Data-Privacy Focused Federated Learning Framework for Industrial IoT

R25-039

Supervisor - *Dr. Sanika Wijesekara*

Co-Supervisor - *Mr. Tharaniyawarma Kumaralingam*

Project Group

Supervisor

Supervisor - *Dr. Sanika Wijesekara*

Co-Supervisor

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

Introduction

Creating a Framework for Federated Learning for Industrial IoT focusing Data-Privacy.

Focusing

- Secure Aggregation
- Secure Command and Control
- Privacy Preservation
- Attack defence and resilience

Research Question

While IIoT revolutionizes industries, it introduces cybersecurity vulnerabilities. Does Federated Learning guarantee privacy protection, or are there still potential risks?

Privacy Benefits

Local data processing, no raw data transfer
Reduces sensitive data exposure

Potential Risks

Model Inversion Attacks
Gradient Leakage
Data Poisoning/Backdoor Attacks
Cross-device Variability
Adversarial Attacks

What are the exist technologies used in FL?

Differential Privacy
Homomorphic Encryption
Secure Multi-party Computation (SMPC)
Trusted Execution Environments (TEEs)
Federated Averaging with Regularization

Research Gaps

- Security solutions may not scale with large networks
- Lack of universal privacy standards for FL
- Cross-domain Privacy Compliances
- Privacy risks in FL, including model inversion and data poisoning.
- Lack of scalable and lightweight attack detection methods
- Limitations in current secure aggregation techniques.

Research Solution

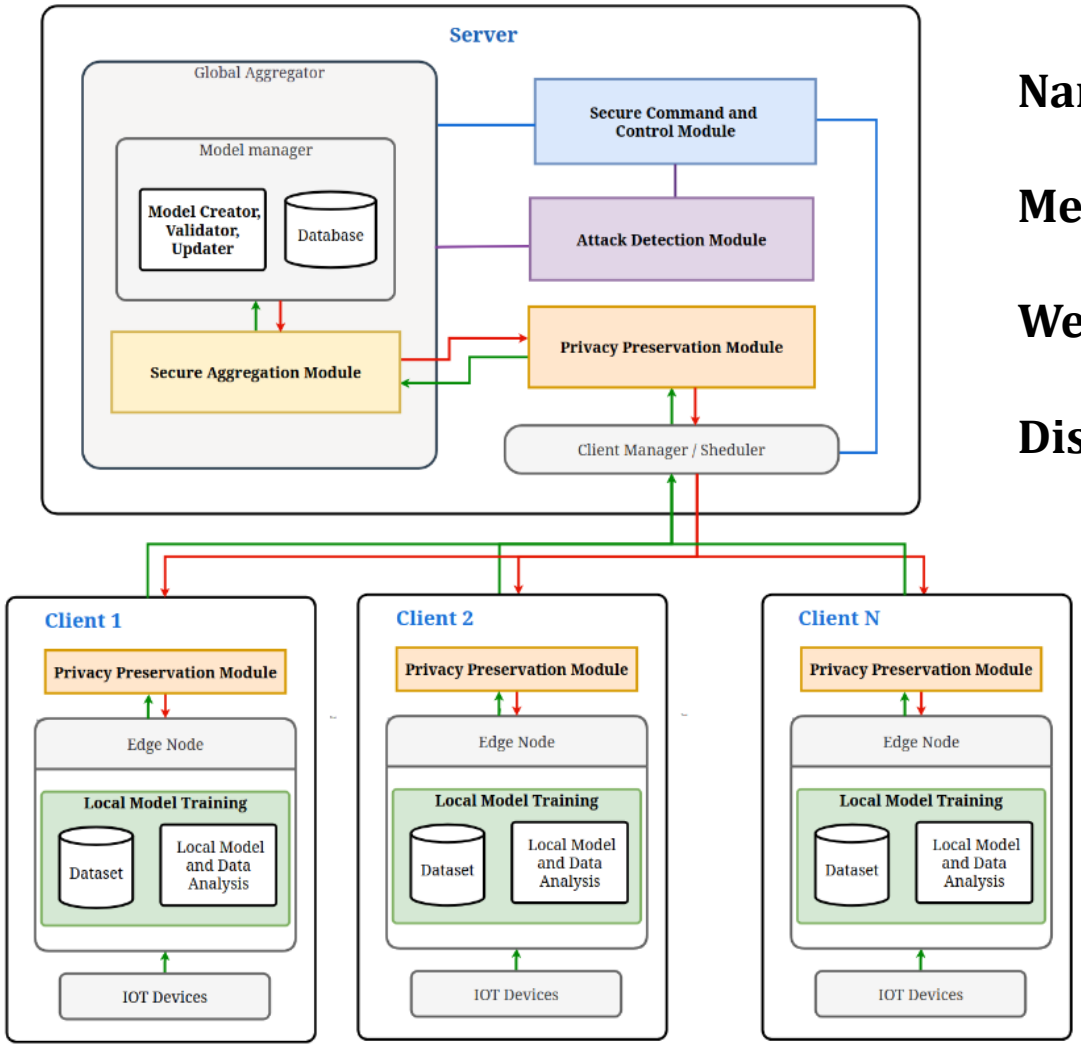
Main Objective

Develop a privacy-focused Federated Learning framework tailored for IIoT, addressing challenges like secure aggregation, attack resilience, privacy preservation, and robust communication.

Sub-Objectives

Attack Detection and Resilience
Hybrid Privacy-Preserving Techniques
Secure Aggregation Protocols
Secure Command and Control (C2)

System Architecture



Nanayakkara Y.D.T.D - Attack detection and resilience.

Mendis H.R.M - Hybrid privacy-preserving techniques.

Weerasinghe K.M. - Secure aggregation protocols.

Dissanayaka K.D.A.R. - Secure Command and Control (C2).

IT21826368 | NANAYAKKARA Y.D.T.D

Attack Detection and Resilience

Introduction

While Federated Learning ensures privacy in IIoT systems, does it provide sufficient defence against robust cybersecurity attacks, or are there gaps in its protection?

Research problem

How can attack detection and resilience be effectively integrated into Federated Learning for Industrial IoT environments ?

GAPS From others

Work	IIOT related	FL - Related	Focused attack nature	Features	Limitations with Existing Defense
[6]	No	yes	Label Inference Attack	• Model for label inference and model poisoning attacks	• Monitoring and anomaly detection for label leakage, training data subsampling, model regularization result in poor defense for other types of attacks.
[3]	yes	yes	Model poisoning Attack	• Attack Detection Secure. • Aggregation Technical overview	• Limited to specific model poisoning defenses; same as secure aggregation methods.
[4]	No	yes	Byzantine attacks	• Multi-Layered Defense Architecture • Optimization Strategies for Robust Learning	• Hight computational power use • Scalability issues • Euclidean Distances like Ineffectiveness for Coordinated Attacks • Increased Computational Demands
[5]	No, iot based	No	IoT related anomaly defense	• Traffic Behavior Monitoring • Anomaly Detection • Predictive Analysis	• Scalability Issues • Not build for dynamic Attack Patterns • Trust-based Routing Defenses
[7]	No	NO	IoT related anomaly defense	• Attack Detection using ASAE (Adversarial Sparse Autoencoder) • Data Normalization	• Lack of Real-Time Detection • Resource Constraints in IoT Devices

Challenges in IIoT and FL

- Heterogeneity of Devices
  - Diverse hardware and protocols.
  - Varying data types and volumes.
- Attack Resilience and Defence
  - Limited to specific model poisoning defences.
  - Ineffective against coordinated and dynamic attacks.
  - Trust-based routing lacks real-time detection.
- Gaps in real-time anomaly detection.
- Challenges with secure aggregation methods.

Specific Attack Types should be addressed

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

Main Objective

To design and implement lightweight, scalable mechanisms to detect and mitigate malicious activities in Federated Learning models for IIoT.

Sub-Objectives

- Lightweight ADR module for real-time detection.
- Mitigate model poisoning and Byzantine attacks.
- Enhance resilience and scalability.

REQUIREMENTS

Functional Requirements

- Federated Learning-based attack detection module.
- Lightweight resource utilization.
- Heterogeneity attack adaptation.
- Real-time anomaly detection and response.
- Privacy-preserving intrusion detection.

