

Data-Privacy Focused Federated Learning Framework for Industrial IoT

Component 04 – Secure Command and Control

R25-039

Project Proposal Report

Dissanayaka K.D.A.R. A – IT21828348

Supervisor - *Dr. Sanika Wijesekara*

Co-Supervisor - *Mr. Tharaniyawarma Kumaralingam*

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
Dissanayaka K.D.A.R. A	IT21828348		

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

A key element of Federated Learning (FL) for Industrial IoT (IIOT) is Secure Command and Control (C2), which guarantees dependable and secure communication between devices and the central server. Implementing a strong Secure C2 framework that tackles important issues including data tampering, illegal access, and changing cyberthreats is the main goal of this study. The suggested approach guarantees confidentiality, integrity, and restricted access by combining Role-Based Access Control (RBAC) to limit sensitive commands, HMAC for data integrity validation, and TLS 1.3 for encrypted communication with mutual authentication. Furthermore, real-time anomaly detection improves defenses against replay and man-in-the-middle (MitM) assaults. The framework offers a safe basis for Federated Learning in industrial settings because it is scalable, lightweight, and designed for IIOT devices with limited resources.

CONTENTS

1	INTRODUCTION	5
1.1	Background Study	6
1.2	Literature Review	6
1.3	Research Gap.....	7
1.4	Research Problem.....	8
2	RESEARCH OBJECTIVES.....	8
2.1	Main Objective.....	8
2.2	Specific Objectives.....	9
3	METHODOLOGY	9
3.1	System Diagram	9
3.2	Work Breakdown Structure.....	11
3.3	Gantt Chart	12
3.4	Commercialization of the product.....	13
4	SOFTWARE SPECIFICATIONS.....	14
4.1	User Requirements	15
4.2	Functional Requirements.....	15
4.3	Non-functional requirements.....	15
5	DESCRIPTION OF PERSONAL AND FACILITIES	16
6	REFERENCES	16
7	APPENDICES.....	18
7.1	Plagiarism check - Turnitin	18

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

1 INTRODUCTION

Federated Learning (FL), which trains models locally on devices without disclosing raw data, is a viable method for decentralized machine learning in the Industrial Internet of Things (IIOT). However, the integrity and dependability of FL operations depend on secure communication between devices and the central server, sometimes known as Command and Control (C2). FL orchestration requires C2 signals, including task assignments, synchronization instructions, and model update requests. These signals could be intercepted, altered, or executed without authorization if strong security measures aren't in place. This could jeopardize the system as a whole.

Existing research underscores the importance of secure communication in FL for IIOT. Kairouz et al. (2021) emphasize that while FL decentralizes learning, the communication layer remains a significant attack surface, necessitating advanced cryptographic and authentication protocols [1]. Similarly, Sharma et al. (2022) discuss the risks of man-in-the-middle (MitM) and replay attacks in distributed systems and advocate for secure session management and integrity validation [2].

To address these challenges, Secure Command and Control employs a combination of modern security techniques:

- **TLS 1.3 with Mutual Authentication:** Provides end-to-end encrypted communication and verifies the identities of devices and the central server.
- **HMAC-based Integrity Validation:** Ensures that transmitted data, such as model updates, remains unaltered during transit.
- **Role-Based Access Control (RBAC):** Limits the execution of critical commands to authorized users or devices, enhancing security and compliance.
- **Real-time Anomaly Detection:** Monitors communication patterns to identify and mitigate emerging threats dynamically.

By incorporating these processes into a Secure C2 framework, FL activities are shielded from outside threats and are guaranteed to be scalable and efficient, which makes it ideal for IIOT situations with limited resources. By tackling particular IIOT issues including low latency needs and adherence to industry standards like IEC 62443 and GDPR, this research expands on current solutions.

1.1 Background Study

As the use of both Federated Learning and Industrial IoT continues to rise, the respective benefits of each are irrefutable - offering the ability to train the machine learning systems without the actual data being transferred! Something that goes a long way in ensuring data. Nonetheless, It's important to note that communication between devices and the command and control server needs to be carefully managed. For instance, control signal transmission and the request model updates are essential tasks that need to be sent to the server.

Controlling these tasks with unsecured communication channels can expose the system to a myriad of security threats such as man-in-the-middle attacks, unauthorized access, and even data manipulation. In order to protect against these vulnerabilities, more complex servers such as: TLS 1.3, HMAC-based data and detection of anomalies will be necessary.

