

Data-Privacy Focused Federated Learning Framework for Industrial IoT

Component 03 - Secure Aggregation

R25-039

Project Proposal Report

Weerasinghe K.M - IT21831904

B.S.c (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 y the nonexclusive right to reproduce and distribute m y 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
Weerasinghe K.M.	IT21831904		1/23/2025

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

Name	Role
Dr. Sanika Wijesekara	Supervisor
Mr. Amila Senerathne	Supervisor
Mr. Tharaniyawarma Kumaralingam	Co-Supervisor

ABSTRACT

As the Industrial Internet of Things (IIoT) evolves, protecting data security and privacy in Federated Learning (FL) is still a major problem. FL makes it possible to train models in a decentralized manner without exchanging raw data, but the aggregation process still presents security and privacy issues. This research addresses issues including scalability, performance trade-offs, and adversarial attacks by investigating safe aggregation algorithms intended for IIoT contexts with limited resources. Utilizing privacy-preserving techniques and cryptographic methods to improve security while preserving efficiency is the main goal of the project. Developing a scalable and privacy-preserving FL architecture appropriate for IIoT applications is the goal of this project, which will assess the efficacy of secure aggregation techniques and their resistance to possible threats. The results will support secure decision-making in practical IIoT implementations, enhance model reliability, and reinforce data security.

CONTENTS

1	INTRODUCTION	6
1.1	Background Study	6
1.2	Literature Review	7
1.3	Research Gap.....	9
1.4	Research Problem	10
2	RESEARCH OBJECTIVES.....	11
2.1	Main Objective	11
2.2	Specific Objectives	11
3	METHODOLOGY	12
3.1	System Diagram	12
3.2	System Process	13
3.3	Individual component Diagram	14
3.4	Work Breakdown Structure	15
3.5	Gantt Chart	15
3.6	Expected Outcome.....	16
3.7	Commercialization of the product	16
4	PROJECT REQUIREMENTS	17
4.1	User Requirements	17
4.2	Functional Requirements.....	17
4.3	Nonfunctional requirements	17
4.4	Software requirements.....	17
5	REFERENCES	18

LIST OF FIGURES

Figure 1 proposed overall system architecture	12
Figure 2 system process	13
Figure 3 Proposed component architecture.....	14
Figure 4 Work breakdown Structure	15
Figure 5 Gantt Chart	15

LIST OF ABBREVIATIONS

Abbreviation	Full Form
FL	Federated Learning
IIoT	Industrial Internet of Things
ML	Machine Learning
AI	Artificial Intelligence
SMPC	Secure Multi-Party Computation
LWE	Learning with Errors
AutoGM	Auto-weighted Geometric Median
ELSA	Efficient Learning Secure Aggregation
DP	Differential Privacy
SAFE Learning	Secure Aggregation in Federated Learning

1 INTRODUCTION

1.1 Background Study

Concerns surrounding privacy and network security have greatly increased as a result of the Internet of Things (IoT) devices rapid development across various industries. Large-scale datasets are particularly helpful for models like deep neural networks, which have seen advancements in industries like computer vision and natural language processing due to Machine Learning (ML) [1]. It is commonly known that model efficiency improves with further training information. To train models on a single dataset and achieve better learning outcomes, centralized machine learning techniques are used to rely on gathering data from numerous distributed devices. Despite its effectiveness, this centralized design has dominated training techniques for decades and presents Risks.

Standard ML-based systems are Sensitive device and user information is susceptible to breaches, unauthorized access, and misuse during storage and transmission because systems, for example, gather data from devices throughout the network and process it on a central server. These privacy issues have grown more severe, particularly during the context of the Internet of Things, where devices produce vast amounts of distributed and sensitive data. In order to reduce these risks while preserving the efficacy of ML applications, research has recently shifted toward decentralized and privacy-preserving solutions like Federated Learning (FL) [2] [3].

Federated learning (FL) is a system where multiple users collaborate to solve machine learning issues, with a central aggregator directing the process. In this configuration, training data remains spread between devices to maintain privacy. FL provides cooperative training of models utilizing locally stored data from several data-owners. A central server administers a global model that is updated by local modifications provided by users. These changes are then pooled by the server to enhance the global model. Throughout the process, users don't exchange the data they provide with the server, just the local model changes [4] [5].