Non-functional requirements

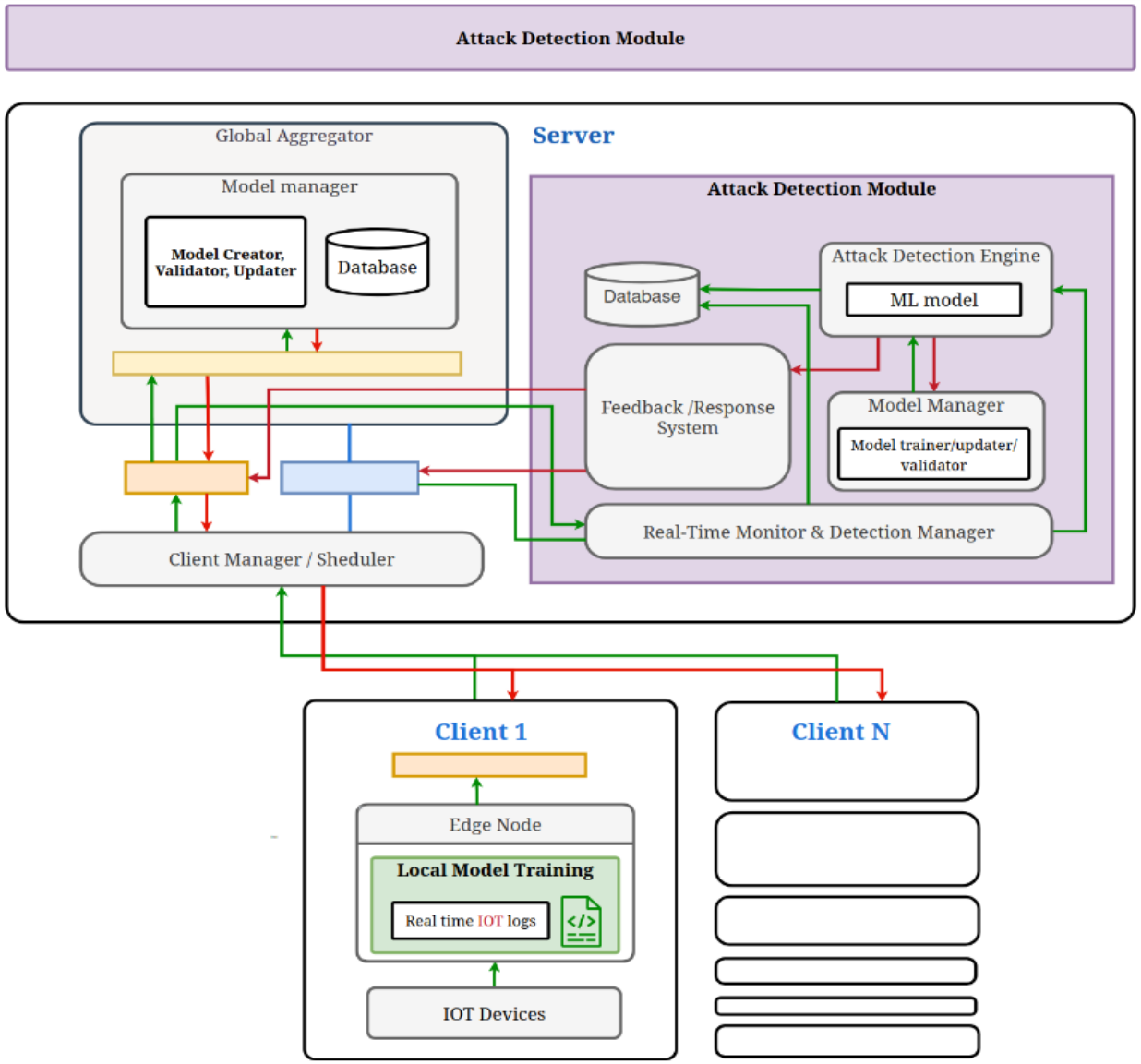
- High scalability to accommodate diverse IIoT devices.
- Minimal latency for real-time operations.
- Energy-efficient design is suitable for constrained devices.

Proposed Methodology

Attack Defense Resillence Model

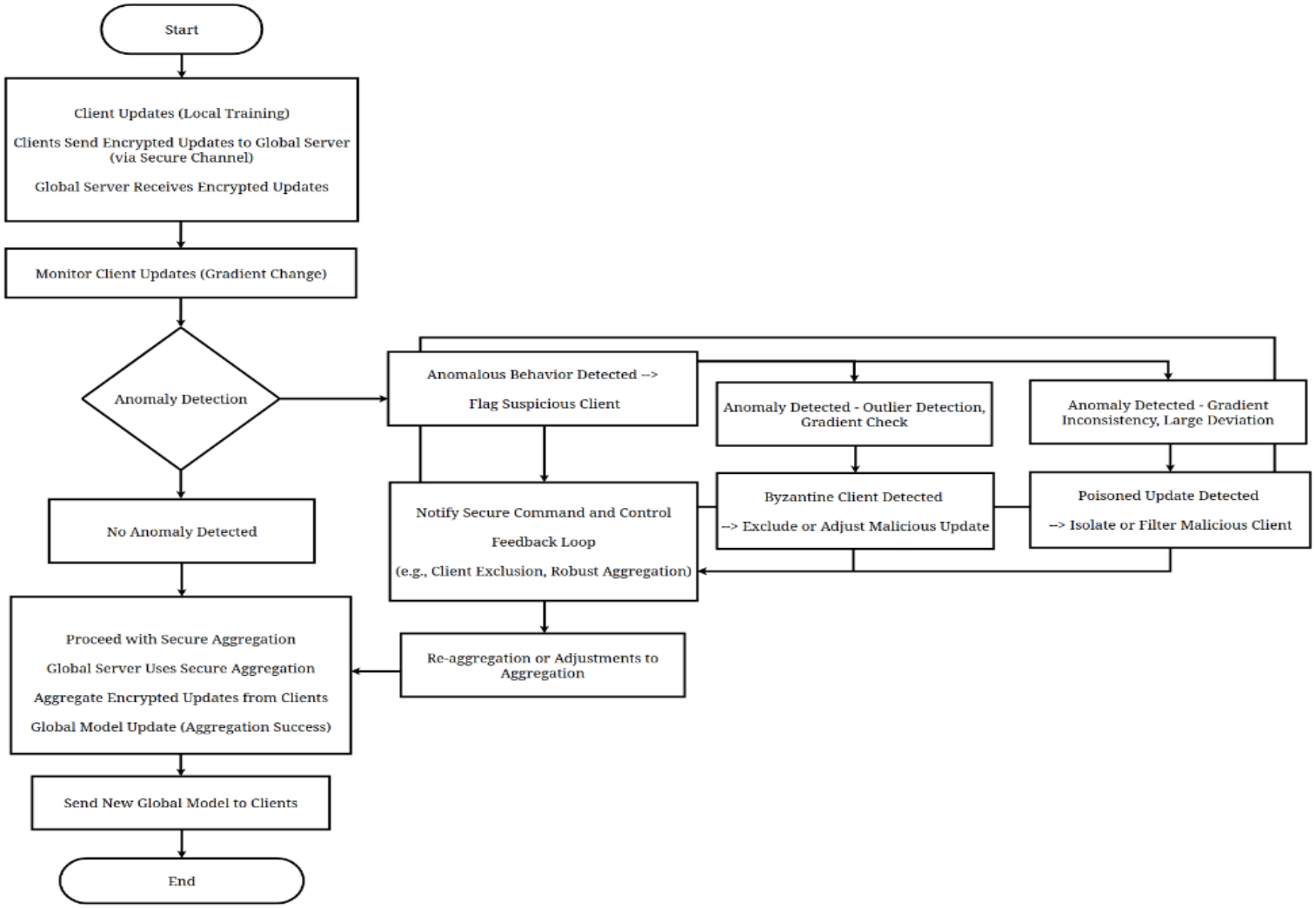
Ensure the defense of the whole federated learning process (*multiple ADR stages*) in pre agggrigation and post aggrigation

Component Diagram



- **Server Module:**
  - Attack Detection Module:
    - Attack Detection Engine: Detects anomalies using machine learning models.
    - Feedback/Response System: Provides secure feedback loop with clients for model updates and anomaly mitigation.
    - Real-Time Monitor & Detection Manager: Monitors client activity and detects deviations or threats.

Component process



ADR WBS

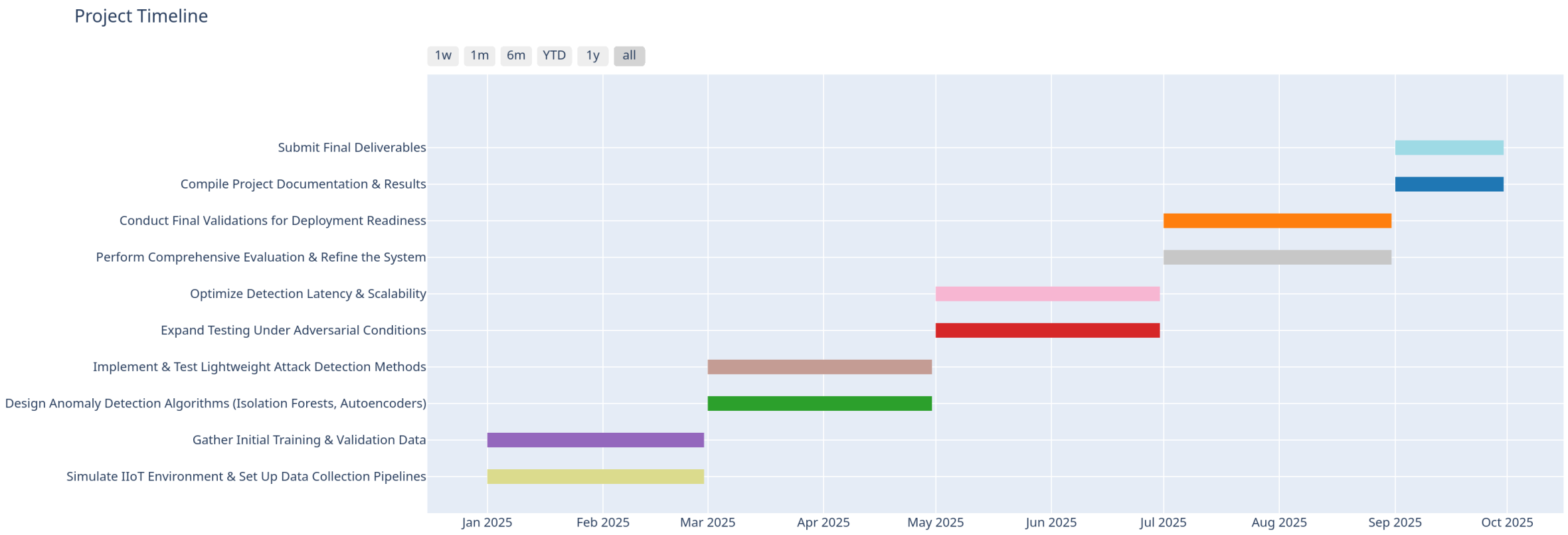
Phase 1: Data Collection and Preprocessing		Phase 2: Model Design and Implementation		Phase 3: Testing and Evaluation	
Simulate IIoT environment with heterogeneous devices.	Collect training data, including normal and anomalous activities.	Implement anomaly detection using Isolation Forests and Autoencoders.	Develop a lightweight module to detect Byzantine and poisoning attacks.	Test the model under adversarial conditions.	Evaluate detection accuracy, latency, and scalability.

- Hardware: Computational power (laptop).
- Software: Python, TensorFlow or ML libraries and related tools.
- Resources: Datasets for training and evaluation (Industrial Control System (ICS) Cyber Attack Dataset, SWaT (Secure Water Treatment) Dataset, IoT-23 Dataset, N-BaIoT)
- Simulation tools for IIoT scenarios.

- **Deliverables:**
  - A scalable, lightweight attack detection module.
  - Comprehensive test results showing system accuracy and robustness.

