

# **Data-Privacy Focused Federated Learning Framework for Industrial IoT**

*Component 02 - Privacy Preservation*

R25-039

Project Proposal Report

*Mendis H.R.M - IT21822612*

Supervisor - *Dr. Sanika Wijesekara*

Co-Supervisor - *Mr. Tharaniyawarma Kumaralingam*

B.Sc. (Hons) Degree in Information Technology Specialized in Cyber Security

Department of Computer Systems and Engineering

Sri Lanka Institute of Information Technology


Sri Lanka

January 2025

**DECLARATOIN OF CANDIDATE AND STATEMENT BY SUPERVISOR**

I declare that this is our own work, and this proposal does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any other university or institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to Sri Lanka Institute of Information Technology the nonexclusive right to reproduce and distribute my dissertation, in whole or in part of print, electronic or other medium. I retain the right to use this context as a whole or part in future works (such as articles or books)

Member Name	Registration Number	Signature	Date
Mendis H.R.M	IT21822612		

The candidate above is carrying out research for the undergraduate dissertation under supervision of the undersigned.

Name	Role	Signature	Date
Dr. Sanika Wijesekara	Supervisor		
Mr. Tharaniyawarma Kumaralingam	Co-Supervisor		

## ABSTRACT

With the rapid stride in IIoT, there has been tremendous growth in gathering and transmitting sensitive data across different devices and networks. Since IIoT systems now form part of the core infrastructures, privacy and security of data have become very important. This study looks at the main concepts of privacy-enhancing techniques, focusing on Differential Privacy and Homomorphic Encryption, and how these methods can be integrated into IIoT systems. The paper highlights the main challenges in developing scalable, efficient, and robust privacy solutions for such systems, while also considering the trade-offs between privacy protection and system performance. Though a number of technologies on privacy protection are proposed, this research finds some important gaps: missing hybrid privacy solutions, challenges in the implementation of these solutions in real-world scenarios, and generally a lack of large-scale IIoT datasets for testing purposes from a privacy perspective. It proposes new solutions to bridge these gaps with the aim of developing a framework that integrates DP and HE techniques for enhancing data privacy without sacrificing performance in IIoT applications. Moreover, it also investigates compliance with existing privacy regulations and resilience against potential privacy attacks.

## **CONTENTS**

1	INTRODUCTION .....	4
1.1	Background Study .....	5
1.2	Literature Review .....	5
1.3	Research Gap.....	7
1.4	Research Problem.....	8
2	RESEARCH OBJECTIVES.....	8
2.1	Main Objective.....	8
2.2	Sub Objective .....	9
	METHODOLOGY .....	10
2.3	System Diagram .....	10
2.4	Systems requirements.....	13
2.5	Workload allocation .....	13
2.5.1	Work Breakdown Structure .....	13
2.5.2	Gantt Chart .....	14
2.6	Commercialization of the product.....	14
3	SOFTWARE SPECIFICATIONS.....	15
3.1	User Requirements .....	15
3.2	Functional Requirements.....	15
3.3	Non-functional requirements.....	15
4	References .....	16
5	APPENDICES .....	18

## 1 INTRODUCTION

## 1.1 Background Study

The Industrial Internet of Things is the revolution of industrials in interconnecting sensors, devices, and machinery for increased productivity and efficiency. However, with the integration of IIoT systems, especially in managing huge amounts of sensitive data generated by industrial devices, several challenges arise. Traditional centralized machine learning systems gather data from devices for model training. but this approach has significant drawbacks, including:

**Data Privacy Risks:** Centralized data collection is prone to breaches or misuse of sensitive industrial information.

**Scalability Issues:** Network transfer of large datasets will introduce latency and bandwidth problems.

**Regulatory Compliance:** Regulations such as GDPR and CCPA demand strict data protection, which cannot be provided by a centralized solution for sensitive IIoT applications.