Secure Aggregation is a Secure Multi-Party Computation technique that allows a number of mutually wary parties, each with a private value, to collectively calculate an aggregate result, without disclosing their individual values. It guarantees that only the final aggregated result is made known, respecting the privacy of each participant's data. In the context of federated learning (FL), secure aggregation is a vital component that allows the server to calculate the global model by acquiring inputs from individuals without exposing their local models. These methods are especially developed to ensure user privacy by assuring that neither the server nor other participants can infer any information beyond the aggregated result [6] [7].

The term "Industrial Internet of Things (IIoT)" refers to the use of sensors and internet-connected devices in industrial settings to monitor and control operations, collect and exchange data, and enhance operational efficiency [8]. Devices such as sensors for tracking temperature, pressure, humidity, and other environmental factors have become essential tools in industries like manufacturing, transportation, energy, agriculture, and healthcare. By collecting and sharing real-

time data, IIoT devices enable enterprises to monitor operations, manage processes, and improve overall efficiency. Through advanced automation, intelligent decision-making, and optimized workflows, IIoT is transforming traditional industrial operations. This shift drives innovation by lowering costs, enhancing efficiency, improving product quality, and promoting worker safety, solidifying IIoT as a critical component of modern industrial practices [8]

1.2 Literature Review

Federated Learning (FL) has emerged as an alternative approach to enable collaborative machine learning while protecting user privacy. However, secure aggregation, which preserves the confidentiality of user inputs throughout the learning process, remains a critical challenge. Researchers have proposed numerous approaches leveraging cryptographic techniques, differential privacy, and resilient aggregation algorithms to solve issues including privacy vulnerabilities, backdoor attacks, and Byzantine failures. This section analyzes significant advances in secure aggregation for FL, highlighting innovative frameworks, their techniques, and contributions toward boosting security, efficiency, and scalability in privacy-sensitive applications.

The researchers **Timothy Stevens et al.** introduced a novel approach for secure aggregation in the study area of Federated learning, which addressed several of the privacy issues that related to standard ML models that were trained on sensitive user data. The researchers suggested a unique technique called *FLDP*, that combines Learning with errors (LWE) to increase the security and efficiency of federated learning systems. The proposed solution FLDP ensures the differential privacy of the trained model while not needing the trusted data aggregator. This solution reduces communication and computational costs when compared to current methods and provides a robust framework for secure aggregation that enhances scalability and maintains the model's accuracy without compromising the user Privacy. The contributions of the author contain the novel malicious secure aggregation protocol that performs better than the gradient aggregation with differential privacy, End-to-End protocol designed for privacy preserving FL and empirical validations with high accuracy on datasets [9].

The *ELSA protocol* presented by the researchers **Rathee et al.** addresses some of the significant challenges in secure aggregation for federated learning. ELSA is a protocol that uses a dual-server design to ensure client privacy, lowering the chance of server intrusions. It uses a client-driven method, eliminating communication overhead and improving the aggregate process. ELSA additionally identifies and mitigates rogue clients, boosting security. With only a minor increase in runtime and negligible additional communication costs, it surpasses earlier protocols, making it a highly efficient alternative for large-scale federated learning. It also has a bandwidth-saver mode for bandwidth-constrained environments. ELSA effectively achieves a balance between security and efficiency, marking a significant breakthrough in secure aggregation for federated learning. Its novel architecture makes it an appealing option for machine learning applications that are concerned about privacy [10].

The researchers **Pierre Sanon et al.** explore a novel approach to secure aggregation in federated learning by combining the *secure multi-party computation (SMPC)* and *homomorphic encryption* which aims to the security and privacy in machine learning in the applications of forecast network traffic. The framework secures sensitive data throughout the aggregation process by using homomorphic encryption, especially the CKKS technique. Additionally, the authors present Secure Multi-Party Computation (SMPC) methods that aggregate encrypted model updates while enabling various clients to use separate private keys. Model weights are encrypted, noise is added, the output is decrypted, and then it is encrypted again as part of the aggregation process. The technique's efficiency in vulnerable applications is demonstrated by evaluating it using simulated data from a 5G network environment. This technique improves safeguards against possible adverse threats. The results of this study open the door for wider adoption in practical applications by providing insightful information about how federated learning can be used successfully in privacy-sensitive sectors.