Completion of the project

- Gantt chart



References

[1] Truong, Nguyen et al., "Privacy Preservation in Federated Learning: An Insightful Survey from the GDPR Perspective," 2024.

[2] Parimala et al., "Fusion of Federated Learning and Industrial Internet of Things: A Survey," 2024.

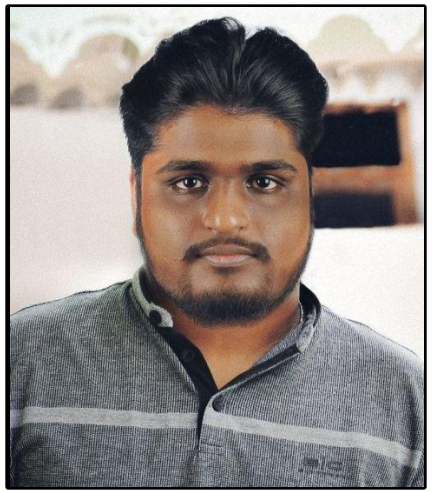
[3] Yazdinejad et al., "A Robust Privacy-Preserving Federated Learning Model Against Model Poisoning Attacks," 2024.

[4] Godavarthi et al., "Federated Learning's Dynamic Defense Against Byzantine Attacks," 2024.

[5] Ahmadi, K., "A Trust-Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation," 2024.

[6] Ding, L., et al., "Threshold Filtering for Detecting Label Inference Attacks in Vertical Federated Learning," 2024.

[7] Prasad, K.S., "Augmenting Cybersecurity through Attention-Based Stacked Autoencoder with Optimization Algorithm for Detection and Mitigation of Attacks on IoT-Assisted Networks," 2024.



IT21822612 | MENDIS H.R.M

Privacy Preservation

Research Problem

The Challenge of Privacy in IIoT Systems with Federated Learning:

- Sensitive Data Risks

  IIoT systems generate private data that must be safeguarded against misuse.

Key Issues:

Gradient Leakage and Adversarial Attacks

High computational overhead of techniques like Homomorphic Encryption (HE).

Accuracy vs. Privacy Trade-Off with Differential Privacy (DP).

Objectives and Research Questions

Objectives

- Identify privacy vulnerabilities in FL for IIoT.
- Propose privacy-preserving mechanisms combining **HE and DP**.
- Optimize computational efficiency for IIoT constraints.
- Validate methods using real-world datasets and scenarios.

Research Questions

- How to address gradient leakage and adversarial attacks in FL for IIoT?
- What strategies balance privacy, scalability, and computational efficiency?
- How to combine HE and DP for enhanced privacy without compromising accuracy?.
- How to adapt techniques to IIoT constraints?
- How to validate methods in real-world IIoT scenarios?

Research Gaps

Gap	Description
Lack of hybrid privacy solutions	While individual techniques like DP and HE are well-researched, their combined use in IIoT systems remains underexplored. A hybrid solution could address both privacy and performance challenges more effectively.
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.

Methodology

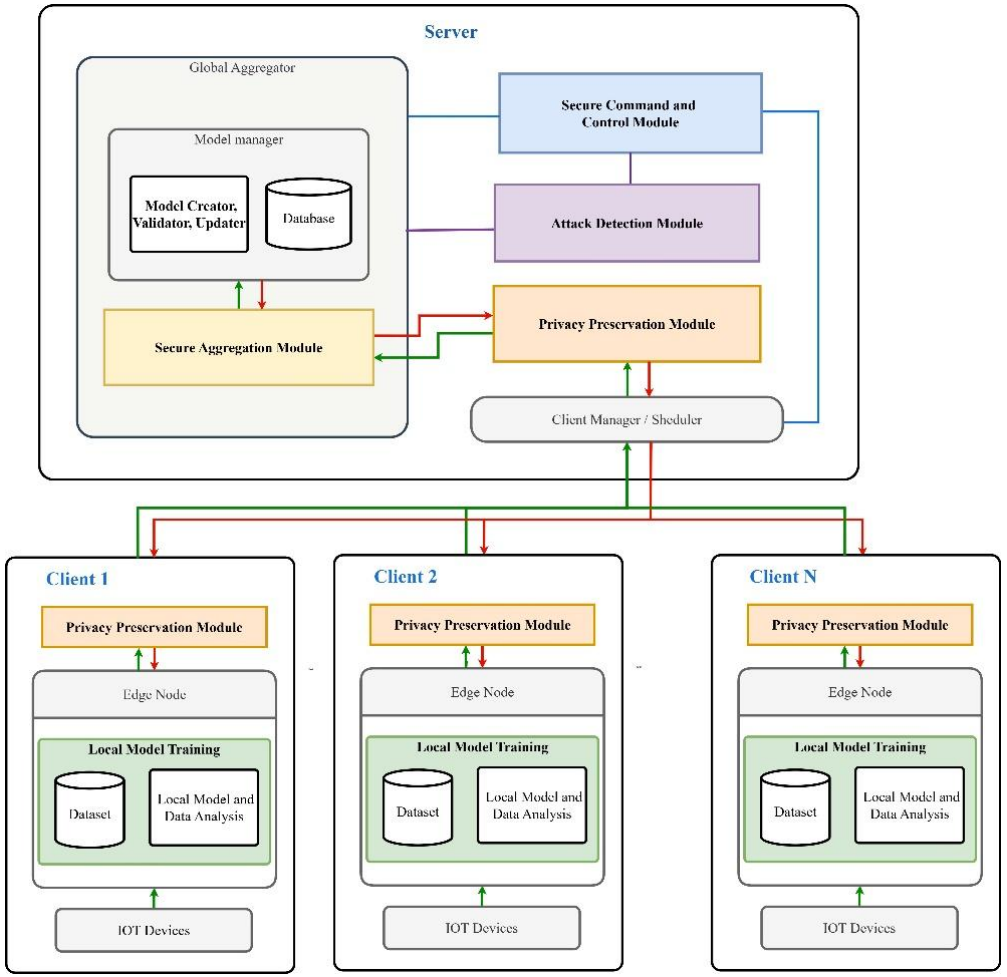
Approach:

- 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:

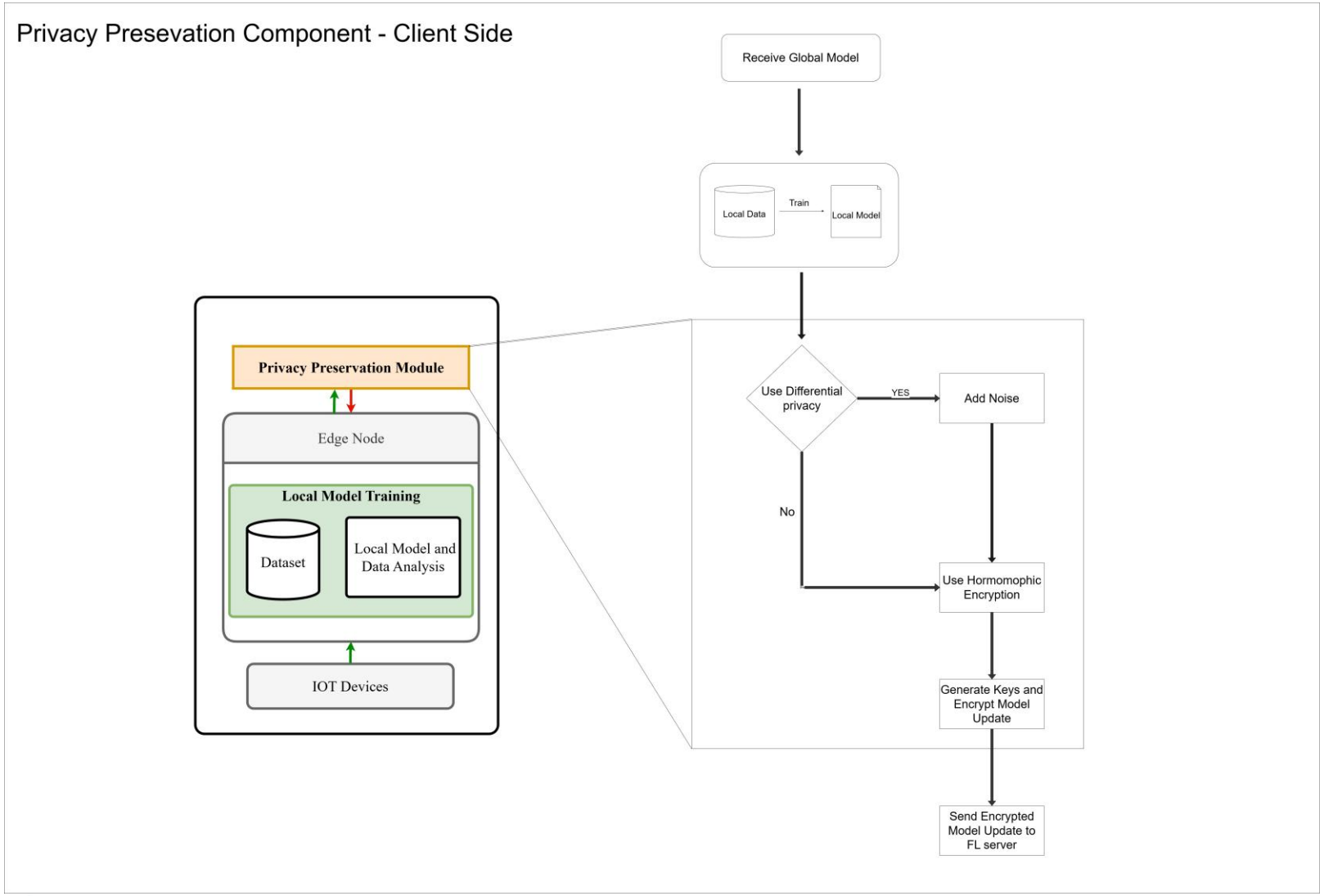
- **Homomorphic Encryption (HE)**: Encrypts gradients, allowing computations on encrypted data without decrypting it. Prevents data leakage even if adversaries intercept communications.
- **Differential Privacy (DP)**: Ensure that individual data points cannot be separated by adding controlled noise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

