

Logbook – Privacy Preservation Module of R25 -039



Project ID: R25 - 039

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

Student Details:	
Names:	Student IDs:
Mendis H.R.M	IT21822612

Supervisor: Mr. Amila Seneratha

Co-Supervisor: Mr. Tharaniyawarma Kumaralingam

Date of Submission: 2025

Contents

1.	Group Details.....	3
2.	Project Details.....	3
3.	Communication Methods	4
4.	Meetings With Supervisors	6
5.	Task Details	7
5.1	Personal task Assigning and Completion	7
6.	System Details	8
6.1	System completion status.....	8
6.2	System Design	9
I.	System Architecture.....	9
II.	Module Architecture	10
6.3	System Testing.....	11
6.4	System Codes.....	12
7.	GitHub Upload	14
8.	Documentation.....	14
8.1	Proposal.....	14
8.2	Presentation 1	15
8.3	Presentation 2.....	15
8.4	Final Presentation.....	16
8.4	Final Product	17
8.5	Research Paper.....	18
I.	Conference Appetence	18
9.	CDAP upload.....	19
10.	Website	20
10.1	Development	20
10.2	Finalize.....	23

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.

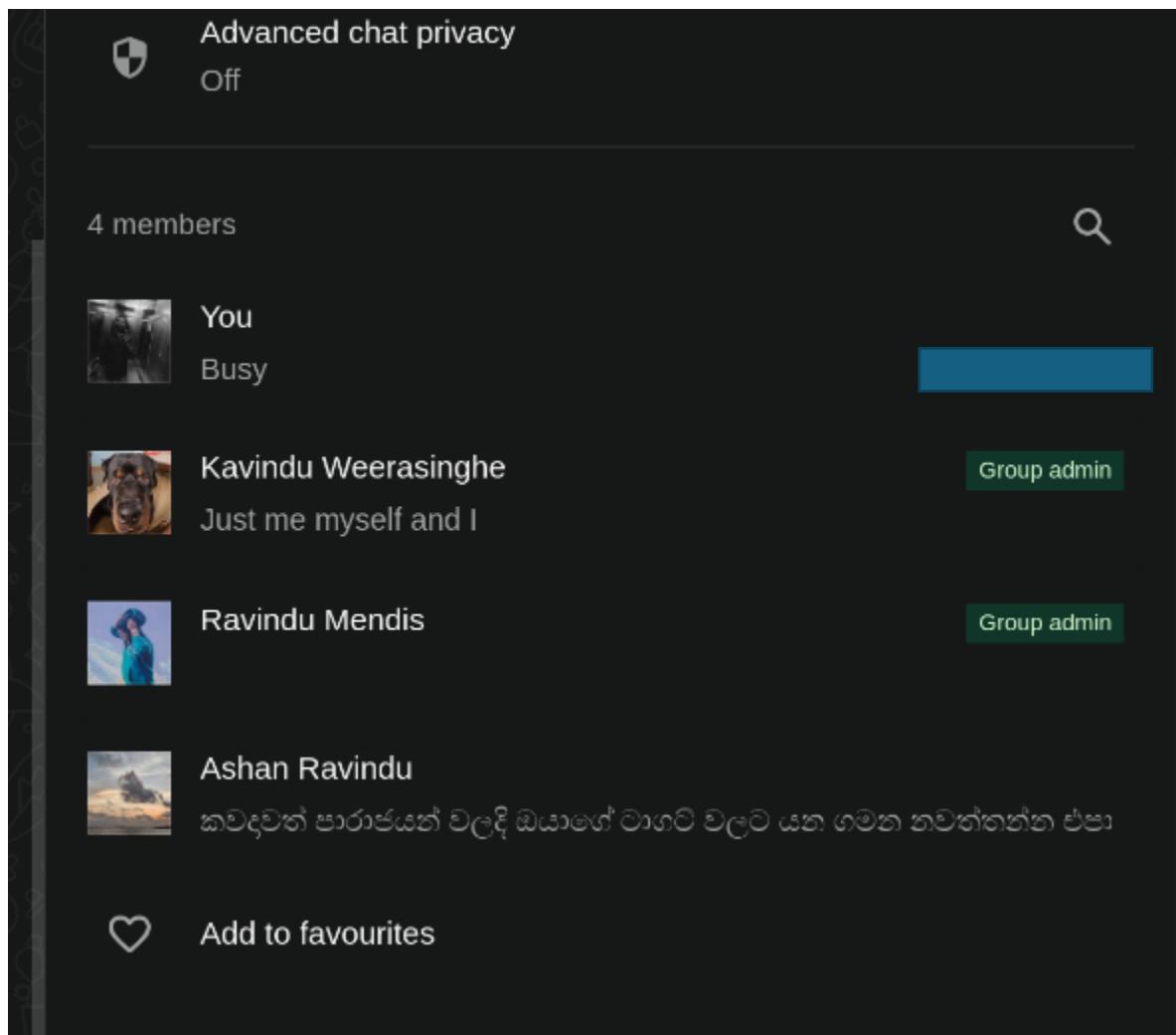
The Challenge: Traditional AI methods require centralizing sensitive factory data, which poses major **privacy risks** and clashes with the distributed nature of industrial operations. Existing FL solutions are insufficient because they fail to simultaneously provide robust security, data privacy, and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

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

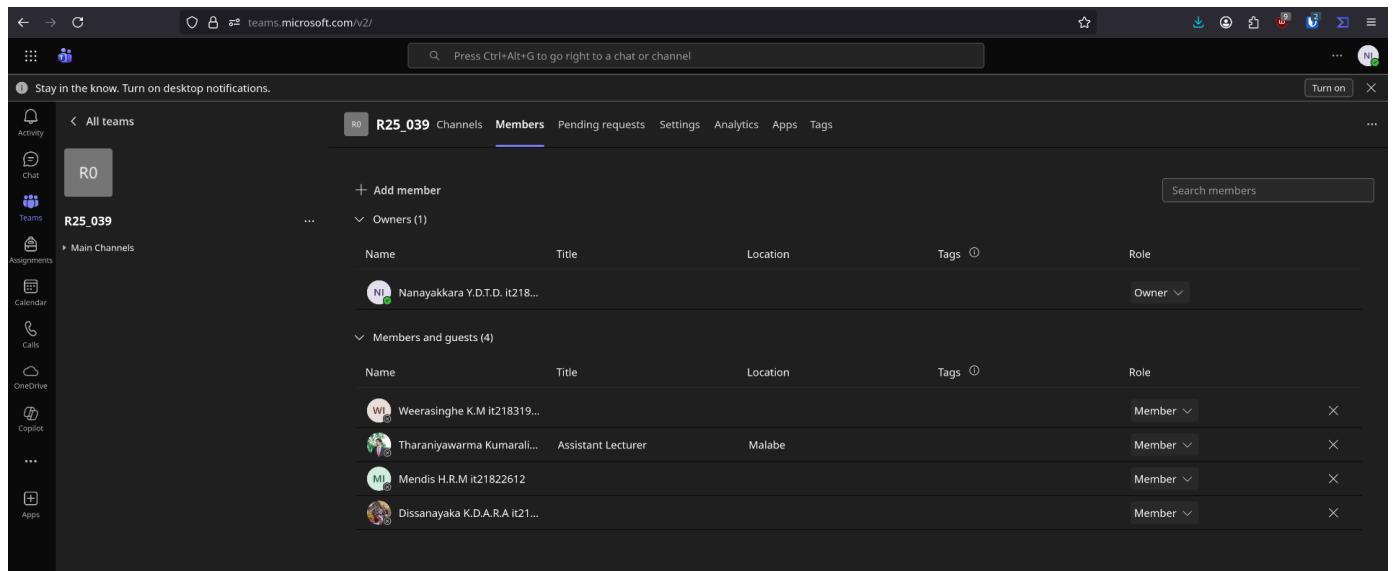
- It uses techniques like **Differential Privacy (DP)** and **Homomorphic Encryption (HE)** to guarantee data confidentiality.
- It implements a robust protocol that uses **client/server validation** to actively block cyber threats such as **Model Poisoning and Byzantine Attacks**.
- The system is optimized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