Shenghui Li et al. address the challenge of ensuring safe and reliable aggregation in federated learning (FL) within Industrial Internet of Things (IIoT) contexts. To enhance resilience against Byzantine failures, including model and data poisoning attacks, they propose *Auto-weighted Geometric Median (AutoGM)*, a robust aggregation algorithm designed to handle outliers and ensure accurate global model updates. The authors develop an alternating optimization approach to compute AutoGM efficiently. They introduce two federated learning solutions: AutoGM_FL, which trains a shared global model, and AutoGM_PFL, which focuses on personalized federated learning. Both solutions demonstrate strong defenses against poisoning attacks while maintaining high efficiency. [11].

Mohamad Mansouri et al. examine secure aggregation in federated learning, proposing a definition to ensure confidentiality while enabling aggregate computations. They categorize existing solutions based on cryptographic primitives and evaluate 37 schemes using techniques like additive homomorphic encryption and functional encryption. Challenges include client failures, scalability, malicious actors, and statistical attacks that compromise privacy. The authors emphasize the need to balance security and performance for practical implementation in federate learning, emphasizing the importance of cryptographic techniques in protecting sensitive data [12].

The *SAFE Learning protocol*, introduced by **Zhuosheng Zhang et al.**, addresses backdoor vulnerabilities in federated learning (FL) under secure aggregation. They combined techniques like Obvious Random Grouping and Partial Parameter Disclosure to prevent malicious collaboration and enable secure anomaly detection. By identifying backdoors and reducing their impact on model accuracy without significantly affecting task performance, SAFE Learning demonstrates resilience against adversarial attacks. Extensive experiments validate its efficiency and practicality, making it a robust solution for real-world FL applications [13].

In conclusion, Secure aggregation is an essential element of privacy-preserving federated learning, tackling issues such as privacy shortcomings, adversarial threats, and scalability. The evaluated

methodologies, *including FLDP, ELSA, and AutoGM*, demonstrate considerable progress in improving privacy, efficiency, and resilience. Methods like homomorphic encryption, secure multi-party computation, and anomaly detection enhance the security of federated learning systems. These solutions emphasize the capability of secure aggregation for promoting privacy-sensitive applications, establishing a robust basis for the progression of federated learning in practical contexts.

1.3 Research Gap

Worked by	Approach	Techniques Used	Limitations and challenges
Timothy Stevens et al.	FLDP (Federated Learning with Differential Privacy)	Learning with Errors (LWE)	<ul style="list-style-type: none"> • Privacy and accuracy tradeoffs • Not scalable in large networks
Rathee et al.	ELSA Protocol	Dual-server design Client-driven aggregation Rogue client mitigation	<ul style="list-style-type: none"> • Runtime increases • Minore communication costs
Pierre Sanon et al.	SMPC, Homomorphic Encryption	Secure multi-party computation (SMPC), CKKS homomorphic encryption	<ul style="list-style-type: none"> • Increased computational overhead • Slower decryption and re-encryption
Shenghui Li et al.	Auto-weighted Geometric Median (AutoGM)	Byzantine resilient	<ul style="list-style-type: none"> • Complexity in large scale FL • Tradeoffs between robustness and efficiency
Zhuosheng Zhang et al.	SAFElearning	Obvious random grouping, Partial parameter disclosure	<ul style="list-style-type: none"> • Limitations in detecting sophisticated attacks • Vulnerable to some adversarial attacks

Table 1 Latest research challenges

There is a significant research gap in the field of secure aggregation for Federated Learning (FL), according to the latest research papers. Although much progress has been achieved in addressing privacy and security during model aggregation.

1. **Adversarial Attack Mitigation:** The Auto-weighted Geometric Median aggregation rule was introduced in the paper "Byzantine-Robust Aggregation in Federated Learning Empowered Industrial IoT," but it highlights the need for more reliable methods that target adversarial attacks like malicious updates and anomalies [11].
2. **Lightweight Cryptographic Solutions:** The authors of "Secure Federated Learning: An Evaluation of Homomorphic Encrypted Network Traffic Prediction" draw awareness to the

complexity of cryptographic schemes such as homomorphic encryption and the need of using lightweight cryptographic techniques for secure aggregation.

3. **Scalability:** The study "SoK: Secure Aggregation Based on Cryptographic Schemes for Federated Learning" suggests that large numbers of participants in federated learning systems require scalable solutions that do not compromise security or speed [12].
4. **Balancing performances:** Understanding how to achieve a balance between security guarantees and performance measurements like latency and throughput is a crucial topic for further study. Assessing these trade-offs is essential, especially for IIoT applications including secure aggregation.