System Architecture

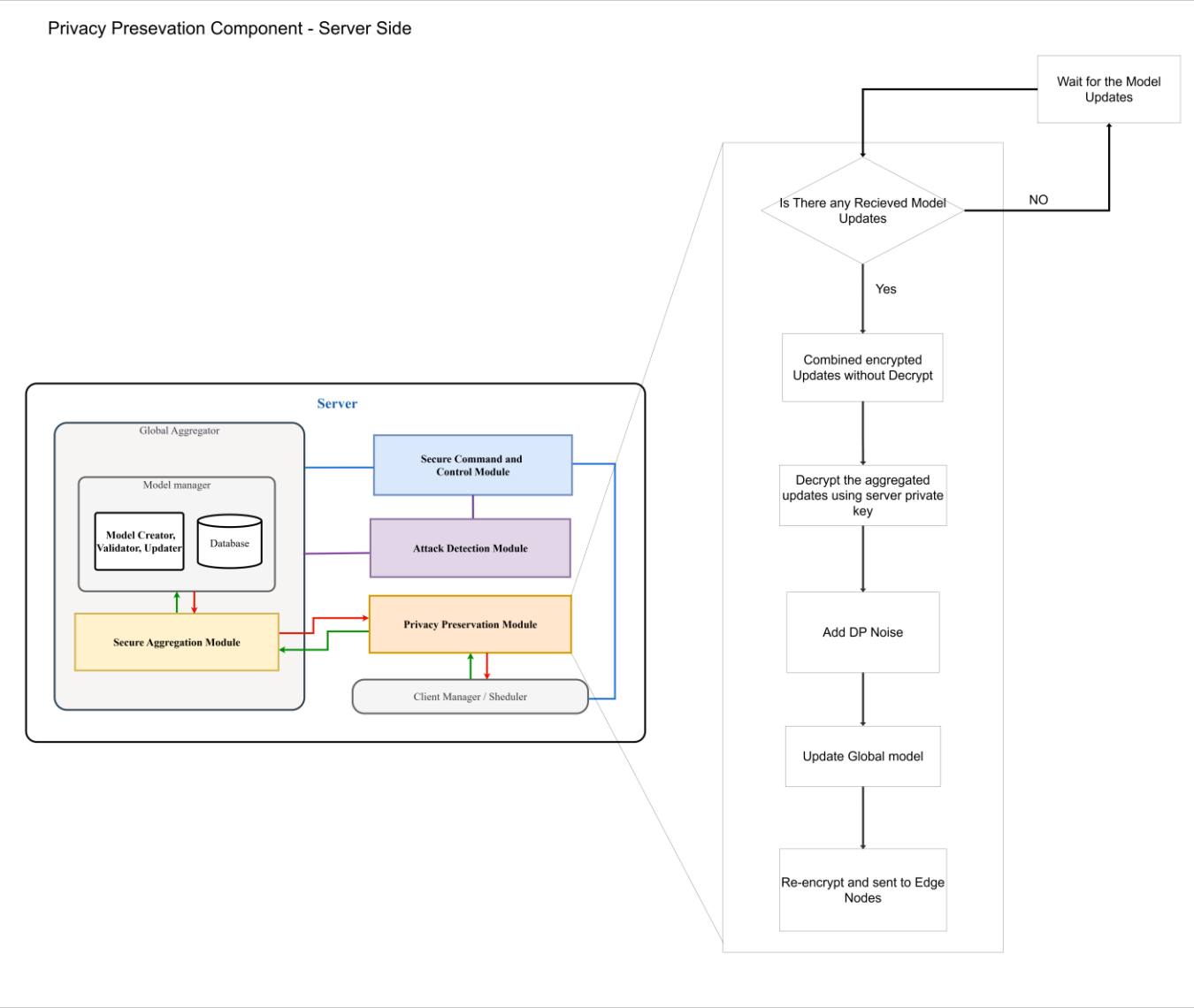


Mendis H.R.M: Hybrid privacy-preserving techniques.

Component Process (Client Side)



Component Process (Server Side)



Functional and non-functional requirements

Functional Requirements

- **Differential Privacy:** Add calibrated noise either to gradients or outputs, then share in the process of federated learning.
- **Homomorphic Encryption:** Perform the encryption of gradients shared between IIoT devices and the central server using Homomorphic Encryption.
- **Threat Simulation:** Simulate some of the privacy attacks, like the reconstruction attack, and test the efficiency of deployed privacy mechanisms.
- **Privacy Audits:** Regular audits should be performed to maintain privacy standards and to identify potential loopholes.

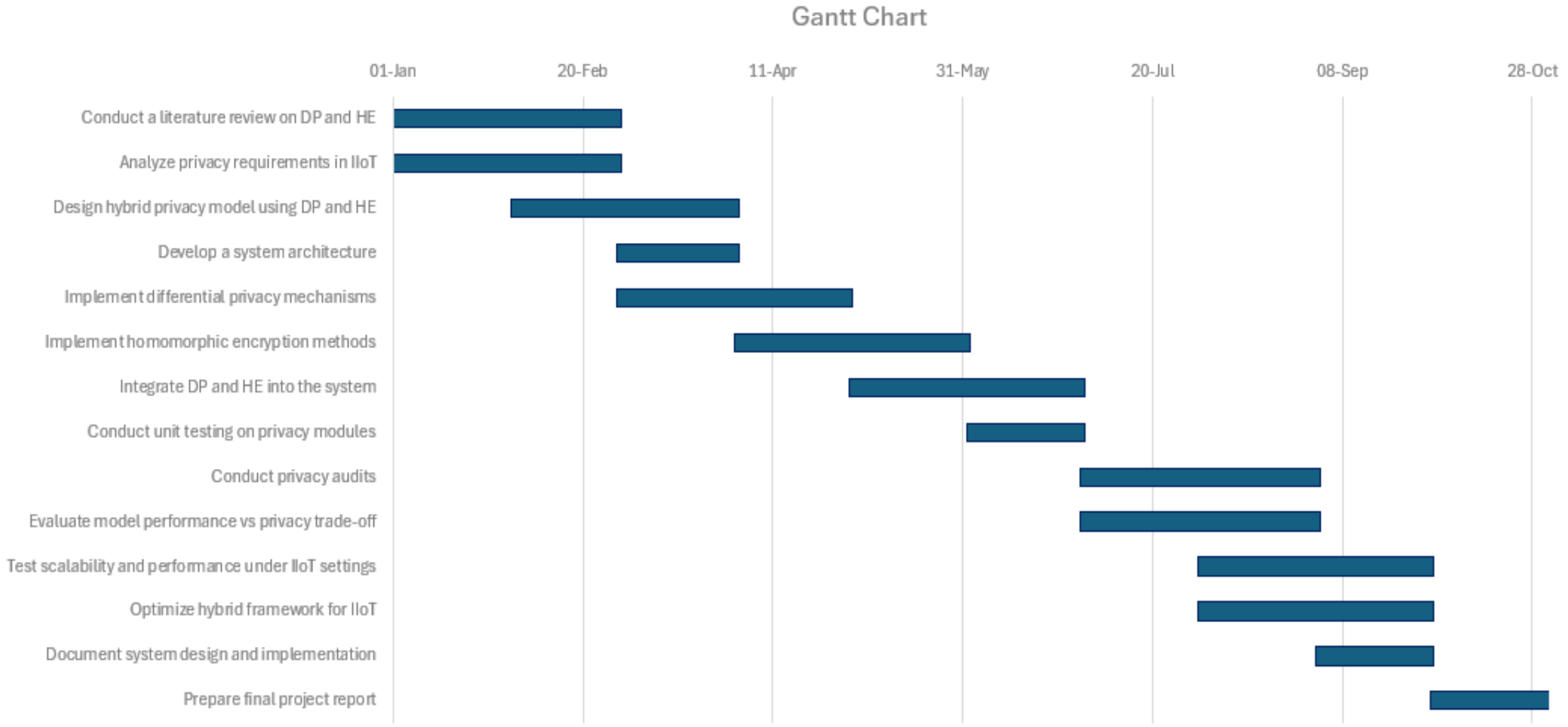
Non-functional requirements

- **Scalability:** The system should scale up when the number of IIoT devices is increasing without significant deterioration in performance.
- **Efficiency:** Both Differential Privacy and Homomorphic Encryption mechanisms should be lightweight w.r.t computational overhead.
- **Security:** Ensure strong encryption mechanisms so unauthorized access or tampering with data could not be allowed.
- **Reliability:** The privacy preservation component has to operate reliably under poor resources such as IIoT networks.
- **Compliance:** Adhere to relevant data privacy regulations such as GDPR, CCPA, or equivalent standards applicable to IIoT environments.
- **Maintainability:** Code must be modular to let updates be performed smoothly or integration of new PPA.

Work Breakdown Structure

Task	Phase
Conduct a literature review on DP and HE	Phase 1 - Research and Design
Analyze privacy requirements in IIoT	
Design hybrid privacy model using DP and HE	
Develop a system architecture	
Implement differential privacy mechanisms	Phase 2 - Implementation
Implement homomorphic encryption methods	
Integrate DP and HE into the system	
Conduct unit testing on privacy modules	
Conduct privacy audits	Phase 3 -Evaluation and Testing
Evaluate model performance vs privacy trade-off	
Test scalability and performance under IIoT settings	
Optimize hybrid framework for IIoT	
Document system design and implementation	Phase 4 - Documentation and Finalization
Prepare final project report	

Completion of the project



References

Dritsas, Elias and Trigka, Maria, "Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications," *Journal of Sensor and Actuator Networks,* vol. 14, p. 9, 01 2025.

Betul Yurdem, Murat Kuzlu, Mehmet Kemal Gullu, Ferhat Ozgur Catak, Maliha Tabassum, "Federated learning: Overview, strategies, applications, tools and future directions," *Heliyon,* vol. 10, no. 19, 2024.

Shaohua Cao, Shangru Liu, Yansheng Yang, Wenjie Du, Zijun Zhan, Danxin Wang, Weishan Zhang, "A hybrid and efficient Federated Learning for privacy preservation in IoT devices," *Ad Hoc Networks,* vol. 170, 2025.