1.2 Literature Review

Protecting C2 communications in Federated Learning for IIOT FL has been and continues to be a huge focus for researchers because of the sensitive nature of information having to do with the security of the distributed learning systems. In IIOT systems, K. Elmazi (2024) put forward the use of fault detection methods and stressed the use of cyberattack mechanisms at the synchronization signals and command signal transmission. This study stressed the threat of low or weak encryption and no mutual authentication in the transmission [3].

Differential Privacy (DP) and blockchain integration in FL systems were examined by A. Hussain (2025), who also showed how privacy-preserving techniques might improve communication security [4]. Nevertheless, the study pointed out that in IIOT contexts with limited resources, high computational overheads can make implementation more difficult. Similar to this, S. Ali (2023) presented a blockchain-based FL framework for intrusion detection that demonstrated how well mutual authentication and integrity checks operate to stop unwanted access, but it did not place enough focus on real-time anomaly detection for changing threats [5].

In addition, Marco & Guerra (2023) looked into the difficulties of C2 interoperability in tactical federated contexts and proposed that Role-Based Access Control (RBAC) would be a useful tool for preventing illegal command runs. Despite these developments, current solutions frequently

ignore the special needs of IIOT, including scalability, low latency, and lightweight implementations designed for devices with limited resources.

In order to ensure reliable and effective communication in FL systems for IIOT, these studies together highlight the necessity for a thorough Secure C2 framework that incorporates contemporary encryption protocols like TLS 1.3, integrity validation with HMAC, and real-time anomaly detection.

1.3 Research Gap

GAP	DESCRIPTION	POTENTIAL SOLUTIONS	REFERENCE
Communication Security	Ensuring secure communication between IoT devices and the command/control module.	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - Use decentralized architecture - Implement edge computing for distributed processing. - Optimize protocols for low overhead. 	[11]

1.4 Research Problem

What techniques may be used to defend Industrial IoT (IIoT) systems' Command and Control (C2) communications in Federated Learning (FL) from changing threats while preserving low latency, high efficiency, and scalability in resource-constrained environments?

The goal of this study is to solve critical weaknesses in Federated Learning (FL) for Industrial IoT (IIoT) in order to improve the security of Command and Control (C2) interactions. In order to safeguard data while it is being transmitted, it suggests using TLS 1.3 for end-to-end encryption, which includes Perfect Forward Secrecy and mutual authentication. HMAC is used as a strong verification method to monitor for possible tampering and guarantee data integrity. Role-Based Access Control (RBAC) is also incorporated to reduce the danger of unauthorized access by limiting the execution of crucial commands to authorized individuals and devices. Real-time anomaly detection, which the framework integrates to further improve resilience and adaptability, allows the system to recognize and react to new threats in a timely and efficient manner.

2 RESEARCH OBJECTIVES

2.1 Main Objective

Through a particular focus on adversarial attacks, performance trade-offs, and resource constraints in Industrial Internet of Things (IIoT) environments, the primary goal of this research project is to

present a novel approach to secure aggregation in Federated Learning (FL) that addresses the research gaps and research problem described in the paper. The goal of the research is to create practical methods that preserve FL systems' efficiency and security while guaranteeing precise decision-making in crucial IIoT applications. Investigating lightweight cryptographic solutions, improving scalability, and striking a balance between security assurances and performance indicators like latency and throughput can all help achieve this.

2.2 Specific Objectives

Ensure Secure Communication

Implement TLS 1.3 for encrypted and authenticated communication.

Validate Data Integrity

Use HMAC to ensure commands and updates are tamper-proof.

Implement Access Control

Implement Role-Based Access Control (RBAC) to limit the execution of commands to those who are permitted.