1.4 Research Problem

The **main research problem** is the difficulty in designing secure aggregation techniques in Federated Learning (FL) that can successfully prevent adversarial attacks, such as malicious updates and outliers, while preserving computational efficiency in resource-constrained Industrial Internet of Things (IIoT) environments.

In these contexts, it is essential to make sure that the aggregation process does not impact the security or performance of the global model. Thus, the project seeks to explore solutions that balance security, accuracy, and computing efficiency, enabling effective decision-making in important IIoT applications. To address this problems, we hope to answer the following research questions:

- How can secure aggregation in FL mitigate adversarial attacks in IIoT?
- What lightweight methods can ensure secure aggregation in resource-constrained IIoT devices?
- How does secure aggregation affect decision-making accuracy in IIoT applications?
- What novel techniques can improve secure aggregation in IIoT while maintaining performance?

2 RESEARCH OBJECTIVES

2.1 Main Objective

This research aims to develop a novel approach to secure aggregation in Federated Learning for IIoT environments, addressing adversarial attacks, performance trade-offs, and resource constraints. This specified component focuses on lightweight cryptographic solutions, scalability, and security, ensuring efficient and privacy-preserving decision-making in IIoT applications.

2.2 Specific Objectives

To meet this main objective, there are various specific goals that need to be satisfied. These goals concentrate on developing and analyzing secure aggregation protocols, verifying the effectiveness of these protocols in preventing adversarial attacks, measuring their performance in resource-constrained contexts, and optimizing the protocols for large-scale applications. Each individual aim is focused at addressing a critical component of the main issue, delivering a strong, efficient, and scalable solution for secure aggregation in FL inside IIoT scenarios.

- **Design and Implement Secure Aggregation Protocols Using Secret Sharing and Cryptography solutions:** Develop a secure aggregation protocol that leverages Secret Sharing and Cryptography to prevent adversarial manipulation of model updates. The protocol will ensure that only a subset of devices can decrypt the aggregated updates, safeguarding the model from corruption by any single malicious device.
- **Demonstrate the Secure Aggregation Protocol in Preventing Adversarial Attacks:** validate the robustness of the secure aggregation protocol against various adversarial attacks, such as malicious model updates and outliers, in IIoT environments.
- **Optimize and Scale the Secure Aggregation Protocol for Large-Scale IIoT Applications:** Scale the secure aggregation protocol for large-scale deployment in IIoT applications, focusing on efficiency, scalability, and ease of integration with existing systems.

3 METHODOLOGY

3.1 System Diagram

Below is the proposed architecture, which outlines the integration of **secure aggregation techniques** in Federated Learning (FL) for Industrial IoT (IIoT) environments. The system is designed to enhance **privacy preservation, attack detection, and secure model training** while addressing the challenges posed by resource-constrained IIoT devices.