Hijazi, Neveen Mohammad and Aloqaily, Moayad and Guizani, Mohsen and Ouni, Bassem and Karray, Fakhri, "Secure Federated Learning With Fully Homomorphic Encryption for IoT Communications," *IEEE Internet of Things Journal,* vol. 11, pp. 4289-4300, 2024.

Mohialden, Yasmin and Mahmood Hussien, Nadia and Salman, Saba and Aljanabi, Mohammad, "Secure Federated Learning with a Homomorphic Encryption Model," *International Journal Papier Advance and Scientific Review,* vol. 4, pp. 001-007, 2023.

Oshamah, Ibrahim and Khalaf, and Algburi, Sameer and Selvaraj, Dhanasekaran and Saeed, Mhd and Elmedany, Wael and Khalaf, Osamah, "Federated learning with hybrid differential privacy for secure and reliable cross-IoT platform knowledge sharing," *SECURITY AND PRIVACY,* vol. 7, 2024.

Anwar, Sayeda and , Asaduzzaman and Sarker, Iqbal, "A differential privacy aided DeepFed intrusion detection system for IoT applications," *SECURITY AND PRIVACY,* 07 2024.

IT21831904 | WEERASINGHE K.M

Secure Aggregation

Introduction

- **Secure Aggregation** ensures that multiple parties can compute an aggregate value, without revealing their individual private data to each other. This means participants only learn the final result and nothing else about others' inputs, preserving privacy while enabling collaboration.

Research Problem

- The main research problem is the lack of secure aggregation solutions in federated learning that addresses the scalability and lightweight cryptographic solutions in secure aggregation while preserving privacy. And in the process of creating this component mitigate adversarial attacks, balance out the performance and security.

Research Question

- What cryptographic algorithms and can be used to create a scalable and lightweight secure aggregation component for the system.
- How is this component integrated into the overall framework? And how it prevents adversarial attacks and helps maintain user confidentiality and privacy.

Research Gap

Secure aggregation solution	Limitations
[1]	• Addresses backdoor attacks and model-poisoning with secure aggregation. • Fails to balancing privacy and model quality as added noise reduces accuracy
[2]	• Struggles to distinguish between malicious servers and clients • malicious privacy is guaranteed, addressing malicious security (poisoning, backdoor, outliers) remains a challenge in a large IoT environment.
[3]	• This solution doesn't address the backdoor attacks or injection attacks

Proposed solutions	• **Utilize cryptographic measures, such as a lightweight model cryptography for scalability.** • **Aggregates model updates so only a subset of devices can decrypt them, preventing corruption by a single malicious device.**

Objectives

The main objective is to develop a scalable and lightweight cryptographic framework that leverages Shamir's Secret Sharing and threshold cryptography to ensure secure, efficient, and reliable aggregation of model updates, protecting against malicious devices while maintaining system scalability.

Design and implement a secure aggregation protocol

Evaluate the model’s performance in IIoT

Integration, optimization and continuous development

Methodology

Data Pre-Processing: Preprocess inputs that are being transmitted

Secret sharing – split updates into secret shares and distribute shares to the aggregators.

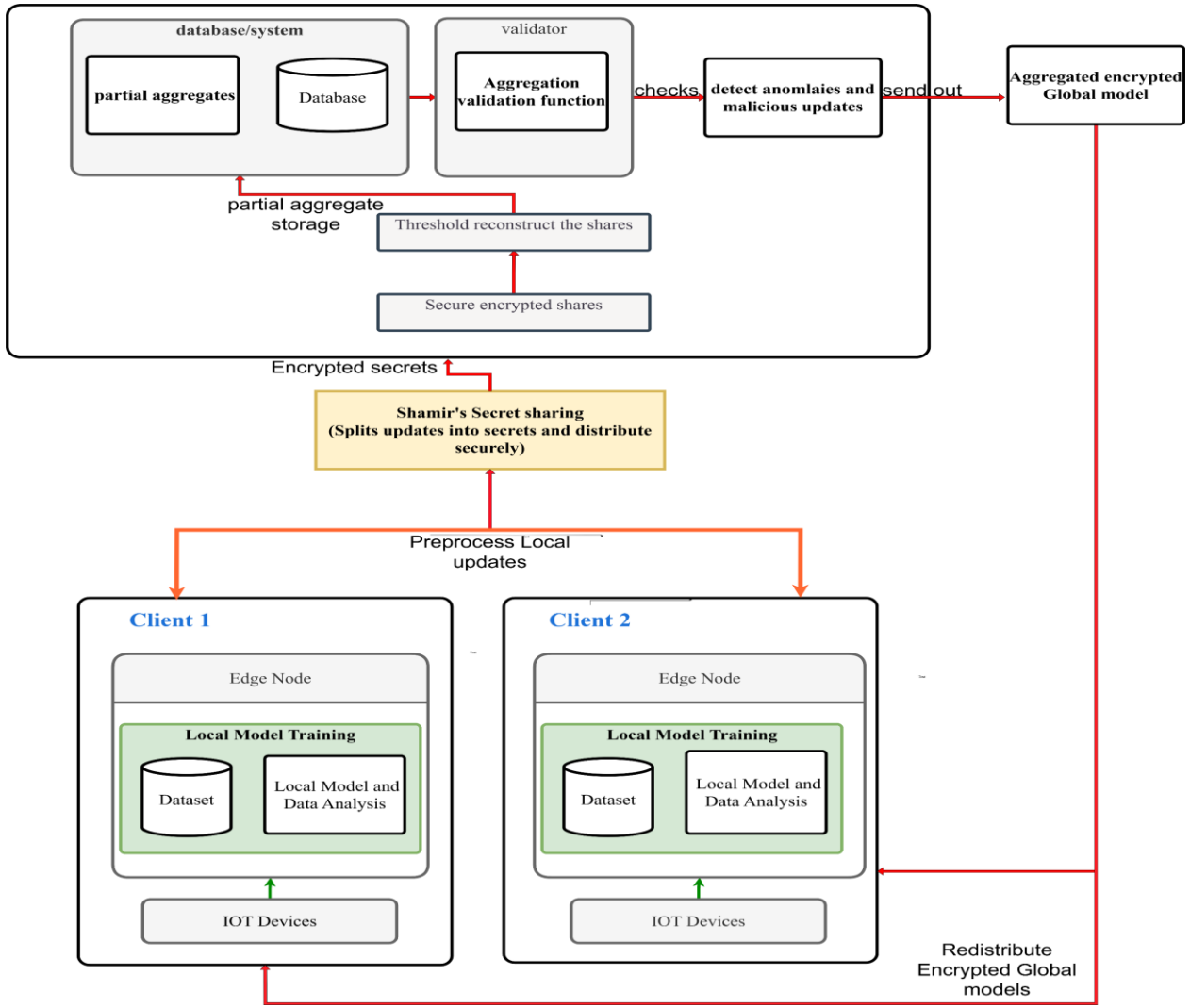
Secure transmission – encrypt shares for secure delivery and authenticate communcations

Reconstruction - aggregate shares upon reaching the threshold and reconstruct and validate data integrity

Aggregation validation detect any anomalies or malicious update and then ensure secure validated outputs

Redistribution – redistribution of the encrypted global model

Component Architecture



Functional and non-functional requirements

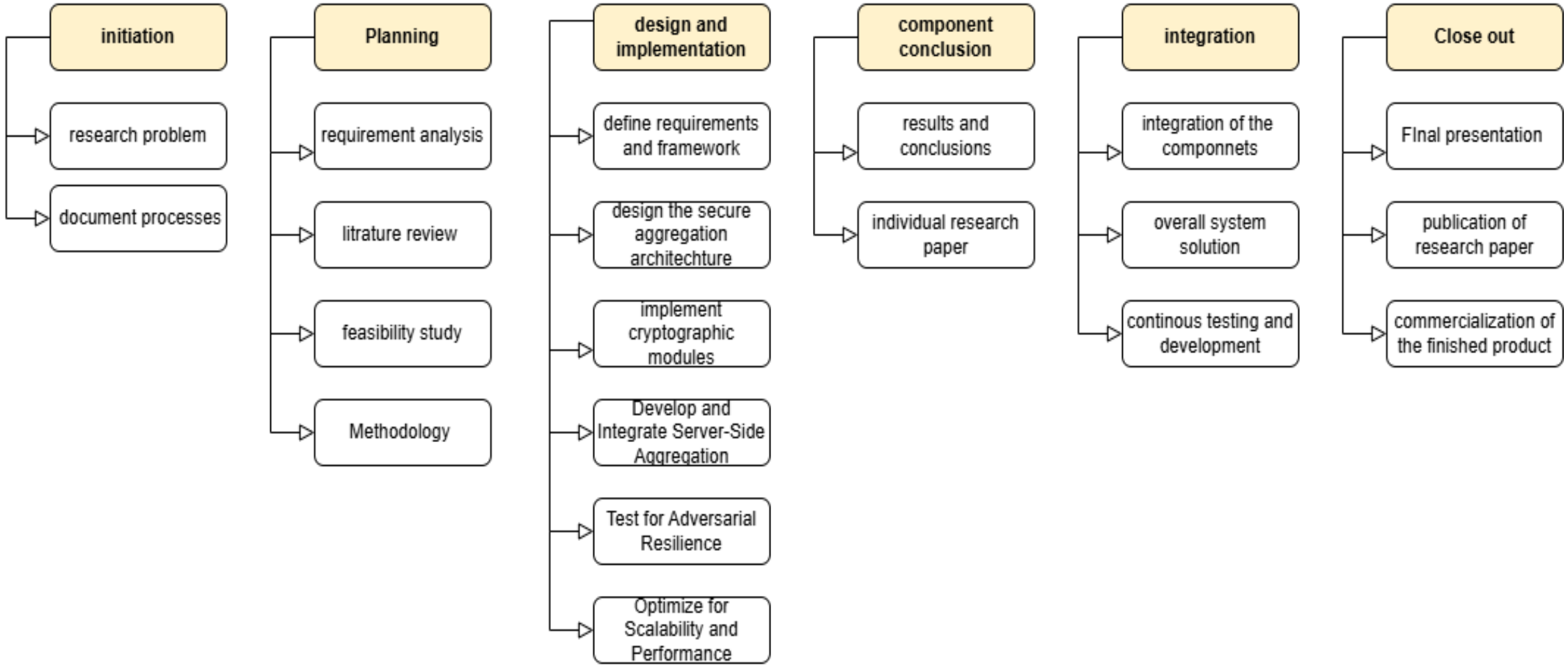
Functional requirements

- **Secure aggregation** – implement a secure aggregation model that compute aggregate values while preserving privacy
- **Update handling** – be able to handle model updates of multiple client user base.
- **Key management** – effective key management of the cryptographic models'
- **Anomaly detection** – detect malicious and benign updates