Enhance Threat Resilience

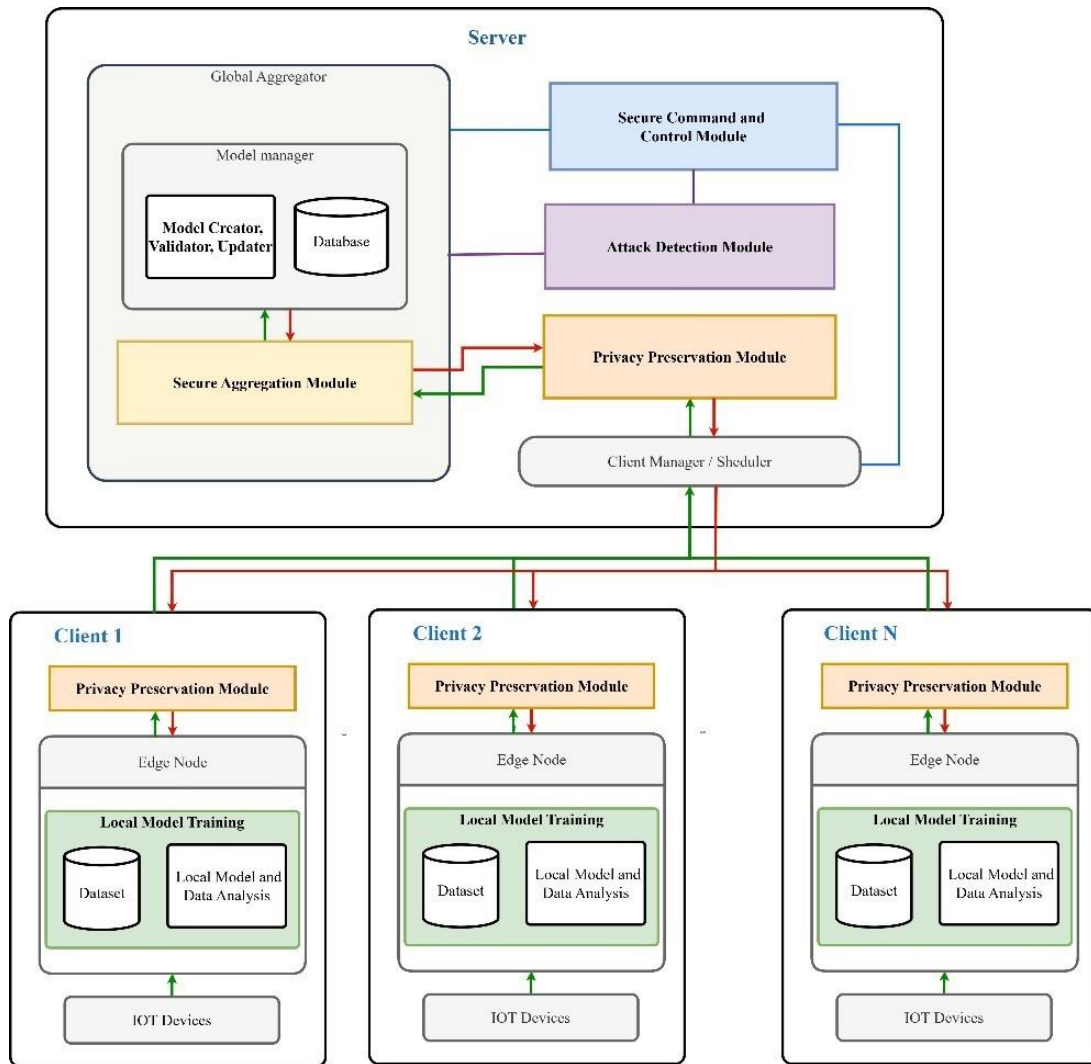
Integrate real-time anomaly detection to identify and mitigate suspicious activities.

Optimize for IIOT Devices

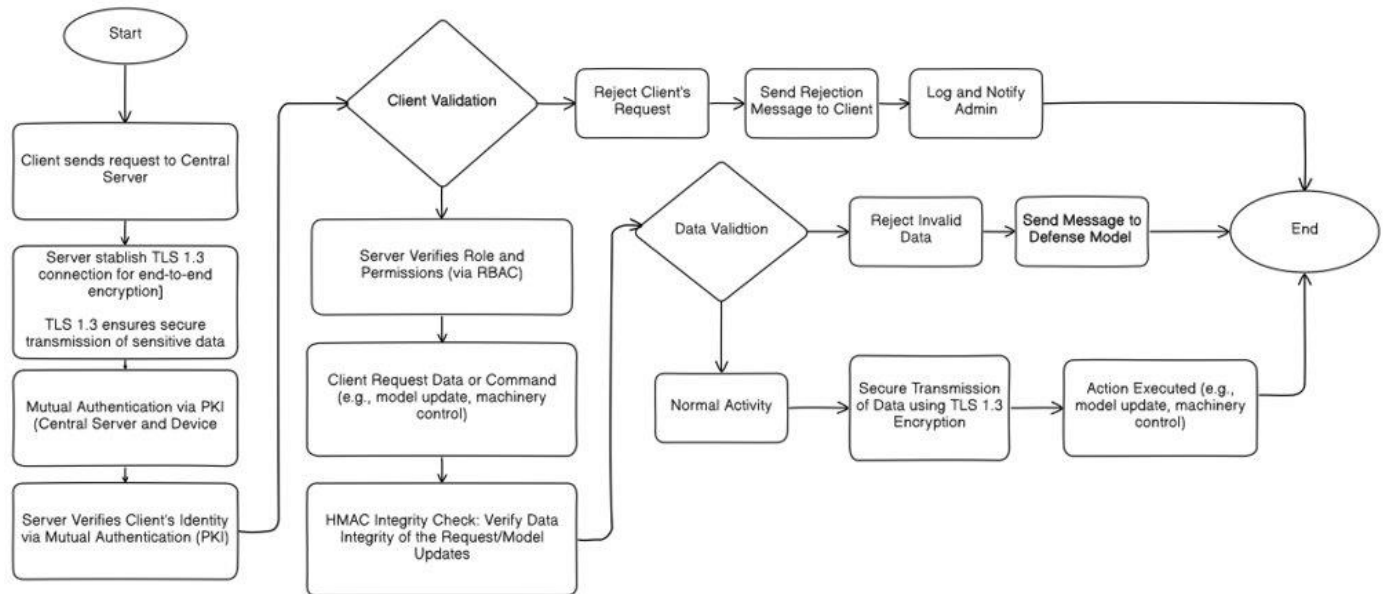
Develop lightweight solutions to support resource-constrained devices with minimal latency.