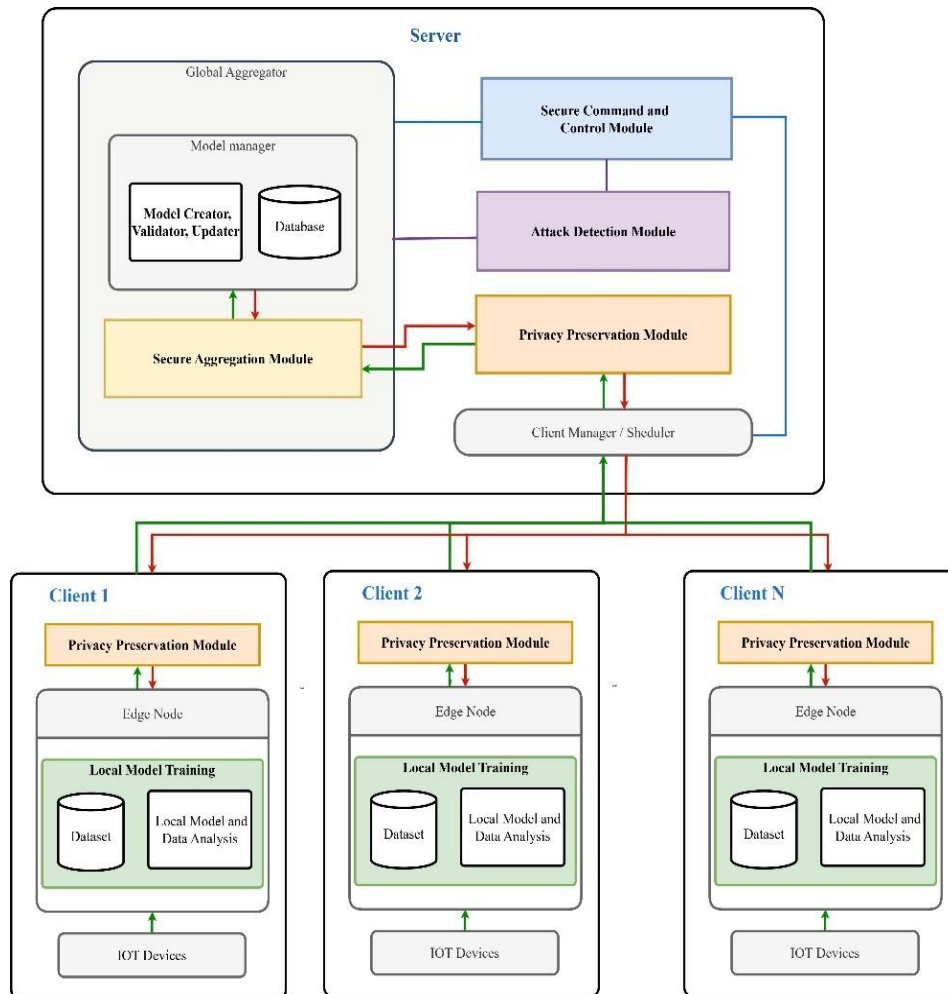


Figure 1 proposed overall system architecture

3.2 System Process

The illustration below depicts the straightforward system process of secure aggregation in Federated Learning (FL) inside Industrial Internet of Things (IIoT) contexts, where numerous client devices locally train models and send encrypted updates to a central aggregation server. The server thereafter does secure aggregation, securing privacy during the global model update. The system employs cryptographic solutions and anomaly detection algorithms to mitigate adversarial attacks and unauthorized access, while preserving data privacy, model integrity, and scalability for practical IIoT applications.