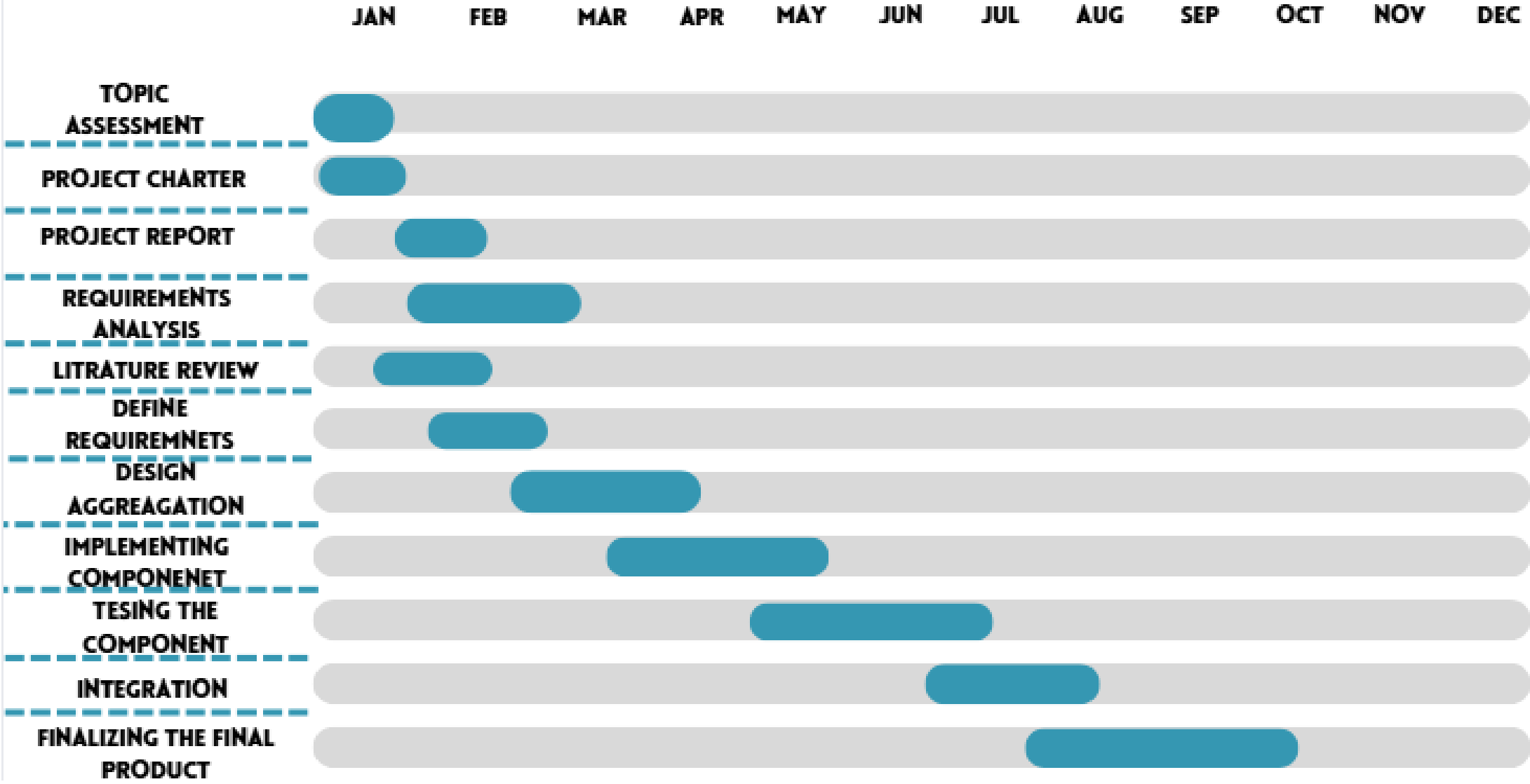
Non-functional requirements

- **Performance Efficiency**: The process must perform well with low latency and overhead
- **Fault Tolerance and Reliability**: tolerate failures of clients without compromising availability or integrity of the aggregation process.
- **Scalability**: handle a large set of user models
- **Compliance with Regulations**: comply with regulations to preserve user privacy
- **Security**: Maintain confidentiality and integrity of model updates throughout the process.

Work breakdown structure



GANTT CHART


JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
TOPIC ASSESSMENT
PROJECT CHARTER
PROJECT REPORT
REQUIREMENTS ANALYSIS
LITRATURE REVIEW
DEFINE REQUIREMNETS
DESIGN AGGREAGATION
IMPLEMENTING COMPONENET
TESING THE COMPONENT
INTEGRATION
FINALIZING THE FINAL PRODUCT

References

[1] Zhang, Zhuosheng and Li, Jiarui and Yu, Shucheng and Makaya, Christian, "SAFELearning: Secure Aggregation in Federated Learning with Backdoor Detectability," Institute of Electrical and Electronics Engineers (IEEE), 2023.

[2] Rathee, Mayank and Shen, Conghao and Wagh, Sameer and Popa, Raluca Ada, "ELSA: Secure Aggregation for Federated Learning with Malicious Actors," 2023.

[3] Shenghui Li, Edith Ngai, Thiemo Voigt, "Byzantine-Robust Aggregation in Federated Learning," 2021.

[4] Mohamad Mansouri, Melek Önen, Wafa Ben Jaballah, Mauro Conti, "SoK: Secure Aggregation Based on Cryptographic Schemes for," petsymposium.org, 2023.

[5] Hongbin, Fan and Zhi, Zhou, "Privacy-Preserving Data Aggregation Scheme Based on Federated Learning for IIoT," 2023.

IT218268348 | DISSANAYAKA K.D.A.R. A

Secure Command and Control

Research Problem

"How can secure communication mechanisms be implemented in a Command and Control (C2) system for Federated Learning, ensuring proper communication between devices and clients, as well as between clients, while validating incoming data to prevent malicious actions and ensure data integrity?"

Research Gaps

Gap	Description	Solution	References
Communication Security	Ensuring secure communication between IoT devices and the command/control module.	- Implement TLS 1.3 with ECC for lightweight encryption. - Use PSK for session resumption. - Explore post-quantum cryptography.	[6]
Data Integrity	Making certain that information is not altered while being sent or stored	Use HMAC with dynamic key rotation. - Combine HMAC with digital signatures. - Implement lightweight MACs like GMAC.	[7]
Access Control	limiting access to devices and users that are permitted	- Implement mutual TLS (mTLS). - Use role-based access control (RBAC). - Integrate MFA for users.	[8]
Threat Detection	Detecting and mitigating potential security threats in real-time	- Use ML-based anomaly detection. - Implement rate limiting and throttling. - Monitor for unusual command patterns	[9]
Resource Constraints	Addressing limited computational power, memory, and energy in IoT devices.	- Use lightweight cryptography - Optimize TLS with ECC and PSK. - Implement delta updates for firmware.	[10]
Scalability	Ensuring the system can handle a growing number of devices and users.	- Use decentralized architecture - Implement edge computing for distributed processing. - Optimize protocols for low overhead.	[11]

Objective

Develop a **Secure Command and Control (C2) Module** for IIOT.

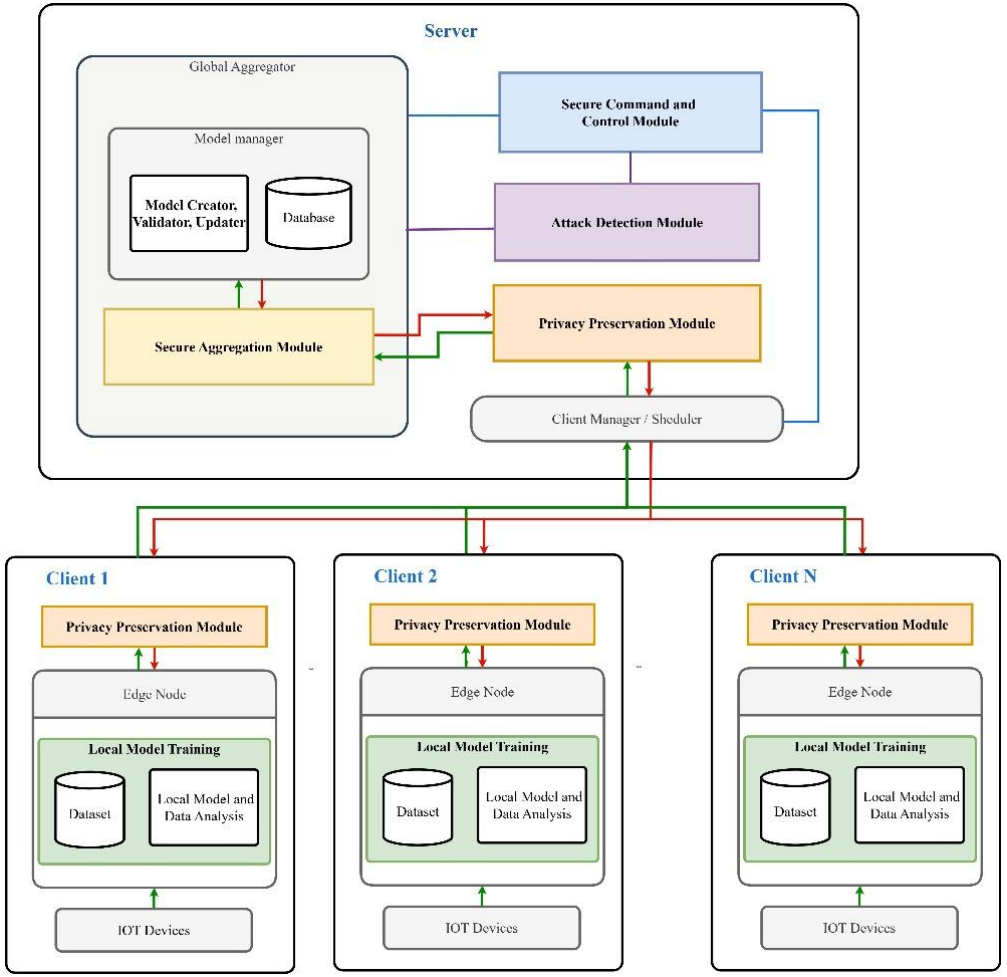
Ensure reliable communication and **client data validation**.

