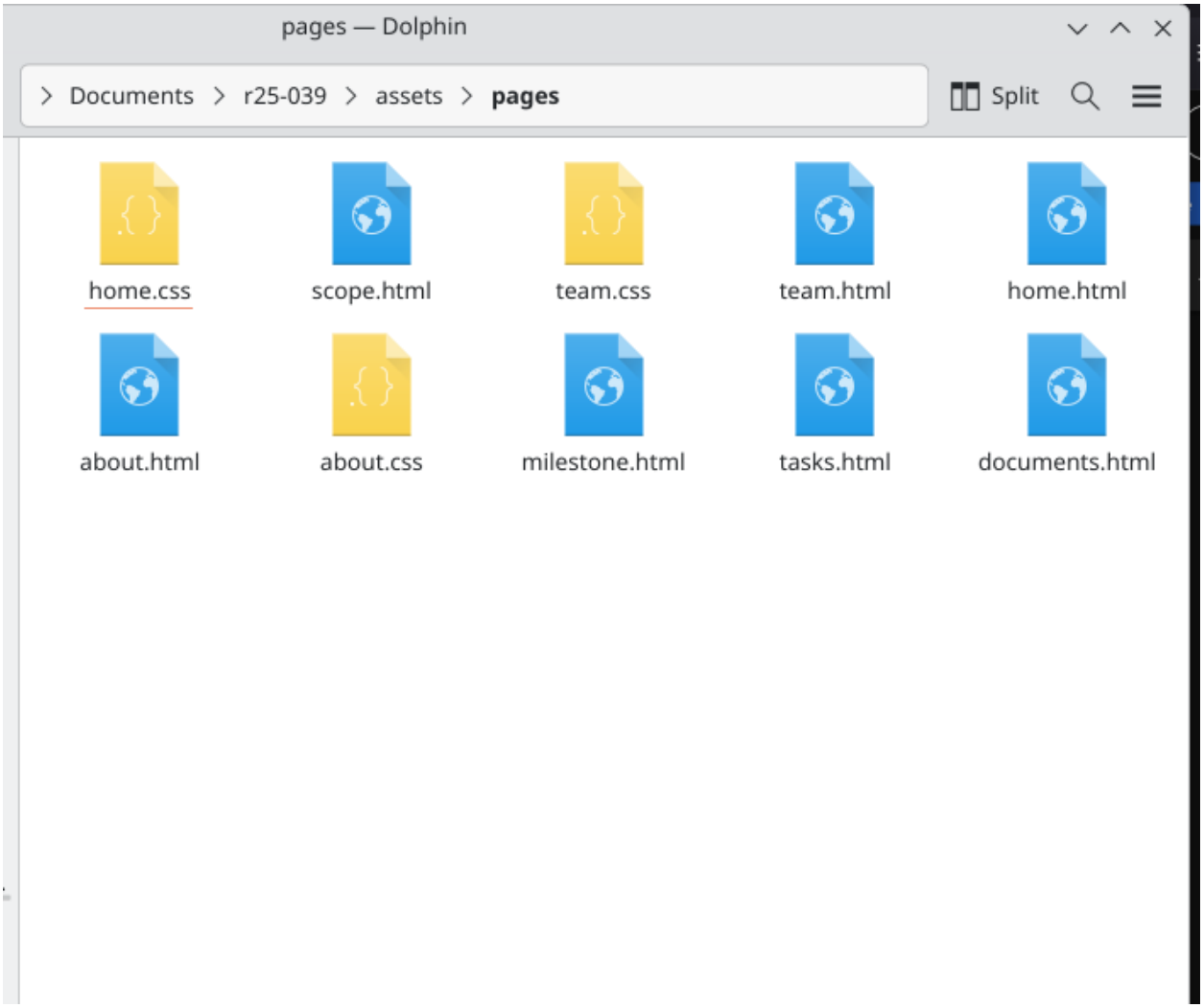
10. Website

10.1 Development

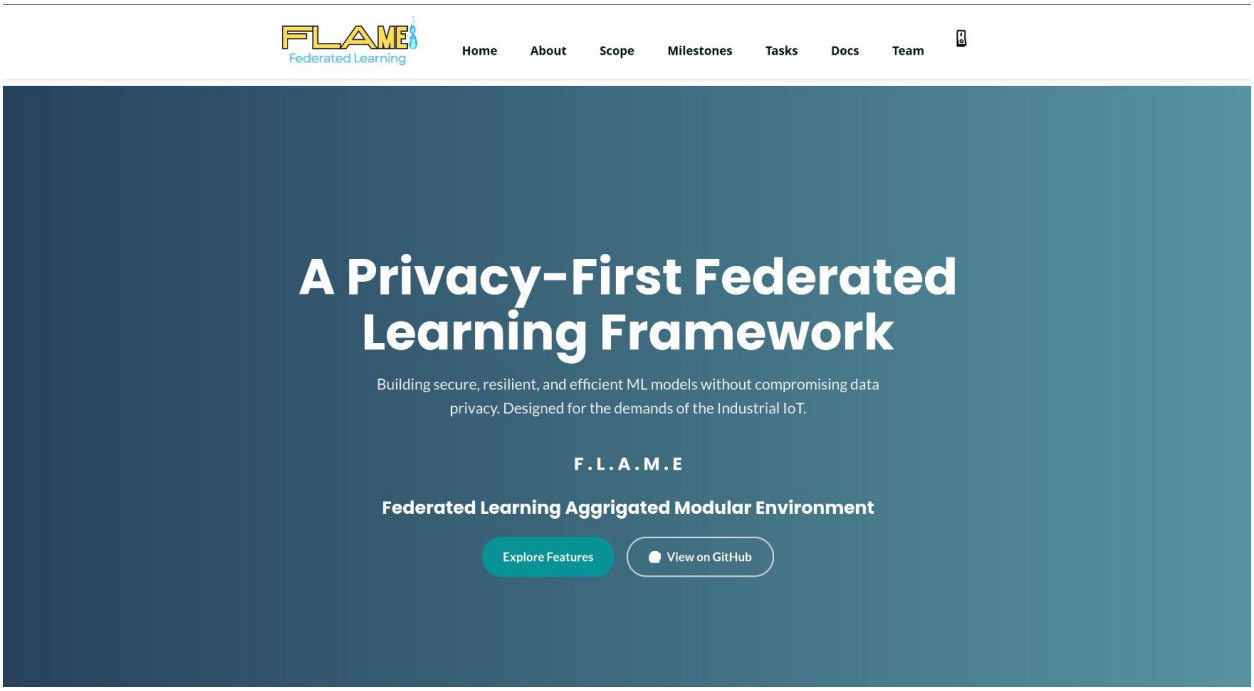



assets — Dolphin
Documents
r25-039
assets
Split
pages
styles
images
documents


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


pages — Dolphin
Documents
r25-039
assets
pages
Split
home.css
scope.html
team.css