3. Communication Methods

WhatsApp Group – Team

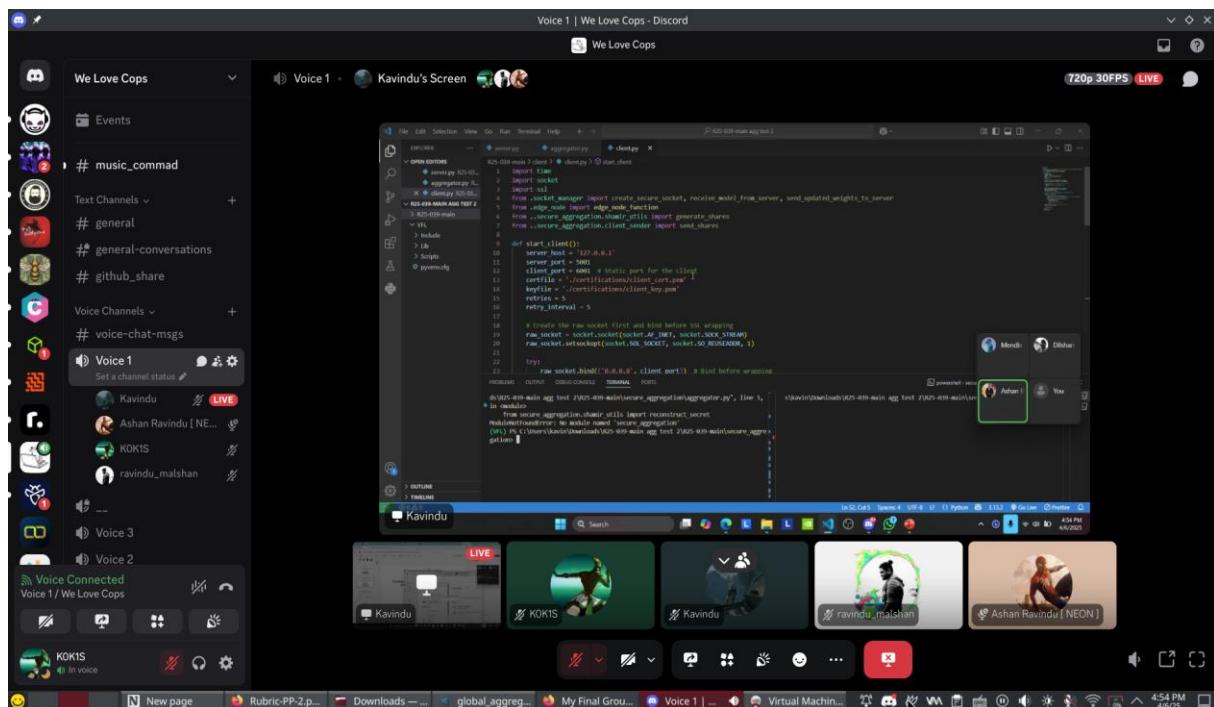


Microsoft Teams - All



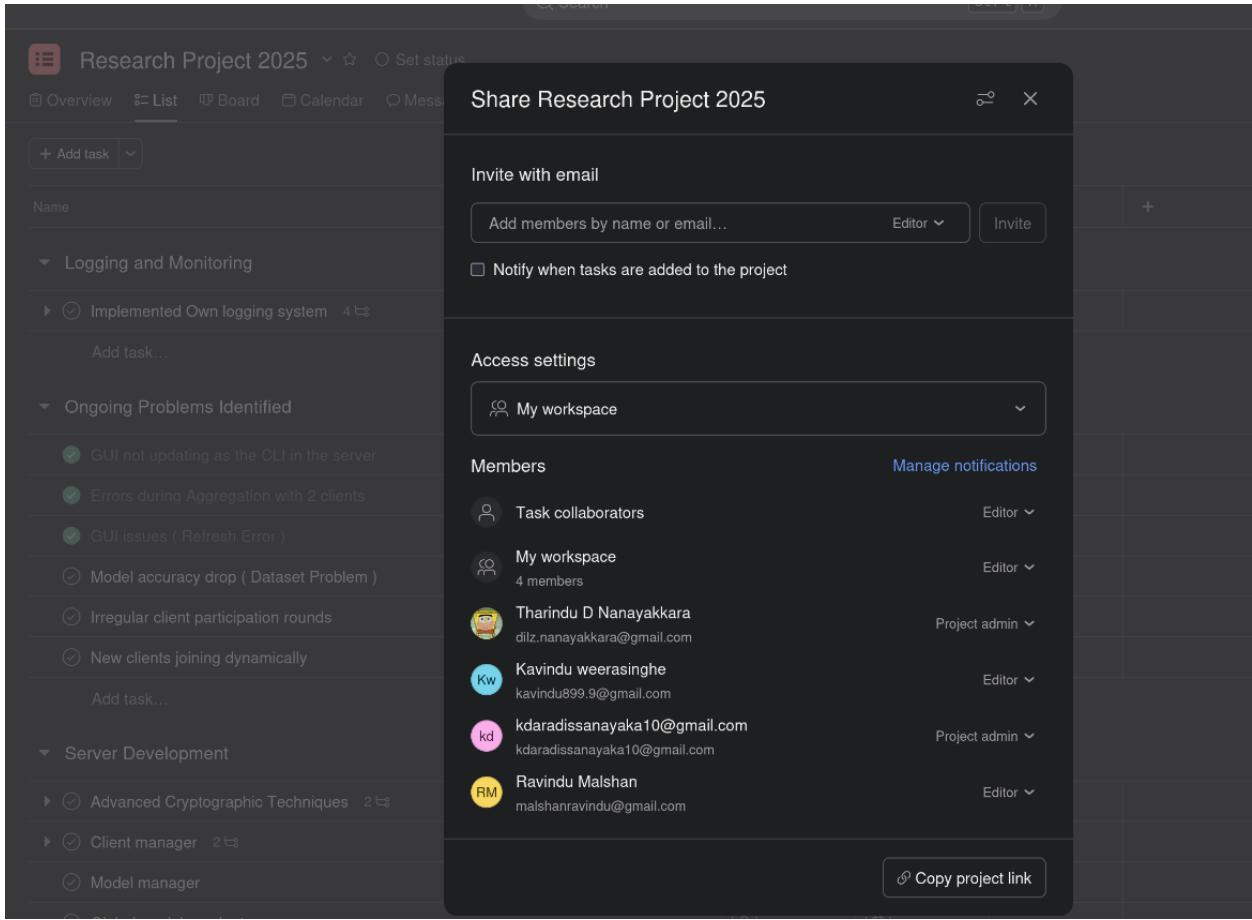
The screenshot shows the Microsoft Teams interface for the 'R25_039' channel. On the left, there's a sidebar with various team-related links like Activity, Chat, Teams, Assignments, Calendar, Calls, OneDrive, Copilot, and Apps. The main area displays the channel members. At the top, there are tabs for Channels, Members (which is selected), Pending requests, Settings, Analytics, Apps, and Tags. Below the tabs, there's a search bar and a 'Members' section. It shows one owner, Nanayakkara Y.D.T.D. it218..., and four members/guests: Weerasinghe K.M it218319..., Tharaniyawarma Kumarali... Assistant Lecturer from Malabe, Mendis H.R.M it21822612, and Dissanayaka K.D.A.R.A it21... . Each member has a role listed as 'Owner'.

Group Meetings – Discord – Team



The screenshot shows a Discord server named 'We Love Cops'. On the left, there's a sidebar with channels like '# music_command', '# general', '# general-conversations', '# github_share', '# voice-chat-msgs', 'Voice 1' (which is live), 'Voice 2', and 'Voice 3'. In the center, there's a video player for 'Kavindu's Screen' and a code editor window titled 'R25-039 MAIN AGG TEST 2'. The code editor contains Python code related to socket aggregation. On the right, there's a preview of the video feed for 'Kavindu' and other users like 'Ashan Ravindu [NEON]' and 'ravindu_malshan'. The bottom of the screen shows the Windows taskbar with various open applications.

Asana – Task Assigning – Team

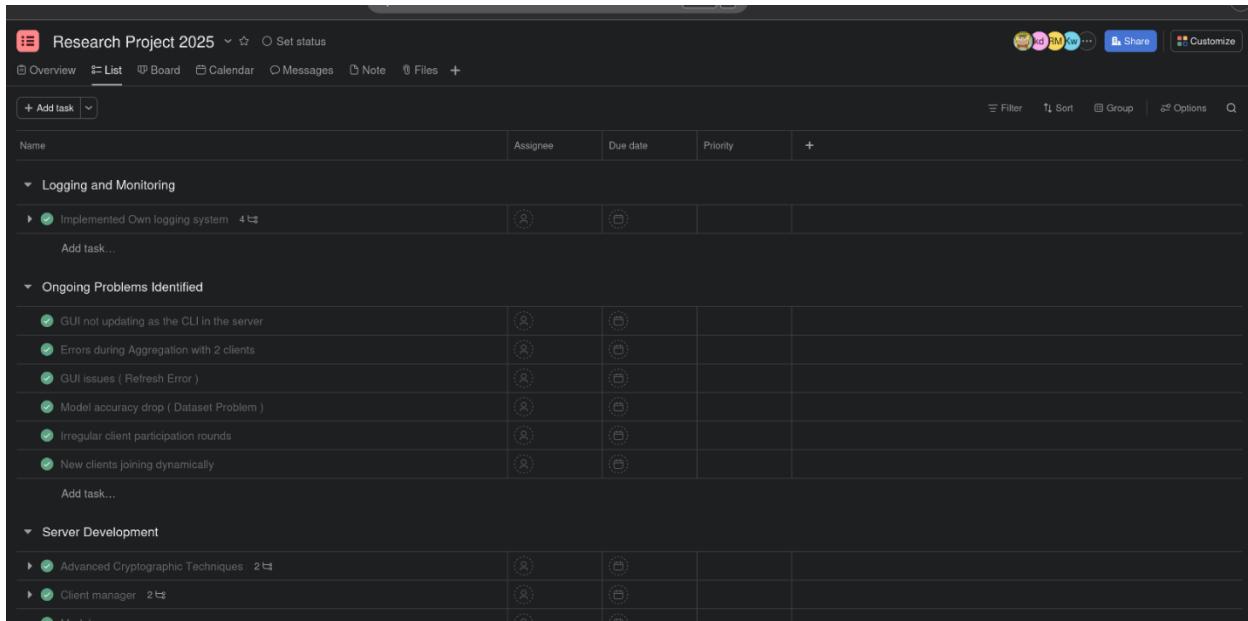


The screenshot shows a project management interface for 'Research Project 2025'. On the left, there's a sidebar with sections like 'Logging and Monitoring', 'Ongoing Problems Identified' (with items like 'GUI not updating as the CLI in the server'), and 'Server Development'. A central area displays a 'Share Research Project 2025' dialog box. This dialog has tabs for 'Invite with email' (containing fields for 'Add members by name or email...' and 'Notify when tasks are added to the project') and 'Access settings' (set to 'My workspace'). Below these are 'Members' and 'Manage notifications' sections. Under 'Members', there are four entries: 'Task collaborators' (Editor), 'My workspace' (Editor, 4 members), 'Tharindu D Nanayakkara' (Project admin, dilz.nanayakkara@gmail.com), 'Kavindu weerasinghe' (Editor, kavindu899.9@gmail.com), 'kdaradissanayaka10@gmail.com' (Project admin, kdaradissanayaka10@gmail.com), and 'Ravindu Malshan' (Editor, malshanravindu@gmail.com). At the bottom right of the dialog is a 'Copy project link' button.