Federated learning basically decentralizes model training. While keeping the data on the devices, it shares only the model updates with the central server, say gradients. This reduces the risk of privacy along with bandwidth conservations. FL is not resistant to threats against privacy. Sensitive information can be compromised during model updates through gradient leakage or adversarial attacks.

Such risks can be mitigated by the employment of some privacy-preserving techniques: **Differential Privacy and Homomorphic Encryption.** DP allows obfuscation of every individual's data contribution by adding noise in model updates, while HE enables computations on encrypted data and hence ensures privacy throughout the aggregation. This work integrates these techniques into a federated learning framework optimized for IIoT applications to ensure secure and efficient decentralized learning.

## 1.2 Literature Review

The increasing adoption of the Industrial Internet of Things (IIoT) has brought significant advancements in automation, data-driven decision-making, and predictive analytics. However, it has also introduced critical risk related to data privacy and security in distributed environments.

The Federated Learning (FL) approach has gained attention as a potential solution, but it still faces significant privacy and security issues.

### **Differential Privacy in Federated Learning**

Among the many techniques developed for privacy preservation in machine learning, differential privacy has emerged as a popular approach. It injects controlled noise into data or model gradients to minimize the likelihood of any information being leaked. [1] However, such effectiveness often comes at the cost of model performance, as noise reduces accuracy. This can be a challenging trade-off in IIoT environments, where high precision is critical for making appropriate decisions.

### **Homomorphic Encryption for Secure Computation**

Homomorphic encryption enables different kinds of computations on encrypted data without decryption, hence preserving privacy throughout the process. While fully homomorphic encryption guarantees strong privacy, computational cost is prohibitively expensive for real-time applications. Partial and leveled homomorphic encryption schemes provide a better trade-off between security and computational efficiency for IIoT use cases. [2]

### **Hybrid Approaches: Differential Privacy and Homomorphic Encryption Combined**

Recent developments indeed point toward the combination of DP and HE to overcome individual weaknesses. Whereas DP provides privacy through the addition of noise, HE offers security during computation over encrypted data. [3] Hybrid solutions have achieved a certain balance between model performance and privacy. However, scalability, resource constraints, and resilience against sophisticated attacks are within the scope of current research.

### **Privacy and Security in IIoT**

Moreover, heterogeneity and resource-constrained nature of IIoT devices add to the complexity of implementing techniques preserving privacy. Scaled cryptographic methods with lightweight frameworks are required for ensuring privacy and security in ways that do not degrade performance. [4] Effective mechanisms of preserving privacy must meet the dynamic and large-scale natures of IIoT networks.

### **Comparison with existing Architecture**

Feature	Centralized Learning	Decentralized Learning	Standard Federated Learning	Proposed Secure Federated Learning
---------	----------------------	------------------------	-----------------------------	------------------------------------

<b>Data Privacy</b>	High risk (raw data shared)	Moderate risk (peer-to-peer sharing)	Improved privacy (local training)	Enhanced (Homomorphic Encryption + Differential Privacy)
<b>Security Against Attacks</b>	Vulnerable to data breaches	Susceptible to poisoning attacks	Limited security (basic encryption)	Robust (defense against gradient inversion, poisoning, and inference attacks)
<b>Communication Overhead</b>	High (all data transmitted)	High (frequent model updates)	Lower (only model updates sent)	Optimized (secure aggregation with reduced overhead)
<b>Computational Cost</b>	Moderate	High (due to multiple communication rounds)	Low to moderate	Optimized (efficient encryption and aggregation schemes)
<b>Scalability</b>	Low (central bottleneck)	Moderate	High (supports multiple clients)	High (secure, efficient, and scalable for IIoT applications)

### 1.3 Research Gap

FL has shown great potential in addressing privacy and scalability issues in IIoT, however there are still several important research needs, including [5] [2] [1]:

Research Problem	Gaps Identified
Lack of efficient privacy-preserving techniques in IIoT	Limited research on hybrid approaches combining Differential Privacy (DP) and Homomorphic Encryption (HE) in IIoT systems.