Verify that incoming data is authentic and untampered.

Solution

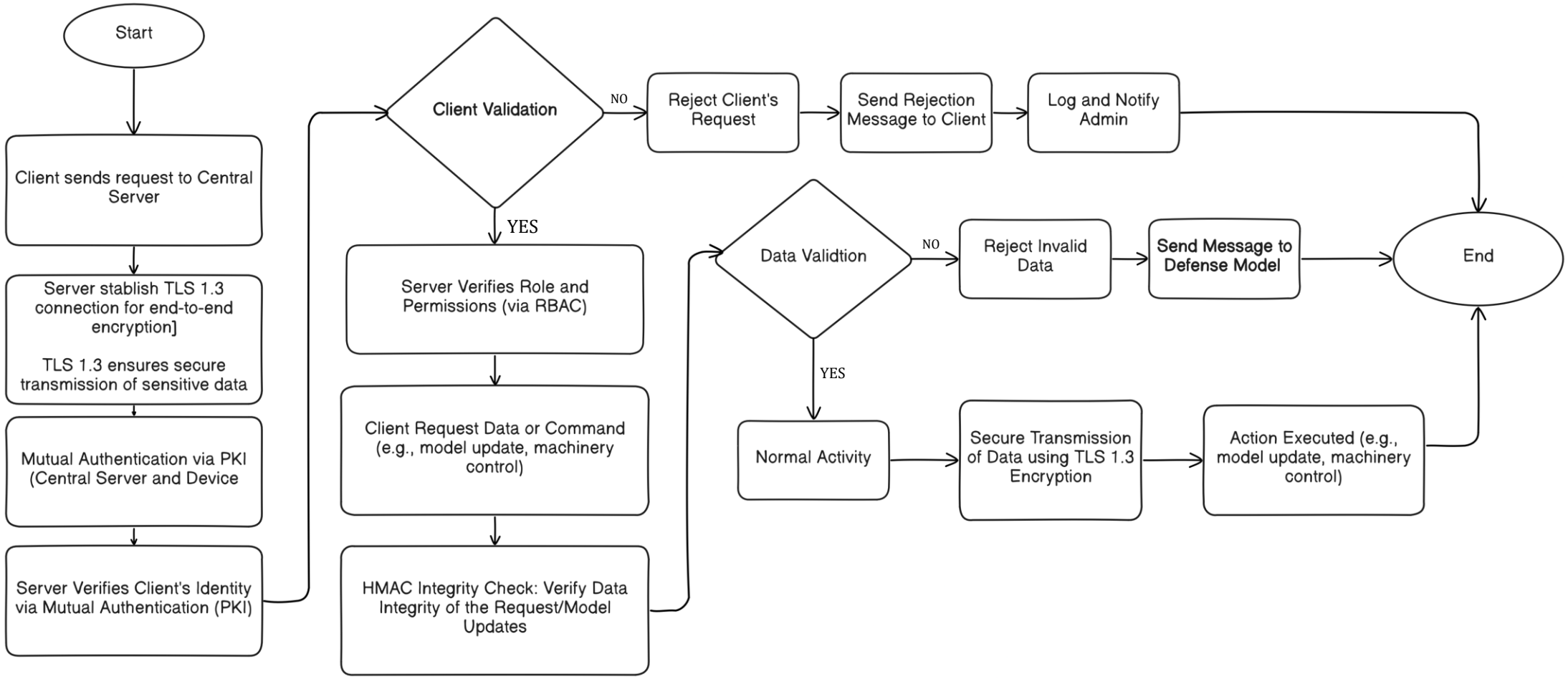
1. **Transport Layer Security (TLS) 1.3**:
    1. Encrypts communication with **Perfect Forward Secrecy (PFS)**.
    2. Ensures **mutual authentication** between client and server.
2. **Hash-Based Message Authentication Code (HMAC)**:
    1. Verifies data integrity using a cryptographic hash.
    2. Ensures that messages have not been altered during transmission.

System Architecture



Dissanayaka K.D.A.R.: Secure Command and Control (C2).

Component Process



Functional and non-functional requirements

Functional requirements

Authentication and Authorization - Implement TLS 1.3 for mutual authentication between devices and the central server.

Data Integrity - Use HMAC (Hash-based Message Authentication Code) to verify the integrity of commands and updates.

Secure Communication - Establish encrypted communication channels using end-to-end encryption to prevent unauthorized access.

Real-time Threat Monitoring - Integrate anomaly detection mechanisms to monitor communication patterns and flag suspicious activities.

Command Execution Feedback - Provide secure, encrypted feedback to devices after executing commands.

Non-functional requirements

Scalability - The system should support hundreds or thousands of IIOT devices without significant performance degradation.

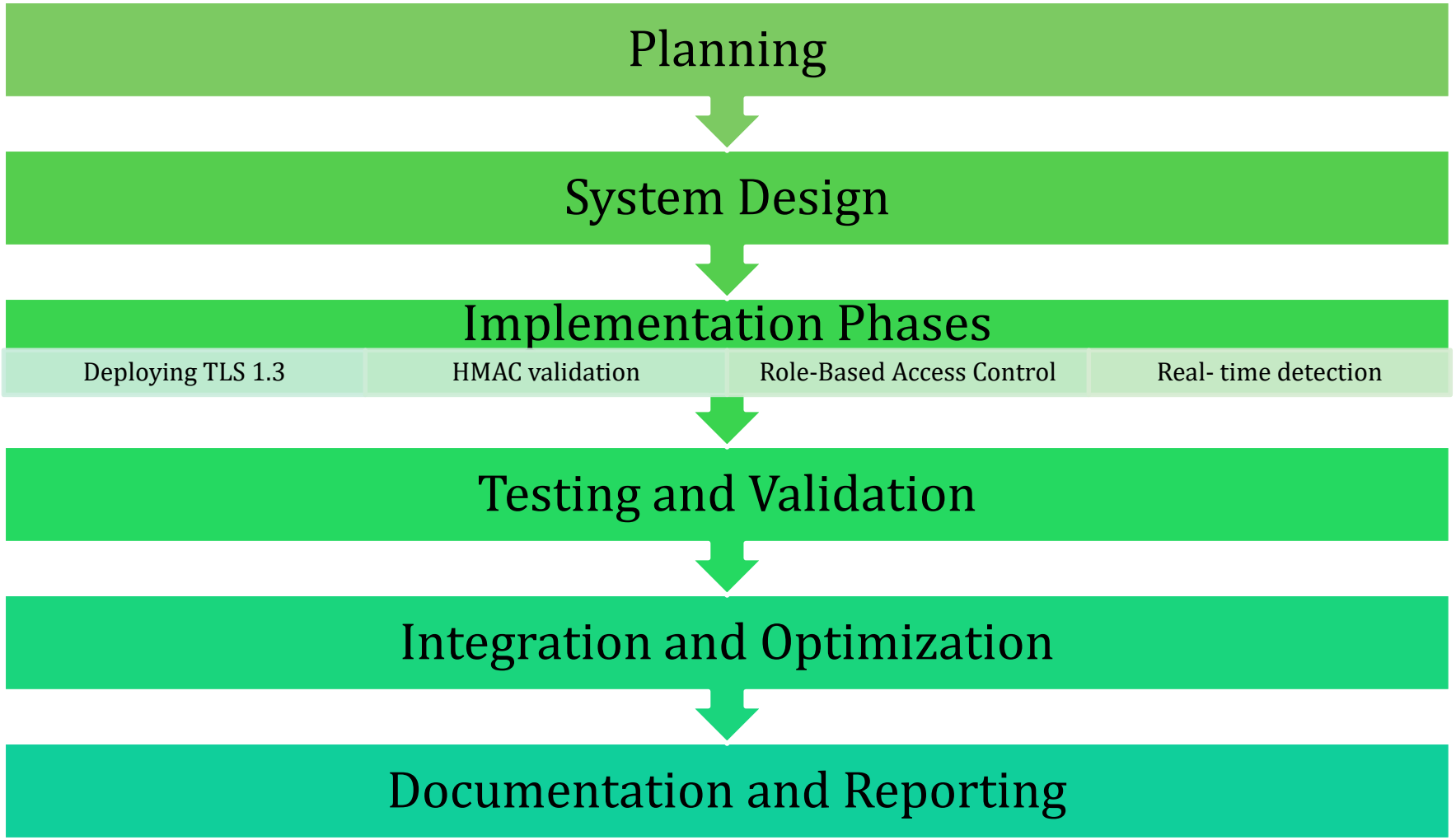
Efficiency - Ensure low latency in command transmission and execution, suitable for real-time operations.

Resource Optimization - Use lightweight cryptographic protocols and algorithms to ensure compatibility with resource-constrained devices.