3 METHODOLOGY

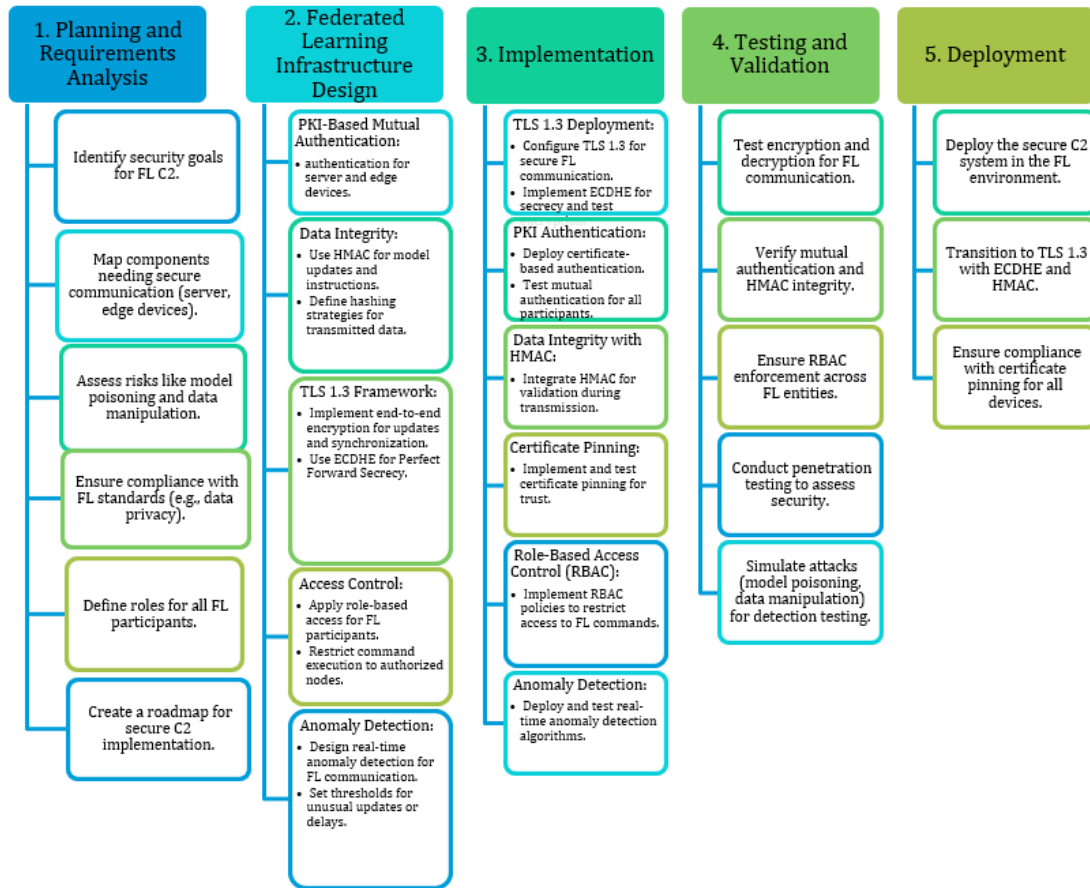
3.1 System Diagram



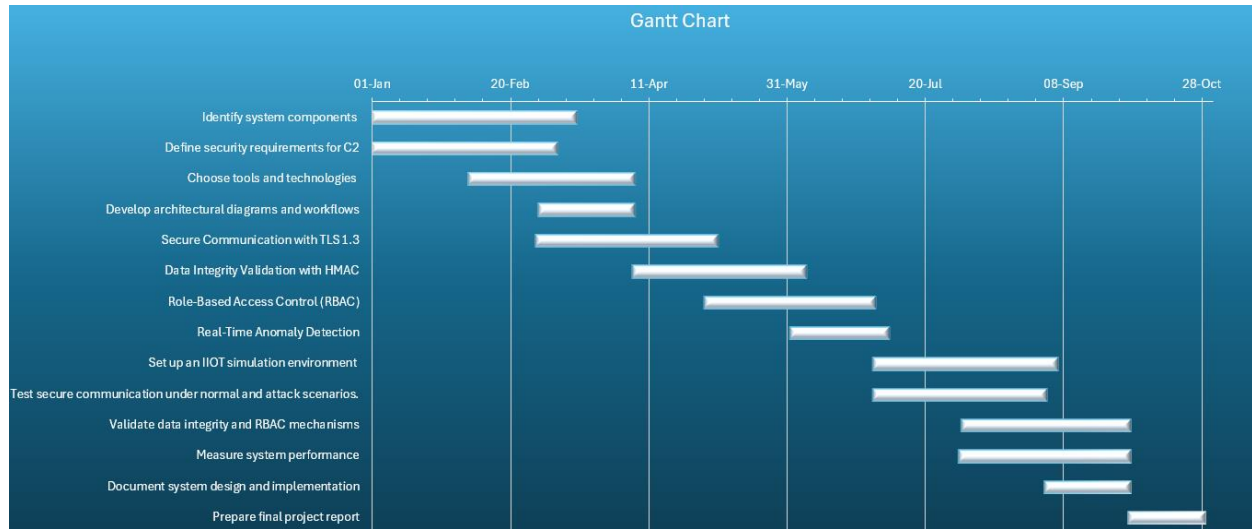
Component Process



3.2 Work Breakdown Structure



3.3 Gantt Chart



3.4 Commercialization of the product

Strong commercialization potential across multiple industrial sectors is provided by the Secure Command and Control (C2) framework for Federated Learning (FL) in Industrial IoT (IIoT), which enables strong security and privacy for crucial systems.

Target Market

The following sectors and industries will be the focus of the framework:

Industries: Industries that significantly depend on IIOT systems include manufacturing, energy, healthcare, and logistics.

Important Clients: businesses that specialize in industrial automation, producers of IIOT devices, and Federated Learning solutions are provided by cloud service companies.

Value Proposition

Enhanced Security: defends vital IIOT systems from threats based on communication (such as replay and man-in-the-middle attacks).

Compliance: Helps industries adhere to regulations like GDPR, NIST, and IEC 62443.

Cost-Effectiveness: Offers lightweight security solutions optimized for resource-constrained devices, reducing operational costs.

Real-time Threat Detection: enhances system resilience through dynamic threat mitigation.

Commercialization Strategies

Licensing: Industrial automation firms and IIOT device manufacturers can purchase licenses for the Secure C2 framework.

Software as a Service: Provide the C2 framework for safe communication in Federated Learning applications as a subscription-based service.

Partnerships: Work together with FL and IIOT solution providers to incorporate Secure C2 into their service portfolio.