Trade-off between privacy and performance in IIoT	Insufficient exploration of the trade-off between privacy (DP, HE) and system performance (e.g., latency, computational cost).
Inadequate privacy audits in IIoT	Lack of comprehensive post-implementation privacy audits in IIoT systems to ensure compliance with data protection standards.
Integration of DP and HE techniques in IIoT systems	Limited real-world integration and performance evaluation of DP and HE techniques together in IIoT environments.
Privacy-preserving mechanisms under attack scenarios	Insufficient research on the robustness of privacy-preserving techniques against potential attacks (e.g., model inversion).
Lack of benchmark datasets for IIoT privacy research	Scarcity of large-scale, public datasets specifically for evaluating privacy-preserving techniques in IIoT systems.

## 1.4 Research Problem

IIoT systems generate sensitive data that should not be exposed or misused. FL provides a decentralized approach to the training of machine learning models without transferring raw data. However, most of the existing frameworks are vulnerable to different kinds of privacy threats, such as gradient leakage and adversarial attacks. Besides, the high computational overhead of privacy-preserving techniques like HE, and the accuracy degradation caused by DP further hinder their practical adoption in IIoT environments.

## 2 RESEARCH OBJECTIVES

### 2.1 Main Objective

The main objective is to develop a **privacy-preserving Federated Learning (FL) framework for Industrial IoT (IIoT)** that enhances security against gradient leakage and adversarial attacks while maintaining computational efficiency. This is achieved by integrating **Homomorphic Encryption (HE) and Differential Privacy (DP)** to protect sensitive data and ensure robust model training without significant performance trade-offs.



## 2.2 Sub Objective

- **Design and implement mechanisms for Differential Privacy:**

Integrate DP for obfuscation of sensitive information by individual IIoT devices on gradient updates and mitigate the associated risks of data leakage.

- **Incorporate Homomorphic Encryption for secure computations:**

Leverage HE to enable computations on encrypted data during the process of aggregation and prevent sensitive data exposure with guaranteed model accuracy.

- **Conduct privacy audits and threat evaluations**

Validate the framework privacy guarantees through rigorous audits and its resilience against various inference and reconstruction attacks.

- **trade-off the model performance with privacy optimally**

Investigate and fine-tune parameters of DP and HE towards the optimal trade-off between robust privacy and high model accuracy.

- **Develop a Lightweight Framework for IIoT Systems**

Ensure the proposed framework is resource-efficient, scalable, and adaptable to the computational constraints of IIoT environments. Test the framework with real-world IIoT datasets