4. Meetings With Supervisors

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

5. Task Details



The screenshot shows a task management interface for a project titled "Research Project 2025". The interface includes a header with user icons and navigation links for Overview, List, Board, Calendar, Messages, Note, Files, and a "+" button. Below the header is a search bar and filter options. The main area displays a table with columns for Name, Assignee, Due date, Priority, and actions. Tasks are categorized under sections like "Logging and Monitoring", "Ongoing Problems Identified", and "Server Development". Each task has a status icon (green checkmark), a title, and a due date.

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

Privacy Preservation Module was assigned.

5.1 Personal task Assigning and Completion



The screenshot shows a task list for the "Privacy Preservation Module (PPM)". The tasks are listed in a table with columns for the task title and assignee. All tasks are assigned to "RM Ravindu Ma...".

Add task...	
Privacy Preservation Module (PPM)	
Differential Privacy values reported (ϵ, δ).	(RM Ravindu Ma...)
Homomorphic Encryption functionality demonstrated.	(RM Ravindu Ma...)
Accuracy comparison: With vs. Without privacy methods.	(RM Ravindu Ma...)
Convergence curve plots included.	(RM Ravindu Ma...)
Memory & time benchmarks of hybrid DP+HE scheme.	(RM Ravindu Ma...)
Communication overhead metrics.	(RM Ravindu Ma...)
graph or table showing privacy utility trade off	(RM Ravindu Ma...)

6. System Details

6.1 System completion status

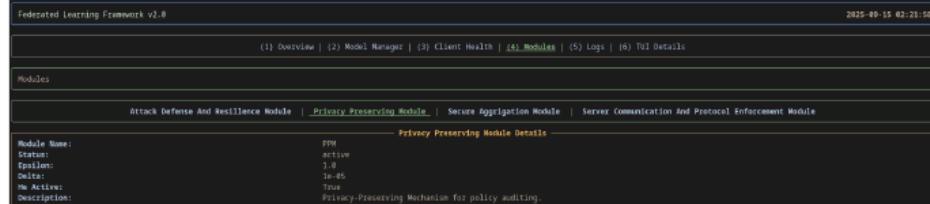
Finished

PPM TUI

```

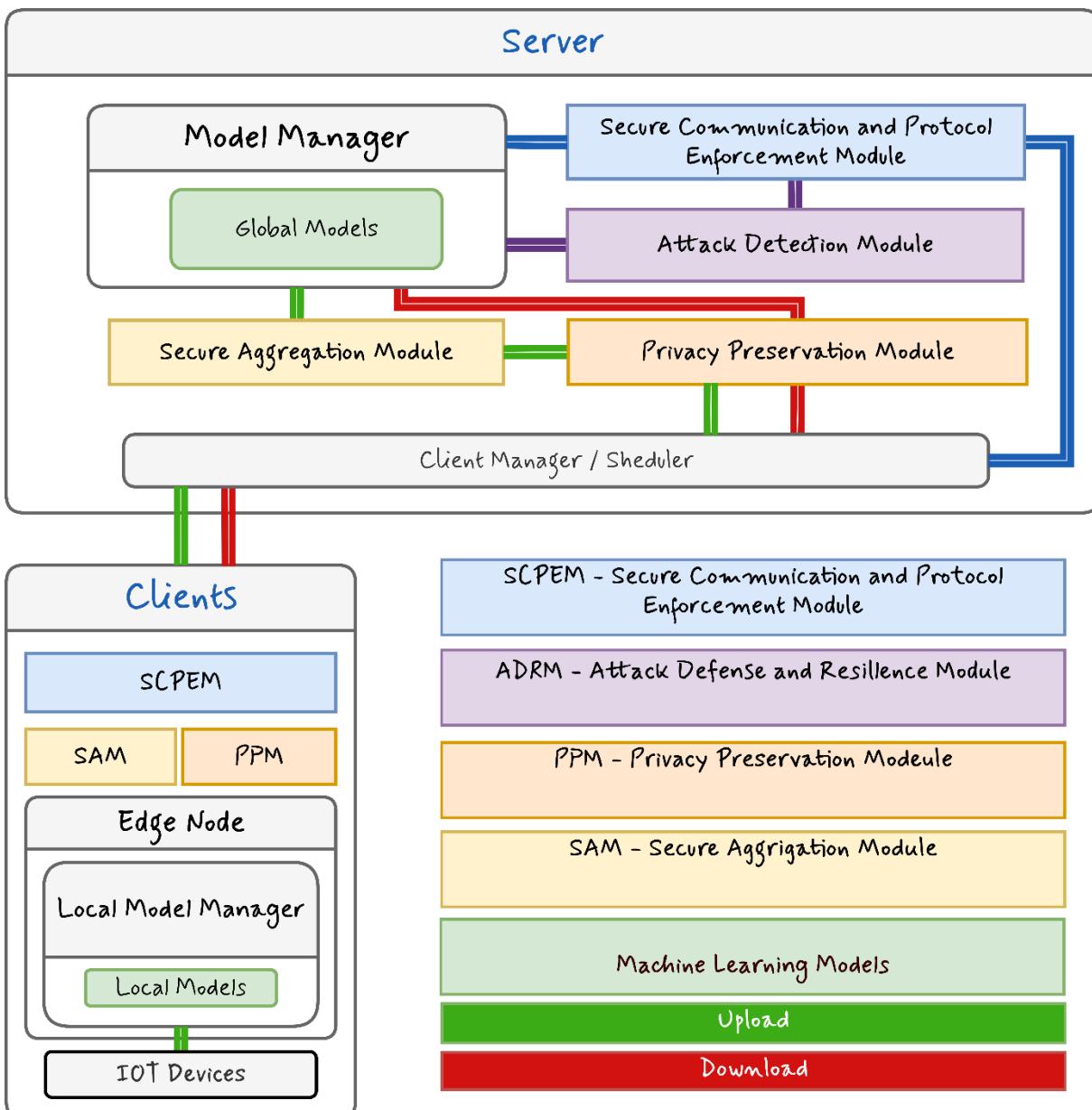
2025-04-07 08:54:03,110 - [DP INIT] Noise Multiplier set to 6.0
Connected to server at 127.0.0.1:5081 from static port 6881.
2025-04-07 08:54:15,729 - INFO - Waiting to receive initial model from the server.
2025-04-07 08:54:15,730 - INFO - Expected 679665 bytes of model data.
2025-04-07 08:54:15,730 - INFO - Successfully received 679665 bytes of model data.
2025-04-07 08:54:15,730 - INFO - [RECEIVE] Received initialized model weights (bytes)
2025-04-07 08:54:15,730 - DEBUG - [MODEL] Loading data and starting training
2025-04-07 08:54:15,730 - DEBUG - [MODEL] Creating new model instance
[venv] PS C:\Users\User\Videos\FL_DP_Tabular> python main.py --mode FL
*** Running mode: FL ***
Round 1/10 | Mode: DPHE | Acc: 75.42% | Comm: 2156000 bytes
Round 2/10 | Mode: DPHE | Acc: 75.82% | Comm: 2156000 bytes
Round 3/10 | Mode: DPHE | Acc: 75.24% | Comm: 2156000 bytes
Round 4/10 | Mode: DPHE | Acc: 75.43% | Comm: 2156000 bytes
Round 5/10 | Mode: DPHE | Acc: 75.23% | Comm: 2156000 bytes
Round 6/10 | Mode: DPHE | Acc: 75.43% | Comm: 2156000 bytes
Round 7/10 | Mode: DPHE | Acc: 75.25% | Comm: 2156000 bytes
Round 8/10 | Mode: DPHE | Acc: 75.40% | Comm: 2156000 bytes
Round 9/10 | Mode: DPHE | Acc: 75.64% | Comm: 2156000 bytes
Round 10/10 | Mode: DPHE | Acc: 75.43% | Comm: 2156000 bytes
[venv] PS C:\Users\User\Videos\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:98
n it allows for much faster training performance, but remember to turn it on and retrain one last
warning, warn()
C:\Users\User\Videos\FL_DP_Tabular\FL_DP_Tabular\venv\lib\site-packages\torch\nn\Module.html:torch_
loss.backward()
Round 1/10 | Mode: DP | Acc: 24.12% | Comm: 2156000 bytes
Round 2/10 | Mode: DP | Acc: 76.65% | Comm: 2156000 bytes
Round 3/10 | Mode: DP | Acc: 24.12% | Comm: 2156000 bytes
Round 4/10 | Mode: DP | Acc: 75.91% | Comm: 2156000 bytes
Round 5/10 | Mode: DP | Acc: 75.02% | Comm: 2156000 bytes
Round 6/10 | Mode: DP | Acc: 76.41% | Comm: 2156000 bytes
Round 7/10 | Mode: DP | Acc: 76.41% | Comm: 2156000 bytes
Round 8/10 | Mode: DP | Acc: 76.40% | Comm: 2156000 bytes
Round 9/10 | Mode: DP | Acc: 76.20% | Comm: 2156000 bytes
Round 10/10 | Mode: DP | Acc: 76.37% | Comm: 2156000 bytes
[venv] PS C:\Users\User\Videos\FL_DP_Tabular> python main.py --mode DPHE