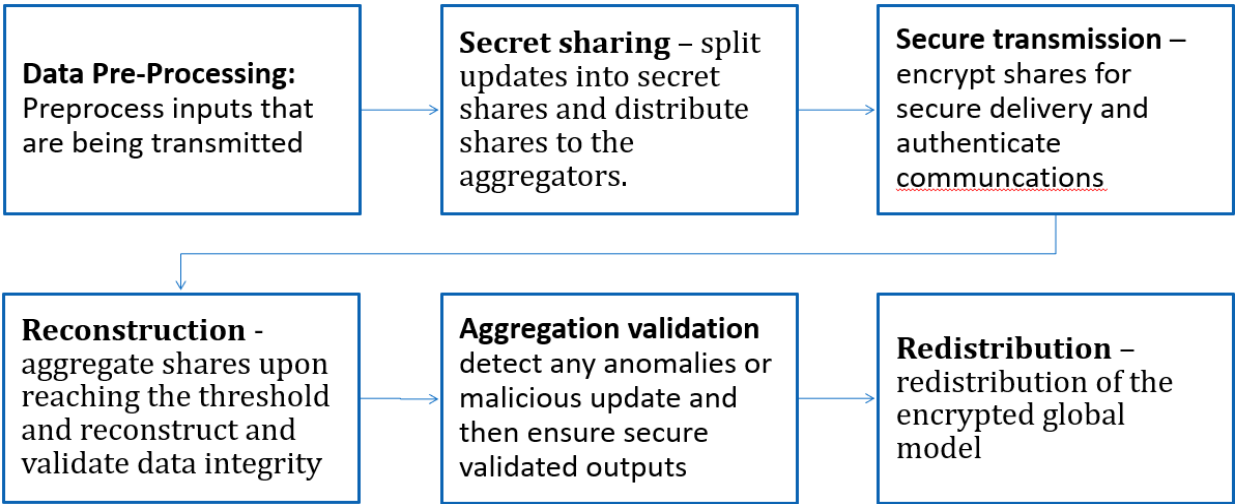


Figure 2 system process

3.3 Individual component Diagram

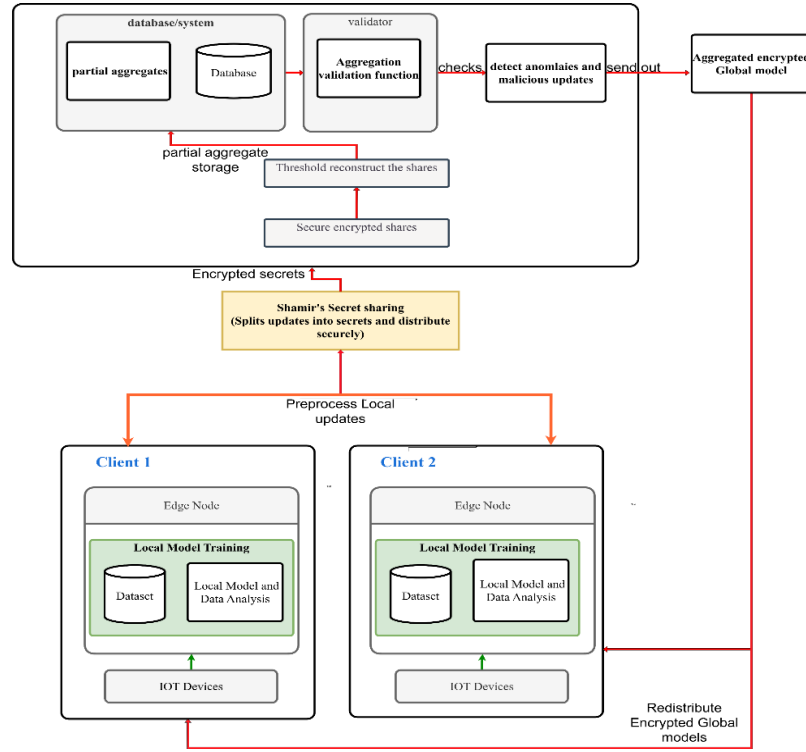


Figure 3 Proposed component architecture

The proposed approach incorporates cryptographic techniques to improve security and privacy, building upon the overall architecture of secure aggregation in FL. There are three primary parts to architecture:

- **Client Nodes (Edge Devices)** – These devices perform local model training using their private datasets and generate encrypted updates before sending them to the server.
- **Aggregation Server** – The central server securely aggregates the encrypted local updates from client nodes and validates them to detect anomalies or malicious updates.
- **Privacy-Preserving Mechanism** – Advanced cryptographic methods ensure that sensitive model updates remain secure throughout the training process, preventing unauthorized access and inference attacks.