## METHODOLOGY

### 2.3 System Diagram

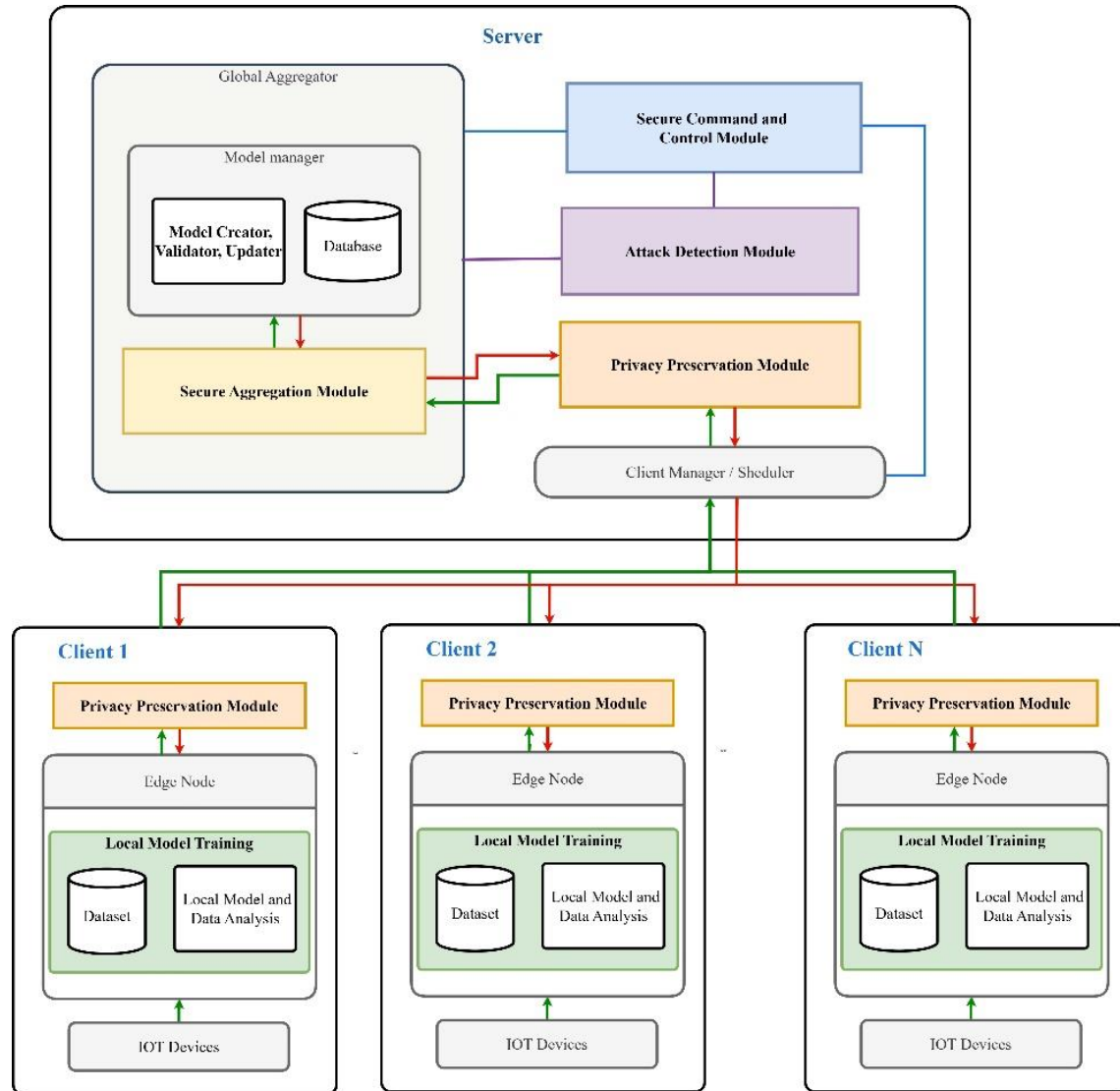


Figure 1 Federated Learning Framework

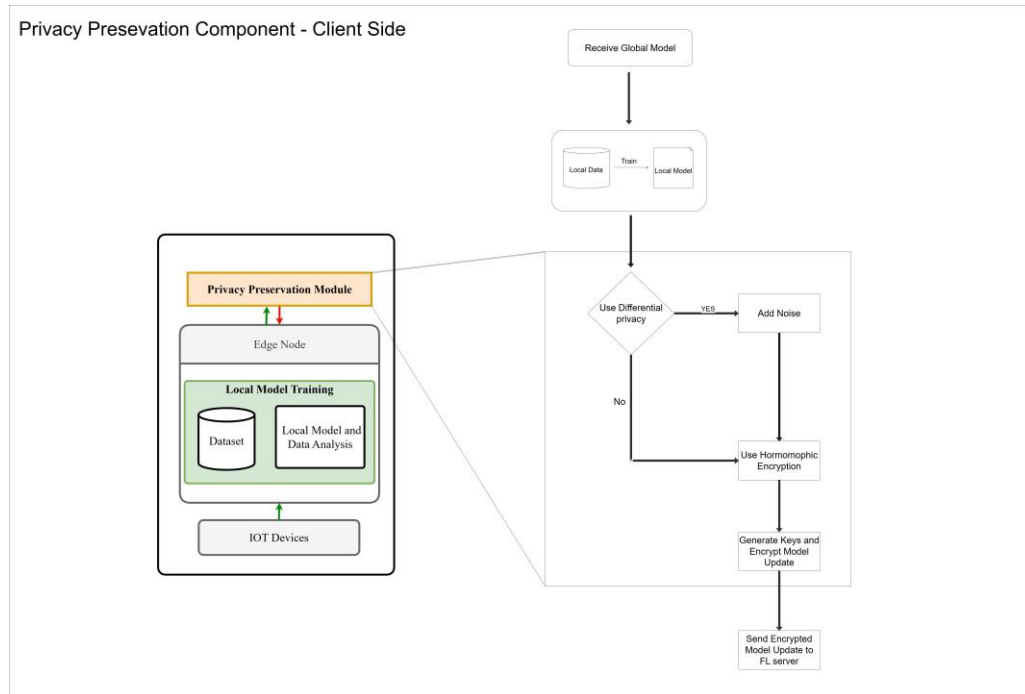


Figure 2: Privacy Preservation - Client Side

1. **Receive the Global Model** – The client waits for the latest global model from the Federated Learning server.
2. **Train on Local Data** – The client trains the model using its own dataset on its edge node, ensuring data privacy.
3. **Apply Differential Privacy (Optional)** – The user/system decides whether to add noise to protect individual data points.
4. **Encrypt the Model Update** – The trained model update is encrypted for security.
5. **Send to Server** – The encrypted update is sent back to the server, which aggregates updates from multiple clients to improve the global model.