```

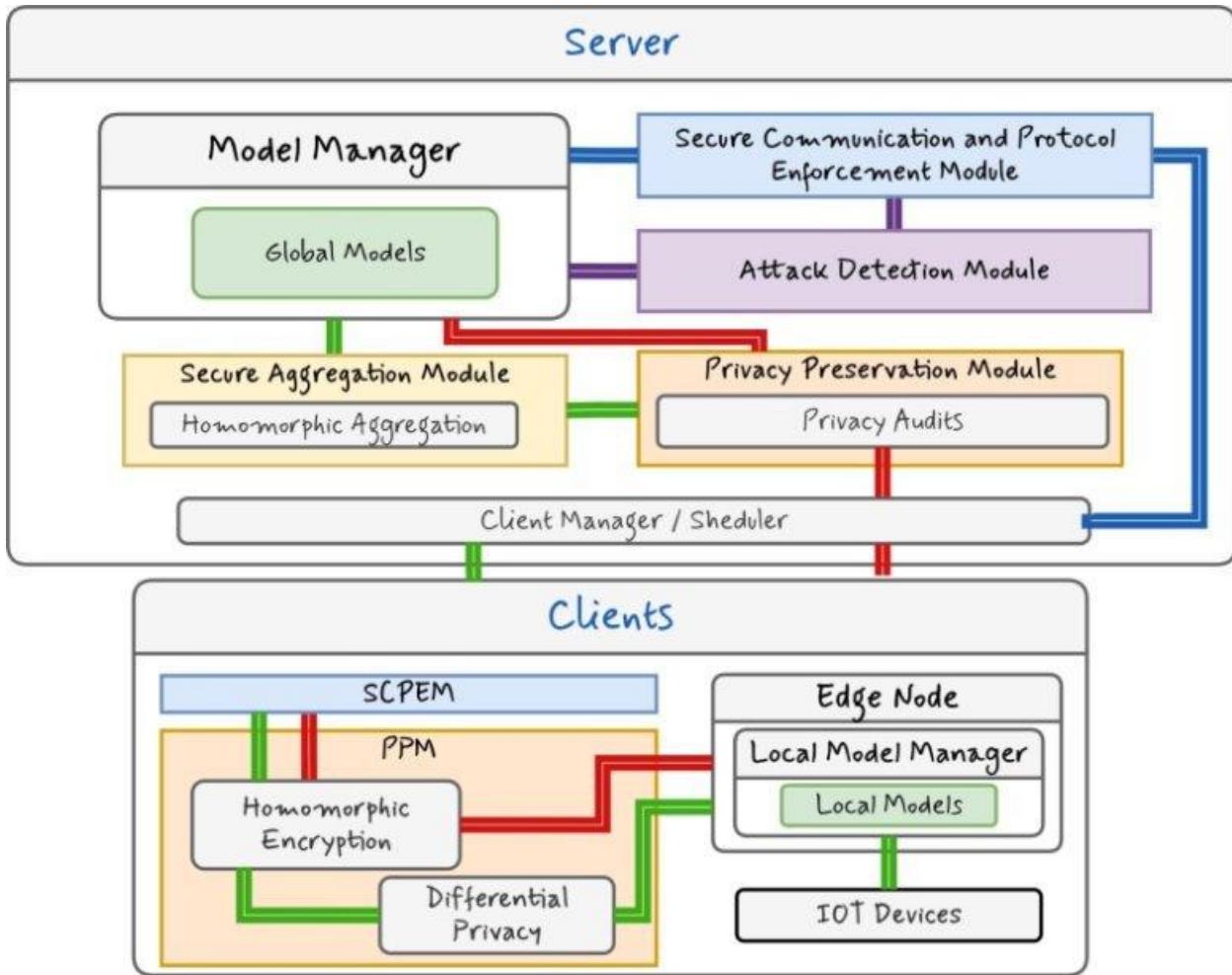


6.2 System Design

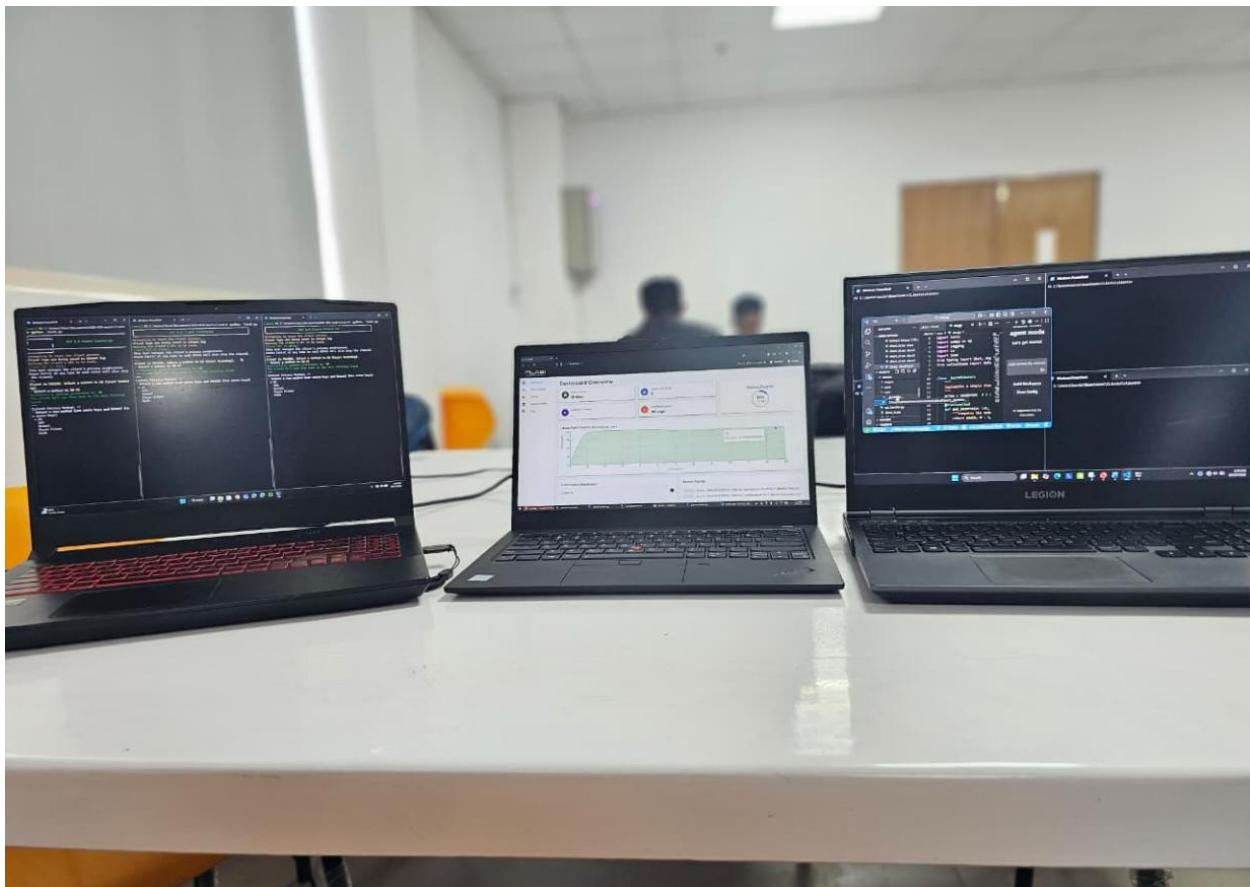
I. System Architecture



II. Module Architecture



6.3 System Testing



6.4 System Codes

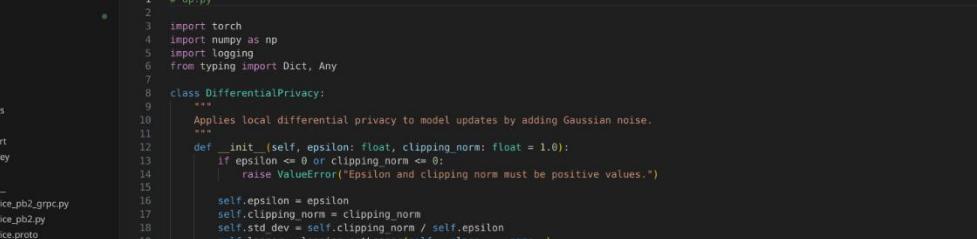
PPM – Server

```
File Edit Selection View Go Run Terminal Help ← → FLF 2.0 EXPLORER ppm.py server > ppm > ppm.py 1 # server/ppm/ppm.py 2 3 import logging 4 from typing import Dict, Any 5 6 from log_manager.log_manager import ContextAdapter 7 8 9 class PPM: 10     """ 11         Privacy-Preserving Mechanism (PPM) for Federated learning. 12         This class is responsible for auditing privacy protocols and guiding the 13         server's aggregation strategy based on policy, not for adding noise itself. 14     """ 15 16     def __init__(self, cfg: Dict[str, Any]): 17         """ 18             Initializes the PPM with configuration parameters for both DP and HE. 19         """ 20         Args: 21             cfg (Dict[str, Any]): The configuration dictionary, expected to contain 22                 'privacy' sub-keys for 'dp' and 'he'. 23         """ 24         # Load DP parameters from config, with safe fallbacks 25         dp_cfg = cfg.get("privacy", {}).get("dp", {}) 26         self.epsilon = dp_cfg.get("epsilon", 1.0) 27         self.delta = dp_cfg.get("delta", 1e-5) 28 29         # Load HE parameters from config 30         he_cfg = cfg.get("privacy", {}).get("he", {}) 31         self.he_active = he_cfg.get("active", False) 32 33         self.logger = logging.getLogger(self.__class__.__name__) 34         self.logger = ContextAdapter(self.logger, {"component": self.__class__.__name__}) 35         self.logger.info( 36             f"PPM initialized. DP: (epsilon={self.epsilon}, delta={self.delta}). " 37             f"HE active: {self.he_active}" 38         ) 39 40     def check_aggregation_policy(self) -> bool: 41         """ 42             Performs a privacy audit to determine if homomorphic aggregation should be used. 43             The policy checks if Homomorphic Encryption is active. 44         """ 45 46         Returns: 47             bool: True if the policy allows for homomorphic aggregation, False otherwise. 48         """
```