Product Bundling: To improve their security capabilities, combine the Secure C2 solution with IIOT management platforms.

4 SOFTWARE SPECIFICATIONS

4.1 User Requirements

User Privacy - Throughout the aggregation process, the framework must guarantee that the data of specific users is kept private and secret.

Robustness Against Adversarial Attacks - The system must be able to withstand reasoning assaults that try to examine the models of specific clients.

Scalability - As the number of devices and data sizes increases, the aggregation architecture must be able to grow with them.

Adaptability to technology - The framework should promote participants' acceptance of new technologies and ease user interaction.

4.2 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.

4.3 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)

5 REFERENCES

6 References

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

- [2] S. S. ., S. S. Vinay K. Gugueoth, "Security of Internet of Things (IoT) using federated learning and deep learning - Recent advancements, issues and prospects," 2023.
- [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] Q. L. ., A. Y. Saqib Ali, "Blockchain and federated learning-based intrusion detection for edge-enabled industrial IoT networks: A survey," 2024.
- [6] [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc8446>.
- [7] [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf>.
- [8] [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.
- [9] [Online]. Available: <https://ieeexplore.ieee.org/document/8736786>.
- [10] [Online]. Available: <https://csrc.nist.gov/projects/lightweight-cryptography>.
- [11] [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf>.
- [12] [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf>.

7 APPENDICES

7.1 Plagiarism check - Turnitin