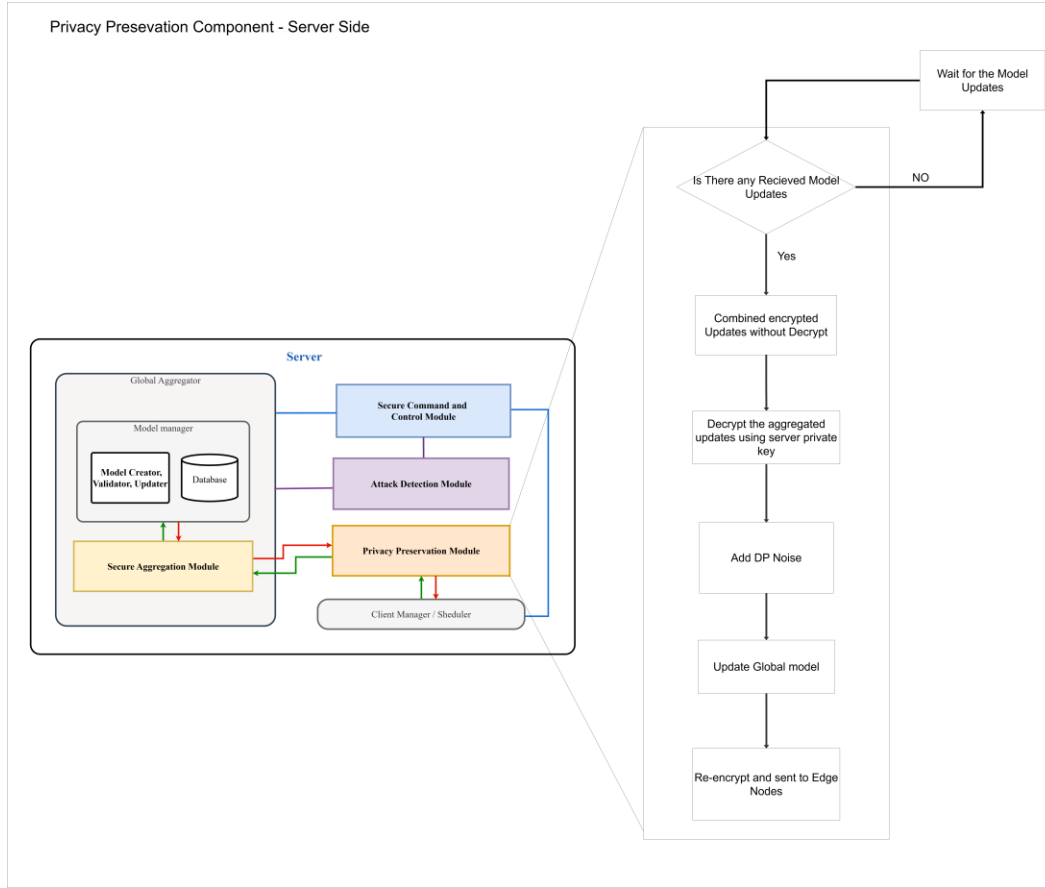


Figure 3: Privacy Preservation - Server Side

1. **Receive Model Updates** – The server waits for encrypted model updates from edge devices.
2. **Aggregate Encrypted Updates** – It combines received updates without decryption, ensuring privacy.
3. **Decrypt Aggregated Updates** – The server decrypts the combined updates using its private key, preventing identification of individual node contributions.
4. **Apply Differential Privacy** – Noise is added to enhance data protection before updating the global model.
5. **Update and Distribute** – The updated global model is re-encrypted and sent back to nodes for the next training round.

## 2.4 Systems requirements

- Hardware: Computational power, if external hardware needed (Raspberry Pi)
- Software: Python, TensorFlow, libraries and other related tools.
- Resources: simulation tools for IIoT scenarios.

## 2.5 Workload allocation

### 2.5.1 Work Breakdown Structure

Task	start date	end date	duration	Phase
Conduct a literature review on DP and HE	01-Jan	01-Mar	60	Phase 1 - Research and Design
Analyze privacy requirements in IIoT	01-Jan	01-Mar	60	
Design hybrid privacy model using DP and HE	01-Feb	01-Apr	60	
Developing a system architecture	01-Mar	01-Apr	32	
Implement differential privacy mechanisms	01-Mar	01-May	62	Phase 2 - Implementation
Implement homomorphic encryption methods	01-Apr	01-Jun	62	
Integrate DP and HE into the system	01-May	01-Jul	62	
Conduct unit testing on privacy modules	01-Jun	01-Jul	31	
Conduct privacy audits	01-Jul	01-Sep	63	Phase 3 -Evaluation and Testing
Evaluate model performance vs privacy trade-off	01-Jul	01-Sep	63	
Test scalability and performance under IIoT settings	01-Aug	01-Oct	62	
Optimize hybrid framework for IIoT	01-Aug	01-Oct	62	
Document system design and implementation	01-Sep	01-Oct	31	Phase 4 - Documentation and Finalization
Prepare final project report	01-Oct	01-Nov	32	