Homomorphic Aggregation

PPM – Clients

Differential Privacy



```
File Edit Selection View Go Run Terminal Help ⏪ ⏩ 🔍 FLF 2.0 EXPLORER ... dp.py x newclients > _pycache_ > vscode > FL > admclient > _pycache_ > cspn > certifications > ca.crt > client_79.crt > client_79.key > protos > _pycache_ > client_service_pb2_grpc.py > client_service_pb2.py > client_service.proto > cspn.py > data > ppm > _pycache_ dp.py he.py sam apihandler.py client_id.txt client.py dash.py model_manager.py admclient2 client _pycache_ cspn data ppm sam apihandler.py client_id.txt client.log
```

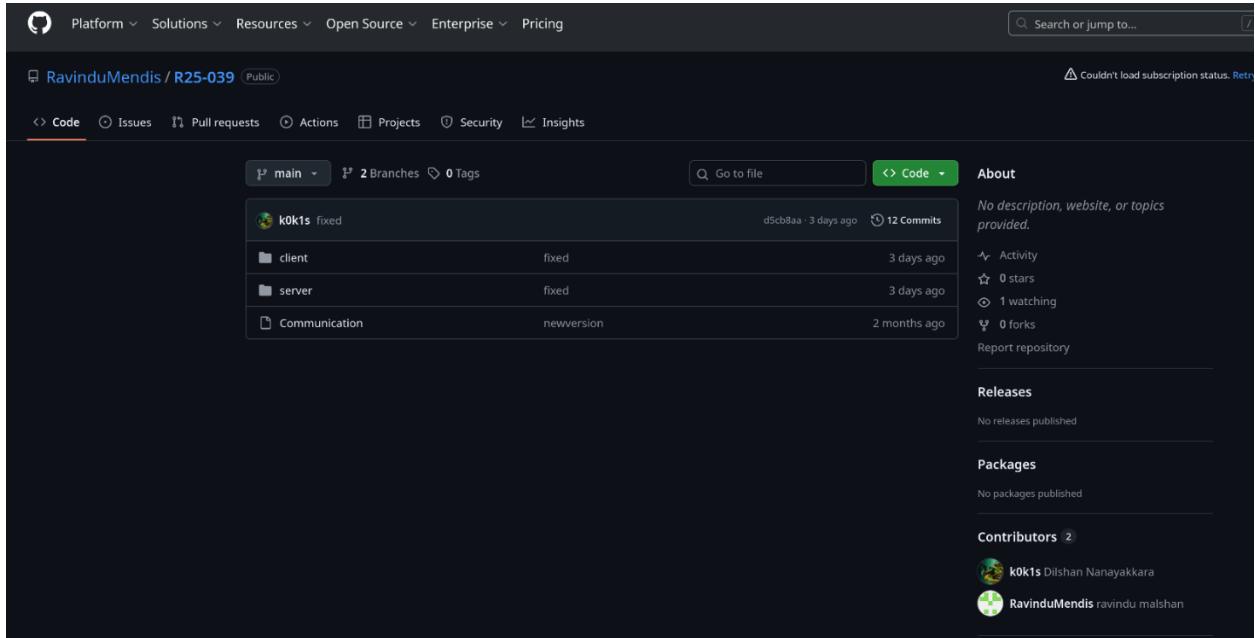
```
newclients > admclient > ppm > dp.py
1 # dp.py
2
3 import torch
4 import numpy as np
5 import logging
6 from typing import Dict, Any
7
8 class DifferentialPrivacy:
9     """
10         Applies local differential privacy to model updates by adding Gaussian noise.
11     """
12     def __init__(self, epsilon: float, clipping_norm: float = 1.0):
13         if epsilon <= 0 or clipping_norm <= 0:
14             raise ValueError("Epsilon and clipping norm must be positive values.")
15
16         self.epsilon = epsilon
17         self.clipping_norm = clipping_norm
18         self.std_dev = self.clipping_norm / self.epsilon
19         self.logger = logging.getLogger(self.__class__.__name__)
20         self.logger.info(f"DifferentialPrivacy initialized with epsilon={self.epsilon}, clipping_norm={self.clipping_norm}, std_dev={self.std_dev:.4f}")
21
22     def add_noise(self, state_dict: Dict[str, Any]) -> Dict[str, Any]:
23         """
24             Clips the norm of the entire model update and then adds Gaussian noise
25             to each parameter.
26         """
27         self.logger.info("Applying differential privacy: Clipping and adding Gaussian noise.")
28
29         # 1. Flatten all parameters into a single vector to calculate the L2 norm
30         flat_params = torch.cat([p.flatten() for p in state_dict.values()])
31         total_norm = torch.linalg.norm(flat_params)
32
33         # 2. Calculate the clipping factor to scale the update if its norm exceeds the threshold
34         clip_factor = min(1.0, self.clipping_norm / (total_norm + 1e-6))
35
36         self.logger.info(f"Update norm: {total_norm:.4f}, clipping factor: {clip_factor:.4f}")
37
38         noisy_state_dict = {}
39         for key, param in state_dict.items():
40             # 3. Apply the clipping factor to each parameter
41             clipped_param = param * clip_factor
42
43             # 4. Add Gaussian noise scaled to the clipping norm
44             noise = torch.randn_like(clipped_param) * self.std_dev
```

Homomorphic Encryption

```
File Edit Selection View Go Run Terminal Help ← → FLF 2.0 08 09

EXPLORER he.py x
newclients > admclient > ppm > he.py
1 # he.py
2
3 import torch
4 import logging
5 import io
6 from typing import Dict, Any
7
8 class HomomorphicEncryption:
9     """
10         A placeholder class for Homomorphic Encryption (HE).
11         This mock version serializes/deserializes PyTorch state dictionaries
12         to and from byte streams, simulating the process.
13     """
14     def __init__(self):
15         self.logger = logging.getLogger(self.__class__.__name__)
16         self.logger.info("HomomorphicEncryption module initialized.")
17
18     def encrypt_model_state(self, state_dict: Dict[str, Any]) -> bytes:
19         """
20             Mocks the encryption of a model state dictionary.
21         """
22         self.logger.info("Encrypting model state with Homomorphic Encryption.")
23         buffer = io.BytesIO()
24         torch.save(state_dict, buffer)
25         encrypted_bytes = buffer.getvalue()
26
27         self.logger.info("Model state encrypted. Sending to server.")
28         return encrypted_bytes
29
30     def decrypt_model_state(self, encrypted_bytes: bytes) -> Dict[str, Any]:
31         """
32             Mocks the decryption of an encrypted model state.
33         """
34         self.logger.info("Decrypting model state from server.")
35
36         buffer = io.BytesIO(encrypted_bytes)
37         state_dict = torch.load(buffer, map_location='cpu')
38
39         self.logger.info("Model state decrypted successfully.")
40         return state_dict
```

7. GitHub Upload



8. Documentation

8.1 Proposal



Slide Number	Content
1	Slide 1: Data-Priv...
2	Slides 2: Project ...
3	Slide 3: Introduc...
4	Slide 4: Research ...
5	Slide 5: Research ...
6	Slide 6: Research ...
7	Slide 7: System Ar...
8	Slide 8: IT218263...
9	Slide 9: Introduc...
10	Slide 10: GAPS ...
11	Slide 11
12	Slide 12
13	Slide 13: REQU...
14	Slide 14: Propos...
15	Slide 15: Compo...
16	Slide 16: Compo...
17	Slide 17
18	Slide 18: Comple...
19	Slide 19: Refere...
20	Slide 20: IT2182...
21	Slide 21: Resear...
22	Slide 22: Objecti...
23	Slide 23: Resear...
24	Slide 24: Metho...
25	Slide 25: System ...
26	Slide 26: Compo...
27	Slide 27: Compari...
28	Slide 28: Compari...
29	Slide 29: Work B...
30	Slide 30: Comple...
31	Slide 31: Refere...
32	Slide 32: IT2183...
33	Slide 33: Introdu...
34	Slide 34: Resear...
35	Slide 35: Resear...
36	Slide 36: Resear...
37	Slide 37: Refere...
38	Slide 38: Metho...
39	Slide 39: Compo...
40	Slide 40: Function...
41	Slide 41: Work b...
42	Slide 42
43	Slide 43: Refere...

8.2 Presentation 1

Contents

Search...

- Slide 1: Data-Priv... 1
- Slide 2: Project G... 2
- Slide 3: Introduc... 3
- Slide 4: Resear... 4
- Slide 5: Research ... 5
- Slide 6: Research ... 6
- Slide 7: System Ar... 7
- Slide 8: IT218263... 8
- Slide 9: Introduc... 9
- Slide 10: GAPS F... 10
- Slide 11 11
- Slide 12 12
- Slide 13: REQUIS... 13
- Slide 14: Propos... 14
- Slide 15: Compo... 15
- Slide 16: Compo... 16
- Slide 17 17
- Slide 18: Comple... 18
- Slide 19: Refere... 19
- Slide 20: IT2182... 20
- Slide 21: Compo... 21
- Slide 22: Objecti... 22
- Slide 23: Resear... 23
- Slide 24: Metho... 24**
- Slide 25: System ... 25
- Slide 26: Compo... 26
- Slide 27: Compo... 27
- Slide 28: Functio... 28
- Slide 29: Visual B... 29
- Slide 30: Compon... 30
- Slide 31: Refere... 31
- Slide 32: IT2183... 32
- Slide 33: Introduc... 33
- Slide 34: Resear... 34
- Slide 35: Resear... 35
- Slide 36: Resear... 36
- Slide 37: Objecti... 37
- Slide 38: Compon... 38
- Slide 39: Compo... 39
- Slide 40: Function... 40
- Slide 41: Work b... 41

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 compliant with existing data protection laws like GDPR, but there's a lack of specific guidelines for IIoT systems.