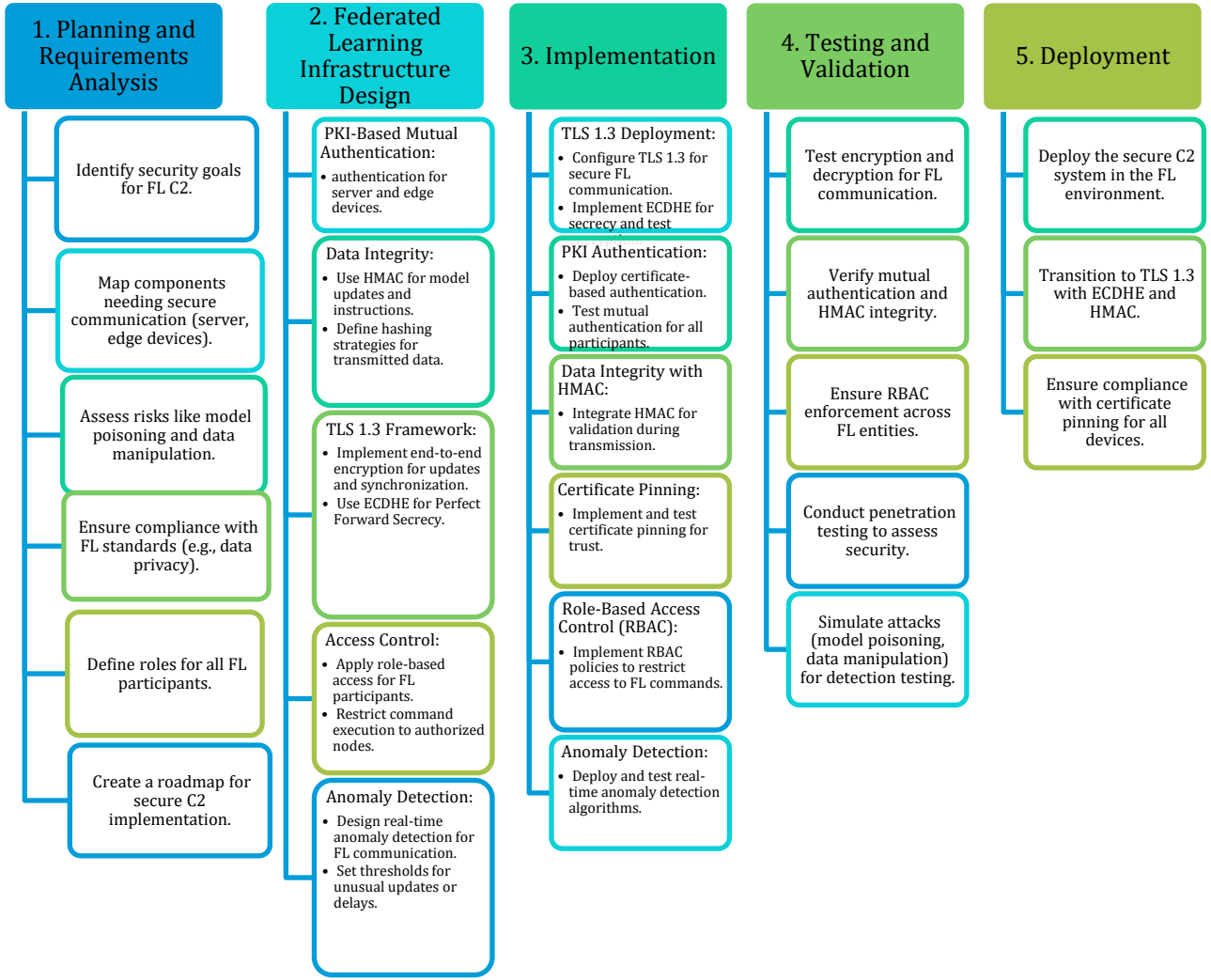
Interoperability - Support common IIOT communication protocols like MQTT and CoAP for broad compatibility.

Resilience - Ensure the system can withstand attacks like man-in-the-middle (MitM), replay, and Denial of Service (DoS).

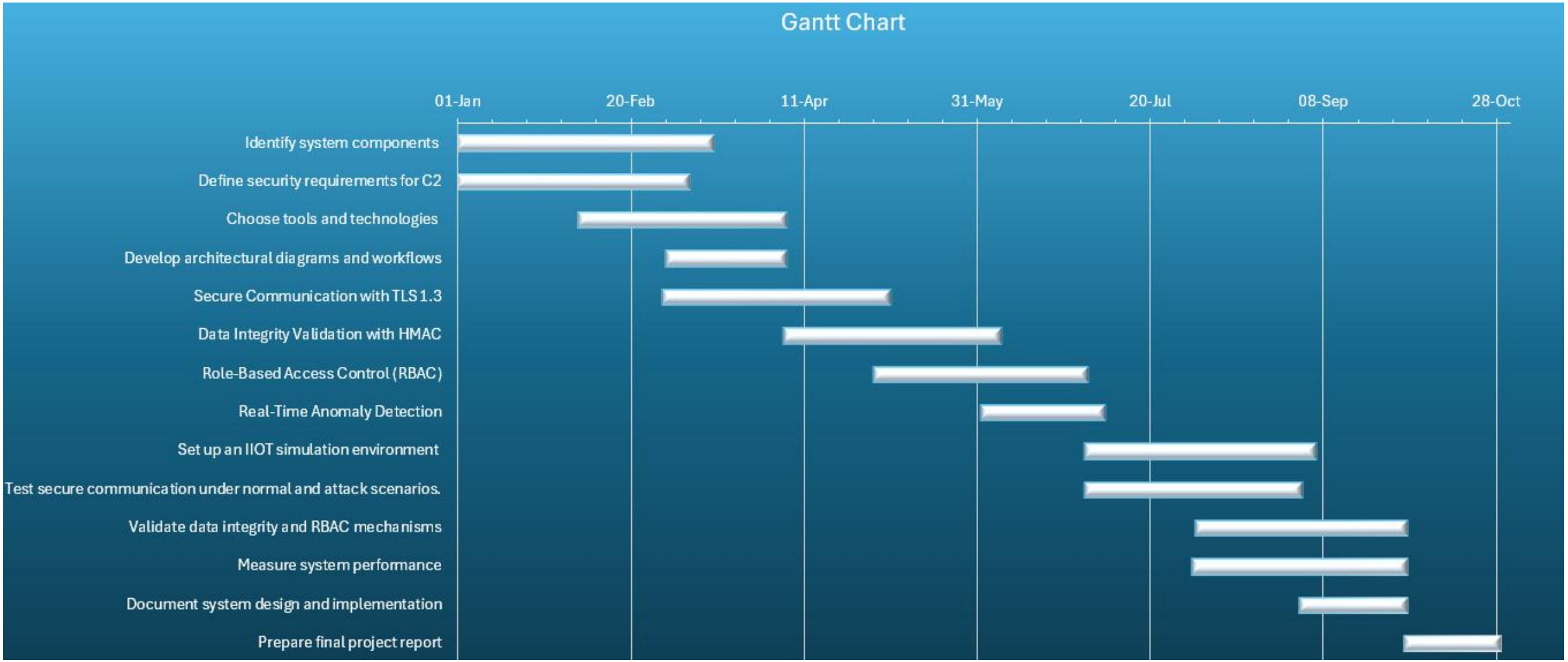
Methodology



Work breakdown structure



Gantt chart


Gantt Chart
01-Jan
20-Feb
11-Apr
31-May
20-Jul
08-Sep
28-Oct
Identify system components
Define security requirements for C2
Choose tools and technologies
Develop architectural diagrams and workflows
Secure Communication with TLS 1.3
Data Integrity Validation with HMAC
Role-Based Access Control (RBAC)
Real-Time Anomaly Detection
Set up an IIOT simulation environment
Test secure communication under normal and attack scenarios.
Validate data integrity and RBAC mechanisms
Measure system performance
Document system design and implementation
Prepare final project report

References

[1] P. Kairouz, "Advances and Open Problems in Federated Learning." Foundations and Trends® in Machine Learning," 2021.

[2] P. Sharma, "Towards Secure Federated Learning: A Review of Threats and Mitigations." Journal of IoT and Security," 2022.

[3] K. Elmazi, "A survey on fault detection in industrial IoT: A machine learning approach with emphasis on federated learning and intrusion detection systems," 2024.

[4] A. Hussain, "Ensuring zero trust IoT data privacy: Differential privacy in blockchain using federated learning," 2025.

[5] S. Ali, "Blockchain and federated learning-based intrusion detection for edge-enabled industrial IoT networks: A survey," 2023.

[6] A. M. Noble Kumari, "A comprehensive and critical analysis of TLS 1.3," *nformation and Optimization Sciences,* 2022.

[7] P. V. Mahima Mary Mathews, "Date time keyed - HMAC," *Online International Conference on Green Engineering and Technologie,* 2016.

[8] H. M. Ryan Ausanka-Crues, *Methods for Access Control : Advances and Limitations,* 2006.

[9] R. S. P. S. G. K. Kumar, "International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS)," *Advancing Industrial Cybersecurity: Machine Learning-Based Detection and Mitigation of IIoT Attacks,* 2024.

[10] M. A. K. K. Abuhasel, "A Secure Industrial Internet of Things (IIoT) Framework for Resource Management in Smart Manufacturing," 2020.

[11] R. K. A. K. P. Brett Glendenning, "Ziggurat: A Framework for Providing Scalability and Security in IoT Blockchains," *International Conference on Computational Science and Computational Intelligence (CSCI),* 2021.

Expected Outcomes

Full Adaptable Security Framework for FL in IIoT

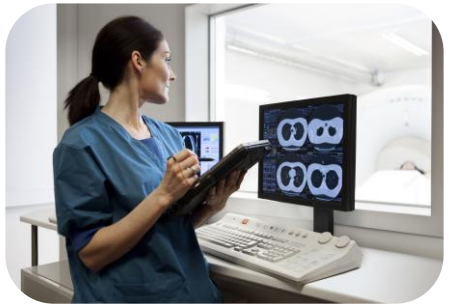
- Enhanced Attack Resilience
- Adaptive Security Measures
- Real-Time Performance
- Heterogeneity Support
- Improved Data Privacy

Commercialization

Target Industries

Manufacturing

Energy



Healthcare

Automobile

Market Differentiators

- Real-time threat detection and mitigation.
- Adaptability to diverse industries and dynamic attack patterns.
- Easy integration with existing IIoT infrastructures.

Business Models

As a SaaS Model or Enterprise Solutions.

Q & A

Thank you