team.html
home.html
about.html
about.css
milestone.html
tasks.html
documents.html

10.2 Finalize



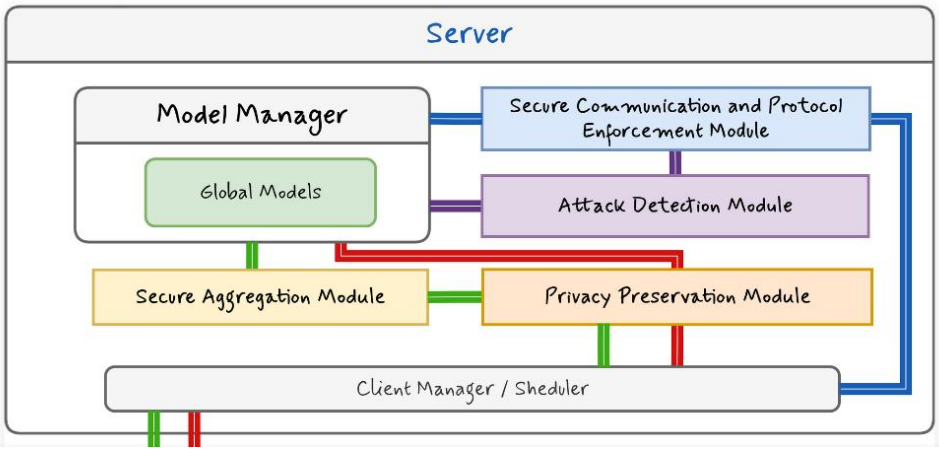
FLAME Federated Learning

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



Mr. Amila Senerathne

Supervisor

Dr. Sanika Wijesekara

External Supervisor

Mr. T. Kumaralingam

Co-Supervisor