Resistance to privacy attacks While current privacy-preserving methods are in place, 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.

IT21822612 | Mendis H.R.M. | R25-039 23

Methodology

Approach:

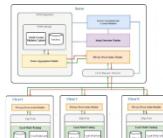
- Analyze existing FL privacy vulnerabilities.
- Combine HE and DP for enhanced privacy.
- Optimize techniques for IIoT-specific constraints.
- Validate Using real-world Datasets

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.

IT21822612 | Mendis H.R.M. | R25-039 24

System Architecture



8.3 Presentation 2

Contents

Search...

- > OVERALL 1
- > ADMR COMPONENTS 15
- > COMPONENT 2 PRI... 23
- > COMPONENT 3 SEC... 33
- > COMPONENT 4 SCPM 40
- > GENERAL END SLIDES 48

DATA-PRIVACY FOCUSED FEDERATED LEARNING FRAMEWORK FOR INDUSTRIAL IOT

R25 - 039

PROJECT GROUP

Team	Supervisors
 <i>Nanayakkara Y.D.T.D</i> <i>IT21826368</i>	 <i>Mr. Amila Nuwan Senarathne</i> <i>Supervisor</i>

8.4 Final Presentation

Contents

Search...

- Slide 1: DATA-PRIVACY ... 1
- Slide 2: PROJECT ... 2
- Slide 3: FRAMEW... 3
- Slide 4: PROBLEMS 4
- Slide 5: SOLUTIONS 5
- Slide 6: SYSTEM W... 6
- Slide 7: System W... 7
- Slide 8: Attack De... 8
- Slide 9: RESEARC... 9
- Slide 10: SOLUTI... 10
- Slide 11: ... 11
- Slide 12: Termin... 12
- Slide 13: ... 13
- Slide 14: Attack... 14
- Slide 15: DETECT... 15
- Slide 16: Logging 16
- Slide 17: Privacy ... 17
- Slide 18: ... 18
- Slide 19: SOLUTI... 19
- Slide 20: PPM Ac... 20
- Slide 21: METHO... 21
- Slide 22: FUNCTL... 22
- Slide 23: FUNCTL... 23
- Slide 24: PROOF... 24
- Slide 25: ... 25
- Slide 26: Secure ... 26
- Slide 27: ... 27
- Slide 28: ... 28
- Slide 29: Module... 29
- Slide 30: SERVER... 30
- Slide 31: OVERA... 31
- Slide 32: Log ma... 32
- Slide 33: Secure ... 33
- Slide 34: ... 34
- Slide 35: ... 35
- Slide 36: METHO... 36
- Slide 37: ... 37
- Slide 38: SAM M... 38
- Slide 39: AGGRE... 39
- Slide 40: USER T... 40
- Slide 41: ... 41
- Slide 42: We are ... 42
- Slide 43: Minis... 42

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



Final Presentation
R25 - 039

PROJECT GROUP
Supervisors

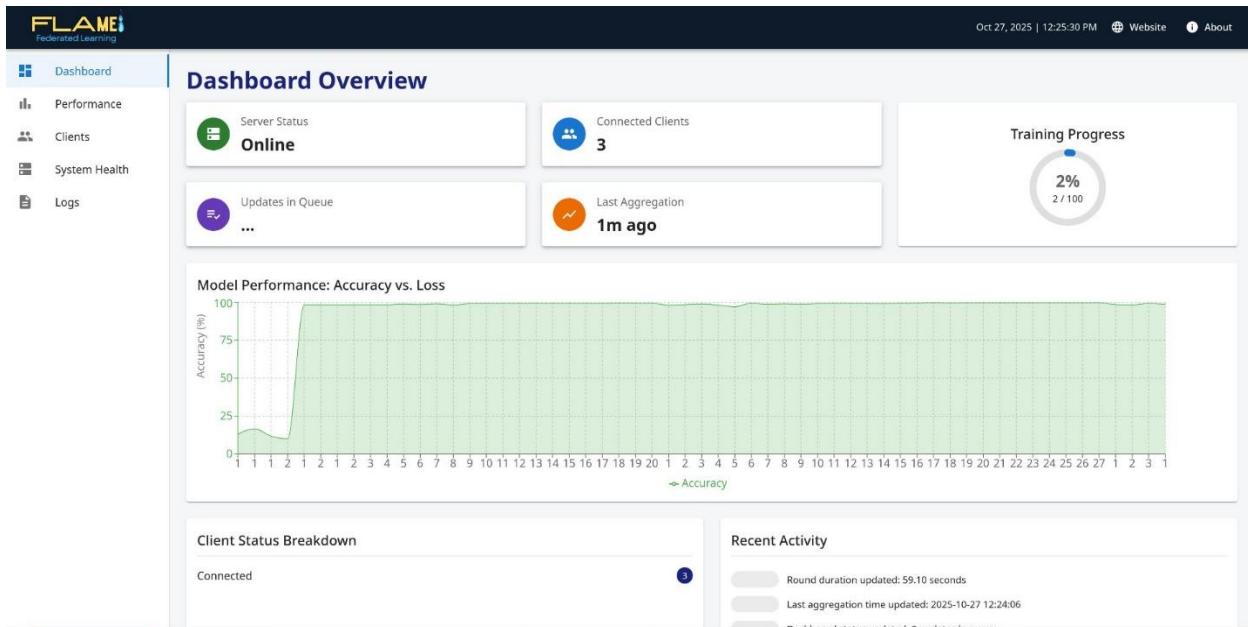
	Mr. Amila Nuwan Senarathne Supervisor		Mr. Tharanikarma Kumaraalingam Co-Supervisor
---	--	---	--

Team

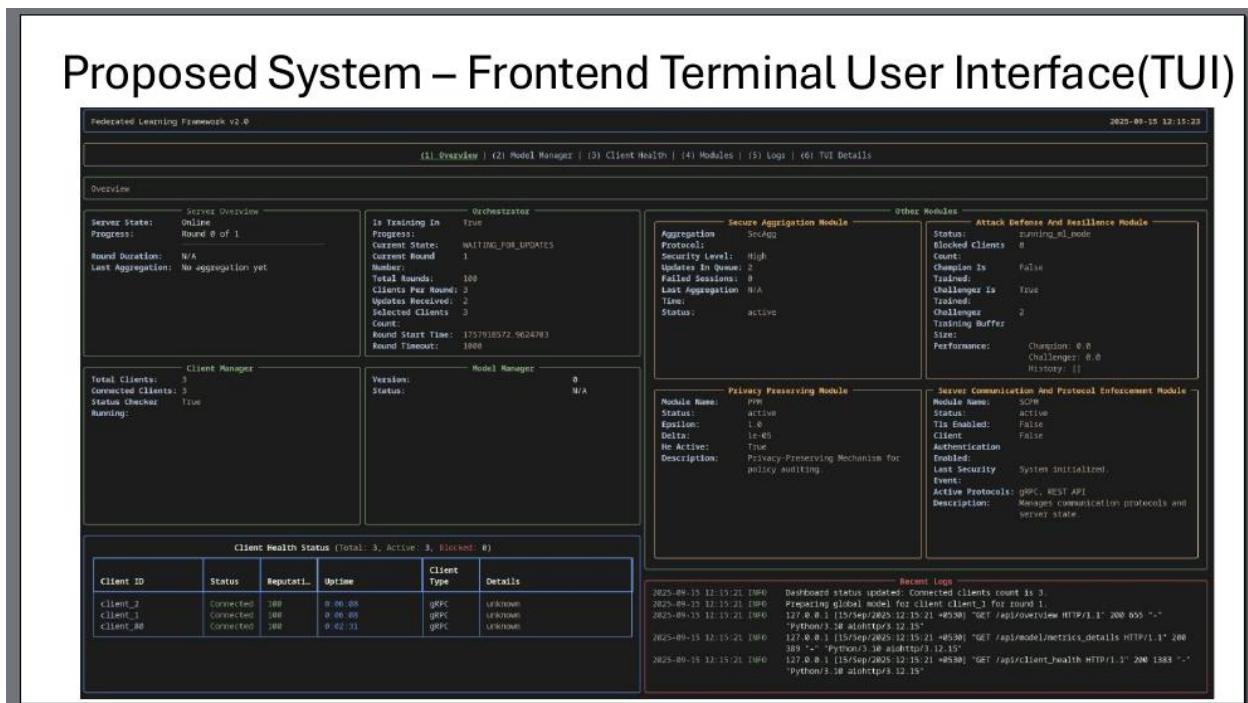
			
Nanayakkara Y.D.T.D IT21826368	Mendis H.R.M IT21822612	Dissanayaka K.D.A.R.A IT21828348	Weerasinghe K.M IT21831904

8.4 Final Product

Web Portal Frontend



Terminal User interface (Frontend)



8.5 Research Paper

I. Conference Apperence

To Tharindu D Nanayakkara <dlz.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.

