Compliance Project Report 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
Mendis H.R.M	IT21822612
Weerasinghe K.M	IT21831904
Dissanayaka K.D.A.R. A	IT21828348

Supervisor: Mr. Amila Seneratha

Co-Supervisor: Mr. Tharaniyawarma Kumaralingam

Date of Submission: 2025

Compliance Project Report

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

Date: 27th October 2025

Project Supervisor: Mr. Amila Senerathana

Project Co-supervisor: Mr. Tharaniyawarma Kumaralingam

1. Project Overview:

What is this document for

The Compliance - Project's goal is to **evaluate and enhance the organization's compliance with regulations and policies**. This involves reviewing current practices, spotting non-compliance or improvement areas, and suggesting necessary improvements. This is essential for **maintaining legal operations, reducing compliance risks, and fostering a compliance culture** across the entire organization.

About the Project

This research project focuses on developing a **Data-privacy based Federated Learning (FL) Framework specifically for Industrial IoT (IIoT)** environments. The primary goal is to create a novel, integrated framework that addresses the unique challenges of IIoT by enhancing **data privacy** and **cybersecurity** while ensuring efficient operation. The framework achieves this by combining a multi-layered security architecture (Differential Privacy, Homomorphic Encryption) with robust attack defense and resource-efficient protocols. The project is essential for enabling secure and collaborative machine learning model training across distributed industrial devices.

2. Project Status:

- ❑ Completed

3. Key Milestones:

- **Milestone 1: Foundational Research and System Design** completed, including the selection of core privacy (DP, HE) and security (Secure Aggregation) techniques.
- **Milestone 2: Secure Communication and Protocol Enforcement Module (SCPM)** developed to establish mutual authentication and a trustworthy communication channel for IIoT.
- **Milestone 3: Attack Detection and Resilience Module (ADRM)** finalized, enabling the identification and isolation of clients involved in Byzantine and model poisoning attacks.

- **Milestone 4: Privacy Preservation Module (PPM)** integrated, utilizing **Differential Privacy (DP)** and **Homomorphic Encryption (HE)** to protect data and model updates.
- **Milestone 5: Secure Aggregation Module (SAM)** fully implemented using **Shamir's Secret Sharing** to ensure model update privacy and resilience to client dropouts.
- **Milestone 6: Efficient System Design** completed, incorporating techniques like **quantization** and hierarchical **architecture** to optimize communication and computation for IIoT devices.
- **Milestone 7: Experimental Setup and Data Acquisition** finalized using real-world IIoT datasets for framework validation.
- **Milestone 8: Performance and Security Validation conducted**, rigorously testing the framework's effectiveness in security, privacy, accuracy, and efficiency.
- **Milestone 9: Results Analysis and Discussion** completed, documenting the findings on attack resilience and cryptographic overhead.
- **Milestone 10: Final Research Paper Completed** and submitted, detailing the comprehensive, integrated Federated Learning framework.

4. Project Findings:

- **Compliance Gap Analysis:**

Identified several areas where current practices do not fully meet regulatory requirements.

- **Risk Assessment:**

Identified high-risk areas requiring immediate attention, including data protection and financial reporting.

- **Training Needs:**

Identified a need for enhanced compliance training programs for employees.

- **Documentation Review:**

Found inconsistencies in compliance documentation and recommended a centralized document management system.

- **Monitoring and Reporting:**

Identified gaps in monitoring and reporting mechanisms, suggesting the implementation of automated tools for better tracking.

5. Compliance Recommendations:

- **Enhanced Training Programs:**

Develop and implement comprehensive compliance training programs for all employees, focusing on areas of non-compliance and high-risk activities.

- **Policy and Procedure Updates:**

Review and update existing compliance policies and procedures to reflect current regulatory requirements and organizational practices.

- **Document Management System:**

Implement a centralized document management system to ensure consistent and accurate record-keeping of compliance-related documents.

- **Monitoring and Reporting Tools:**

Invest in automated tools for monitoring and reporting compliance activities to enhance visibility and accountability.

- **Regular Compliance Audits:**

Conduct regular compliance audits to identify and address any new compliance risks or issues.

6. Next Steps:

- **Implementation Plan:**

Develop a detailed implementation plan for the recommended actions, including timelines, responsible parties, and resources required.

- **Training Rollout:**

Begin rollout of enhanced compliance training programs, starting with high-risk areas and key personnel.

- **Policy Updates:**

Review and update compliance policies and procedures in line with the recommendations, ensuring alignment with regulatory requirements.

- **Document Management System Implementation:**

Initiate the implementation of a centralized document management system, starting with the migration of existing documents.

- **Monitoring and Reporting Tools Implementation:**

Identify and implement suitable automated tools for monitoring and reporting compliance activities.

- **Compliance Audit Schedule:**

Establish a regular schedule for compliance audits and assign responsibilities for conducting them.

- **Stakeholder Communication:**

Communicate with the findings, recommendations, and next steps to all stakeholders, ensuring transparency and accountability.

9. Comments/Notes:

- It is crucial to ensure that all recommendations are implemented in a timely manner to enhance compliance and mitigate risks.
- Regular monitoring and reporting of compliance activities are essential to track progress and identify any new compliance issues.
- Stakeholder engagement and communication are key to the success of the compliance project.
- Continuous review and updating of compliance policies and procedures are necessary to adapt to changing regulatory requirements and business practices.
- Training programs should be tailored to the specific needs of different departments and roles within the organization.

10. Approval:

- ❑ Approved
- ❑ Not Approved

22nd October 2025