3.4 Work Breakdown Structure

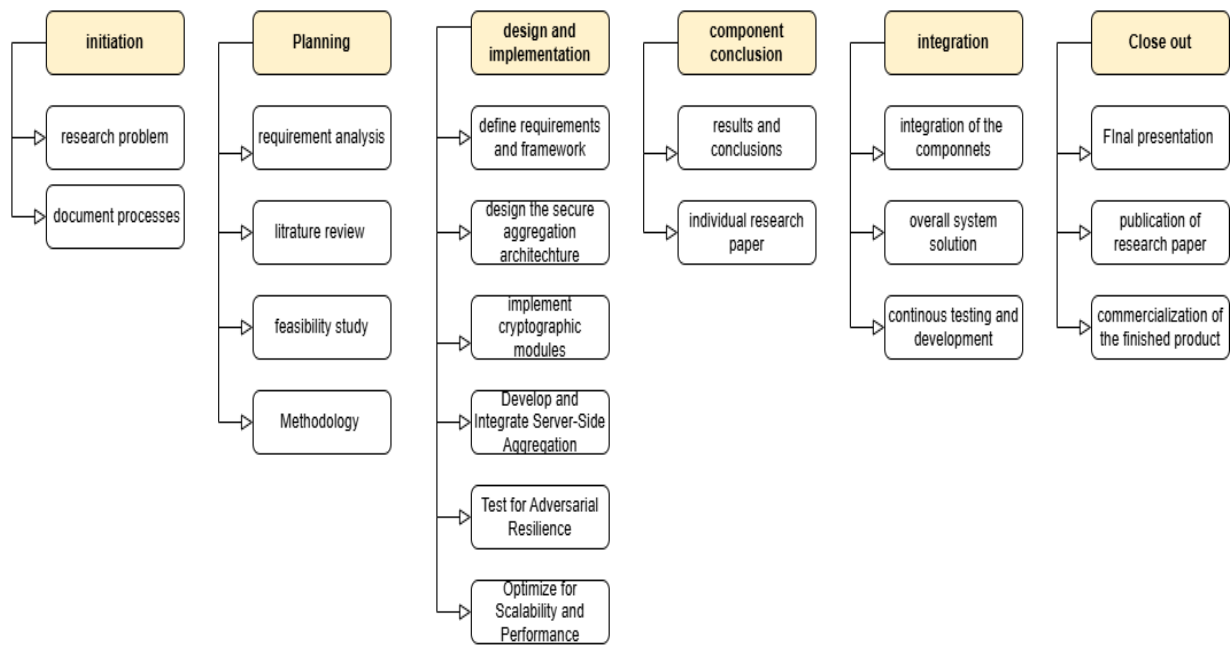


Figure 4 Work breakdown Structure

3.5 Gantt Chart

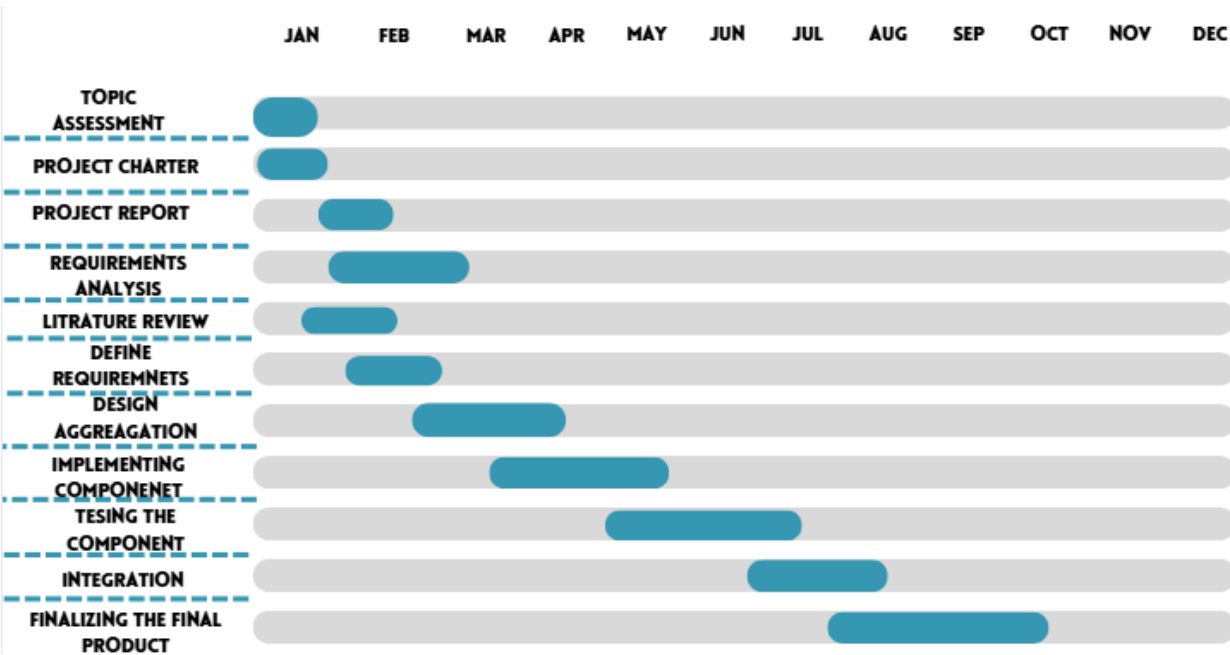


Figure 5 Gantt Chart

3.6 Expected Outcome

The proposed solution aims to provide a secure and efficient federated learning framework for IIoT environments, ensuring privacy and robustness against cyber threats.

- Full Adaptable Security Framework for FL in IIoT
- Enhanced Attack Resilience
- Adaptive Security Measures
- Real-Time Performance
- Heterogeneity Support
- Improved Data Privacy

3.7 Commercialization of the product

This solution is intended for practical implementation across several sectors, including those dependent on extensive data processing and security, such as manufacturing, energy, healthcare, and automotive industries.