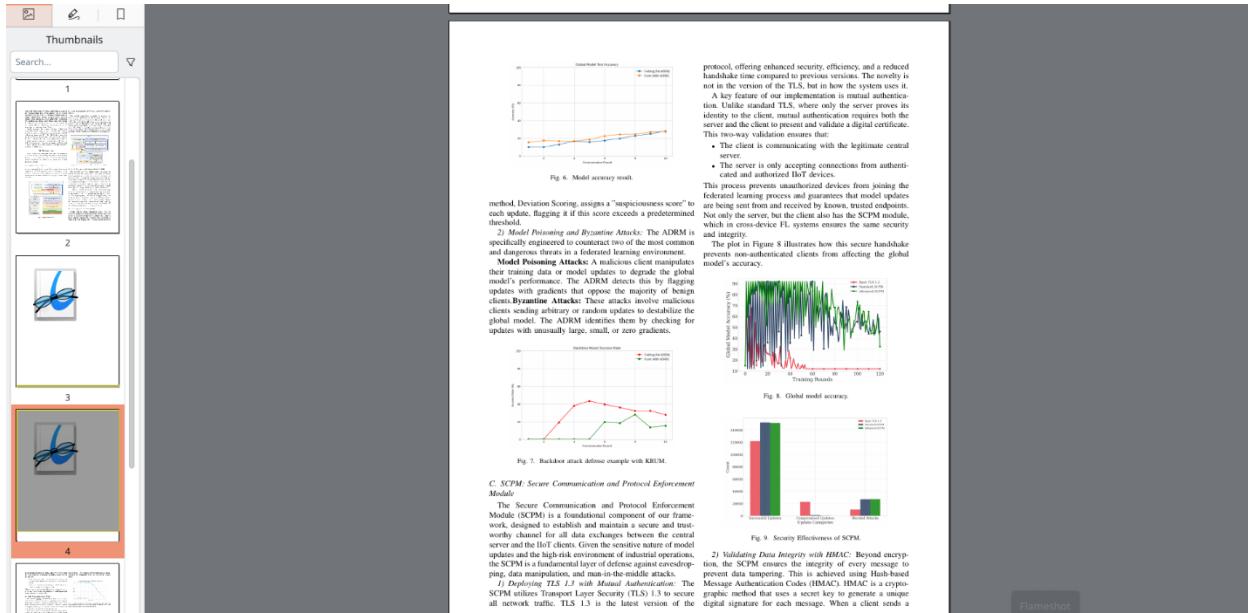
Paper ID: 469

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

CDAPSubmissionCloud 

Private group

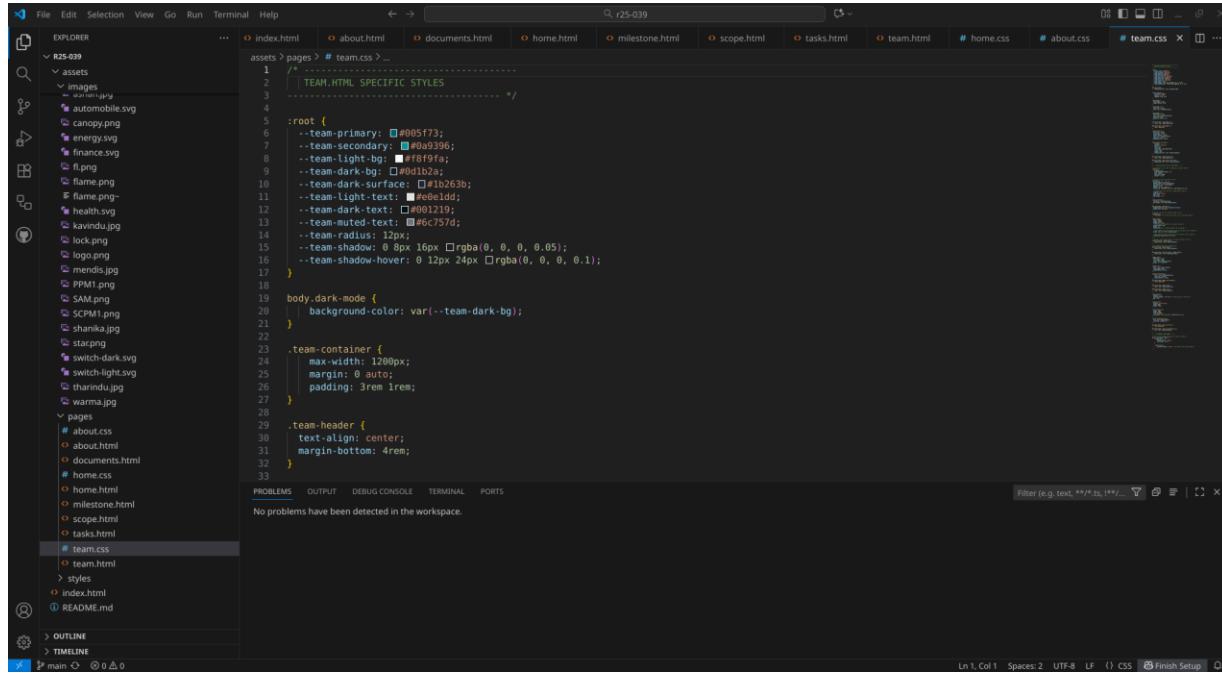
+ New  Upload  Edit in grid view  Share  Copy link  Add shortcut to OneDrive  Download  Export to Excel  Automate  Integrate  Sync

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.xlsx	September 20	CDAP SLIIT

10. Website

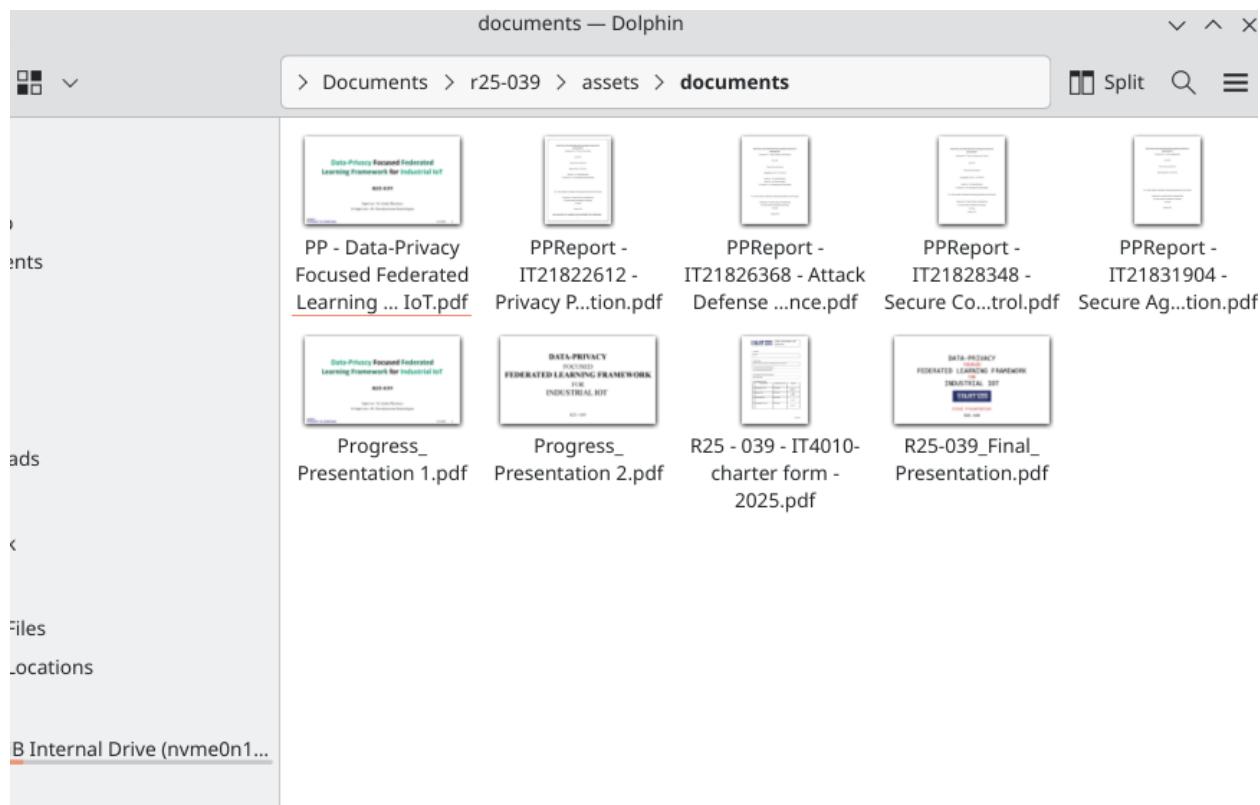
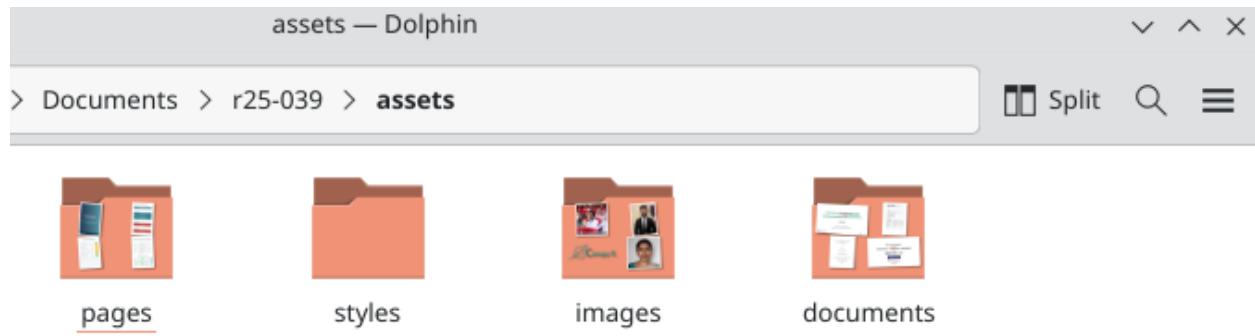
10.1 Development