## 2.5.2 Gantt Chart

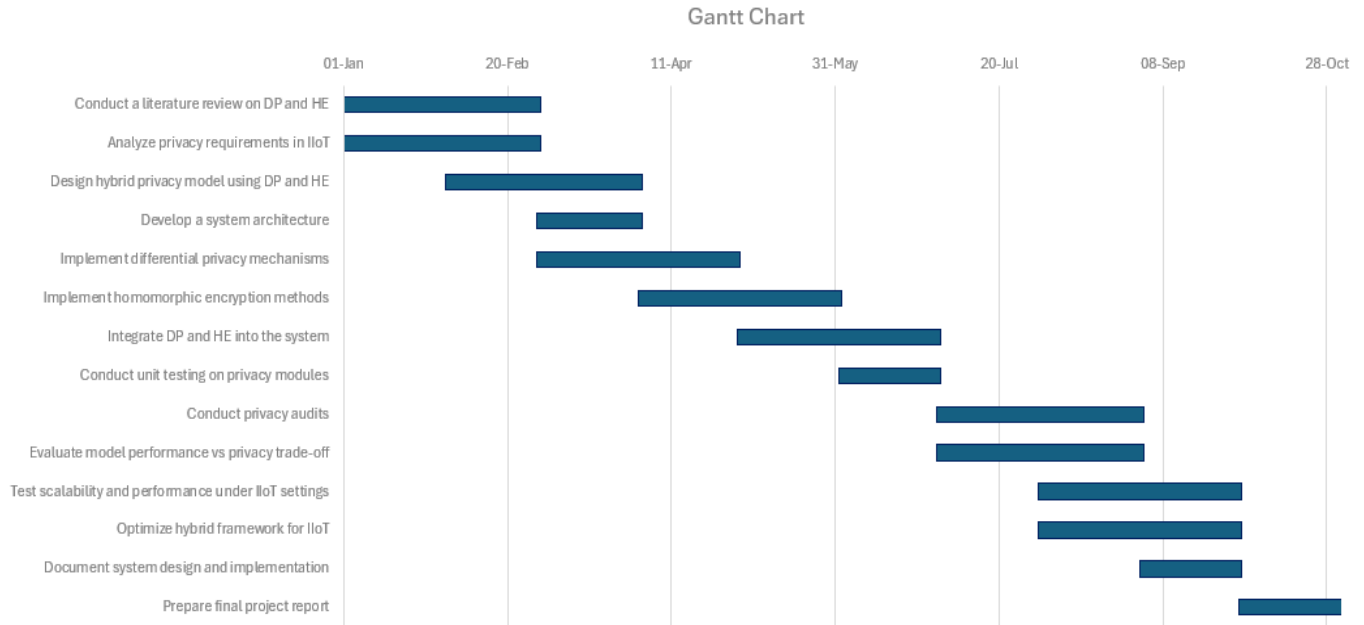


Figure 4: Gantt Chart

## 2.6 Commercialization of the product

The proposed privacy-preserving federated learning framework in Industrial Internet of Things environments has the capability to be commercialized. The following is a detailed outline of its aspects relating to commercialization:

### Target Market

The framework shall target the following industries and sectors:

**Industrial IoT Companies:** Those organizations seeking secure and efficient data-sharing solutions for industrial applications.

**Key Industries:** Sectors like healthcare, manufacturing, and smart grids that emphasize data privacy and security in their operations.

Our framework provides a secure, efficient, and scalable FL model. The business model includes a SaaS subscription, enterprise licensing for large-scale on-premises deployments (custom pricing).

## 3 SOFTWARE SPECIFICATIONS

### 3.1 User Requirements

- **Privacy Protection for IIoT Data:** The system must guarantee that sensitive data generated by IIoT devices (e.g., temperature, pressure, sensor data) is kept private and cannot be accessed or reconstructed by unauthorized users.
- **User Control Over Privacy Settings:** Provide administrators with control over privacy parameters, such as the amount of noise added in Differential Privacy and the choice of encryption methods for Homomorphic Encryption.
- **Transparent Privacy Auditing:** Provide administrators with tools to perform periodic checks on privacy leakage risks and the effectiveness of privacy-preserving measures.
- **Minimal Impact on IIoT Device Performance:** Minimal Impact on IIoT Device Performance
- **Easy-to-Use Interface for Configuration:** Provide a simple, intuitive interface that allows users to easily configure privacy parameters, such as choosing between different privacy algorithms or encryption levels, without requiring deep technical expertise.

### 3.2 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.

### 3.3 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.

## 4 References



- [1] 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.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] Anwar, Sayeda and , Asaduzzaman and Sarker, Iqbal, "A differential privacy aided DeepFed intrusion detection system for IoT applications," *SECURITY AND PRIVACY*, 07 2024.

## 5 APPENDICES

### Plagiarism check - Turnitin

#### About this page

This is your assignment dashboard. You can upload submissions for your assignment from here. When a submission has been processed you will be able to download a digital receipt, view any grades and similarity reports that have been made available by your instructor.

> [Research Paper Checking](#) ?

Paper Title	Uploaded	Grade	Similarity
<a href="#">PPReport - IT21822612 - Privacy Preservation.pdf</a>	02 Feb 2025 22:47	--	<div><div></div></div> 14% <a href="#">↑</a> <a href="#">↓</a> <a href="#">⋮</a>