Market Differentiators
<ul style="list-style-type: none">• Real-time threat detection and mitigation
<ul style="list-style-type: none">• Adaptability to diverse industries and dynamic attack patterns
<ul style="list-style-type: none">• Easy integration with existing IIoT infrastructures
Business Models
<ul style="list-style-type: none">• Software as a Service (SaaS) Model
<ul style="list-style-type: none">• Enterprise Solutions

4 PROJECT REQUIREMENTS

4.1 User Requirements

1. **User Privacy** - The framework must ensure that individual users' data remains private and confidential during the aggregation process.
2. **Robustness Against Adversarial Attacks** - The system should be resilient to inference attacks that attempt to analyze individual clients' models.
3. **Scalability**: The aggregation framework must scale effectively with an increasing number of devices and data sizes
4. **Adaptability to technology** - The framework should facilitate user engagement and encourage technological adoption among participants

4.2 Functional Requirements

1. **Secure aggregation component** - Implement a secure aggregation protocol that allows users to compute aggregate values without revealing their private values.
2. **Model Update Handling** -. The framework must handle model updates from multiple clients efficiently and securely aggregate these updates into a global model.
3. **Key Management** - management of cryptographic keys to enhance security during model updates.
4. **Anomaly Detection Mechanism** - Incorporate mechanisms to detect and mitigate the impact of malicious or benign updates from clients

4.3 Nonfunctional requirements

- **Performance Efficiency** - The system should maintain high performance with low latency and computational overhead during the aggregation process.
- **Fault Tolerance and Reliability** - The framework must be able to tolerate failures of a client without compromising the integrity of the aggregation process.
- **Compliance with Regulations** - Ensure that the framework complies with relevant data protection regulations and ethical standards regarding user data privacy
- **User-Friendly Interface** - Provide an intuitive interface that facilitates easy interaction for users participating in federated learning processes.

4.4 Software requirements

These are the currently identified software requirements to complete the project component,

- **Computing resources** – computational devices for training, cryptography and secure aggregation
- **Development tools** – python, TensorFlow Libraries and PyTorch and cryptographic libraries
- **Data-sets** – Open source IIoT datasets for simulation purposes that are gathered according to ethical requirements.

5 REFERENCES

- [1] H. Z. a. L. H. a. Z. Xie, "Privacy Attack in Federated Learning is Not Easy: An Experimental Study," 2024.
- [2] J. S. a. H. W. a. S. Rakshit, "Privacy in Federated Learning," 2024.
- [3] S. S. a. P. S. a. K. N. a. A. S. a. H. Wang, "FedMADE: Robust Federated Learning for Intrusion Detection in IoT Networks Using a Dynamic Aggregation Method," 2024.
- [4] J. S. a. R. E. A. a. B. G. a. J. J. a. S. Avestimehr, "Securing Secure Aggregation: Mitigating Multi-Round Privacy Leakage in Federated Learning," 2023.
- [5] S. a. M. M. R. a. P. P. a. P. S. Bharati, "Federated learning: Applications, challenges and future directions," 2022.
- [6] Keith Bonawitz and Vladimir Ivanov and Ben Kreuter and Antonio Marcedone and H. Brendan McMahan and Sarvar Patel and Daniel Ramage and Aaron Segal and Karn Seth, "Practical Secure Aggregation for Federated Learning on User-Held Data," 2016.
- [7] Jinhyun So and Ramy E. Ali and Basak Guler and Jiantao Jiao and Salman Avestimehr, "Securing Secure Aggregation: Mitigating Multi-Round Privacy Leakage in Federated Learning," 2023.
- [8] S. a. K. D. a. P. P. a. G. H. Singh, "Impact of Federated Learning on Industrial IoT - A Review," 2024.
- [9] Timothy Stevens, Christian Skalka, Christelle Vincent, John Ring, Samuel Clark, Joseph Near, "Efficient Differentially Private Secure Aggregation for Federated Learning via," 2022.
- [10] Rathee, Mayank and Shen, Conghao and Wagh, Sameer and Popa, Raluca Ada, "ELSA: Secure Aggregation for Federated Learning with Malicious Actors," 2023.
- [11] Shenghui Li, Edith Ngai, Thiemo Voigt,, "Byzantine-Robust Aggregation in Federated Learning," 2021.
- [12] Mohamad Mansouri, Melek Önen, Wafa Ben Jaballah, Mauro Conti, "SoK: Secure Aggregation Based on Cryptographic Schemes for," petsymposium.org, 2023.

- [13] Zhang, Zhuosheng and Li, Jiarui and Yu, Shucheng and Makaya, Christian,
"SAFE Learning: Secure Aggregation in Federated Learning With Backdoor Detectability,"
Institute of Electrical and Electronics Engineers (IEEE), 2023.
- [14] Hongbin, Fan and Zhi, Zhou, "Privacy-Preserving Data Aggregation Scheme Based on
Federated Learning for IIoT," 2023.