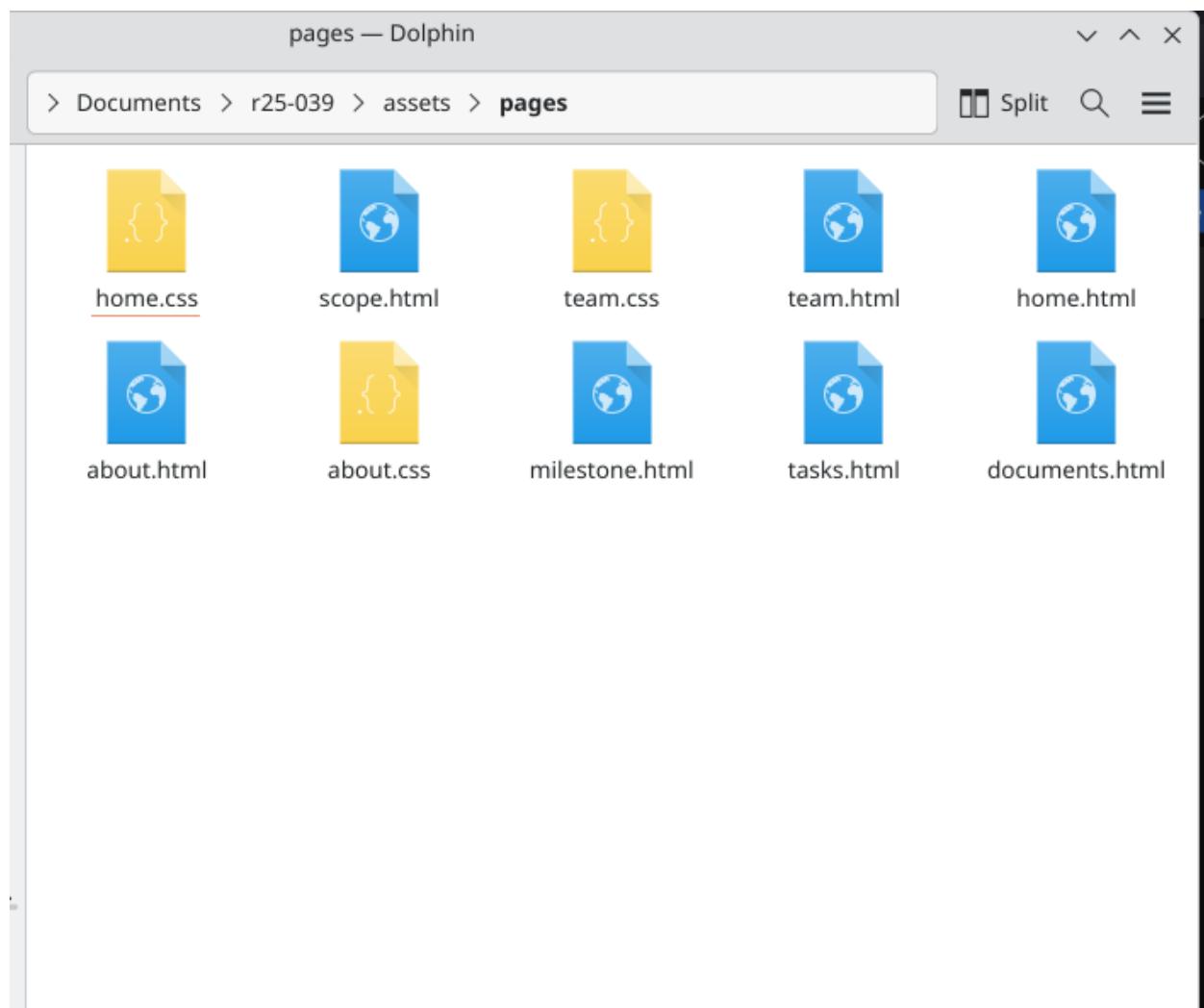


```

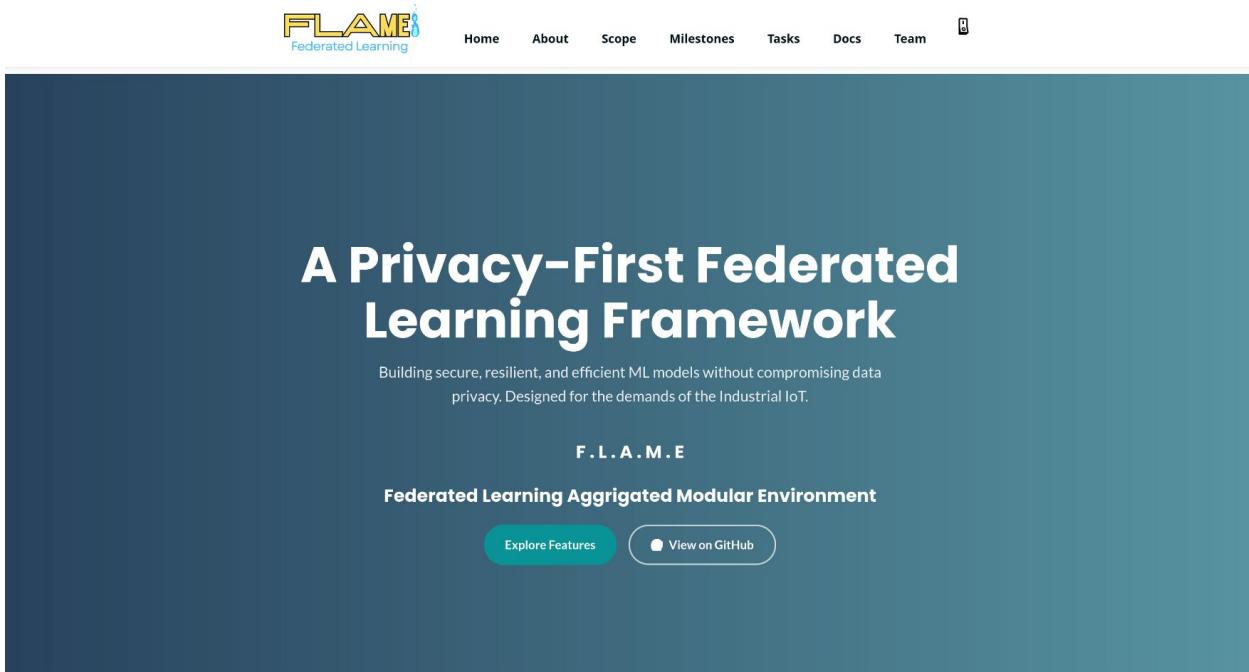
1  /*-----*
2   |TEAM.HTML SPECIFIC STYLES
3   *-----*/
4
5  :root {
6      --team-primary: #005f73;
7      --team-secondary: #0a9396;
8      --team-light-bg: #f8f9fa;
9      --team-dark-bg: #d1b2e;
10     --team-dark-surface: #1b263b;
11     --team-light-text: #e6e0d;
12     --team-dark-text: #001210;
13     --team-radius: 12px;
14     --team-shadow: 0 8px 16px rgba(0, 0, 0, 0.05);
15     --team-shadow-hover: 0 12px 24px rgba(0, 0, 0, 0.1);
16 }
17
18 body.dark-mode {
19     background-color: var(--team-dark-bg);
20 }
21
22 .team-container {
23     max-width: 1200px;
24     margin: 0 auto;
25     padding: 3rem 0;
26 }
27
28 .team-header {
29     text-align: center;
30     margin-bottom: 4rem;
31 }
32
33

```





10.2 Finalize

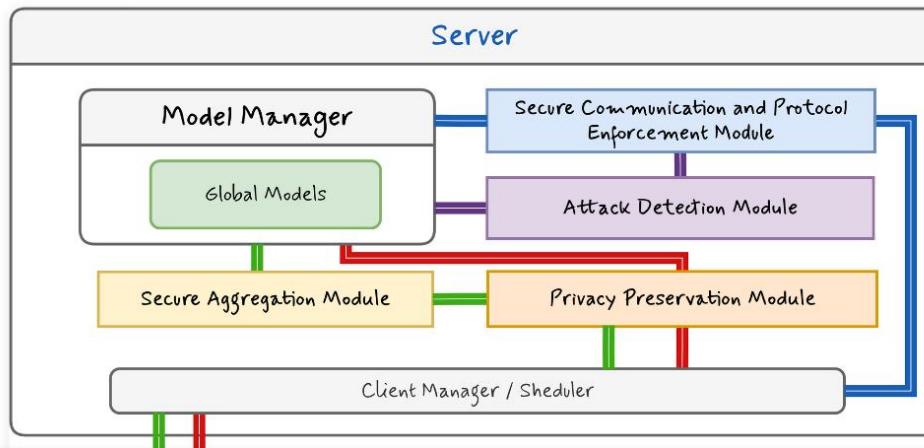


The screenshot shows the FLAME Federated Learning website. At the top, there is a navigation bar with links for Home, About, Scope, Milestones, Tasks, Docs, Team, and a search icon. The main title is "A Privacy-First Federated Learning Framework". Below the title, a subtitle reads: "Building secure, resilient, and efficient ML models without compromising data privacy. Designed for the demands of the Industrial IoT." The acronym "F.L.A.M.E" is displayed above the full name "Federated Learning Aggregated Modular Environment". There are two buttons at the bottom: "Explore Features" and "View on GitHub".

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

