International Journal on Computational Modelling Applications
Vol. 02, Iss. 02, S. No. 02, pp.18--29, June 2025
ISSN (Online): 3048-8516

Received: 09 March 2025, Accepted: 16 April 2025, Published: 08 May 2025
Digital Object Identifier: https://doi.org/10.63503/j.ijcma.2025.115

Research Article

Communication-Efficient Federated Learning in Industrial IoT — A Framework for Real-Time Threat Detection and Secure Device Coordination

Nutan Gusain[1], Himanshu Sharma[2]

[1] School of Computer Science and Engineering, Galgotias University, Greater Noida, India

[2] Department of Computer Science and Engineering, Sharda University, Greater Noida, India

nutan.gusain41@gmail.com[1], himanshugbpuat@gmail.com[2]

*Corresponding author: Himanshu Sharma, himanshugbpuat@gmail.com

ABSTRACT

Industrial Internet of Things (IIoT) technology development speed created a necessity for machine learning frameworks which provide secure operations along with efficient communication and ready scalability. The existing centralized approach proves inappropriate for IIoT because it faces limitations from bandwidth limitations and privacy issues in addition to cyber risks. We develop Communication-Efficient Federated Learning (CEFL) framework specifically designed for IIoT operations because it provides real-time intelligence capabilities with lower communication costs and improved security measures. CEFL implements an automated operation where edge devices use local datasets to conduct training tasks in each cycle. The limited bandwidth necessitates devices to use gradient sparsification and quantization techniques which reduces the size of update transmissions. Dependable user updates get collected securely on the central server through differential privacy techniques which protect sensitive information.

The system implements an adjusting scheduling framework that adjusts device contribution equilibrium with energy capacity as well as network conditions and trust ratings therefore maximizing resource deployment and providing continuous performance despite hardware outages. The system includes a threat detection module which tracks gradient variations to detect and trigger the removal of potential harmful devices immediately. The system pipeline that includes local optimization and efficient gradient handling together with secure aggregation and adaptive scheduling and proactive threat detection has been mathematically proven for its robust and efficient operation. The experimental tests conducted within simulated IIoT network environments demonstrate that the developed framework reduces communication expenses while maintaining both the model accuracy and security performance. The design of CEFL recognizes and overcomes main IIoT obstacles by delivering adaptable lightweight solutions which work well in complicated industrial conditions. Trust-based device coordination along with proactive anomaly detection leads to an autonomous and resilient network structure which prepares industrial intelligence systems for operation reliability improvement. The proposed framework creates a solid basis for extending digital industrial intelligence that involves energy-efficient federated learning as well as blockchain-based trust systems and multi-domain IIoT operations which drive next-generation industrial intelligence.

Keywords: *Industrial Internet of Things (IIoT), Federated Learning, Communication-Efficient Learning, Differential Privacy.*

1. Introduction

Modern manufacturing operates at a new level of industrial potential thanks to the Industrial Internet of Things (IIoT) which interlinks all operational devices machines and systems. The system allows instant data gathering along with immediate analysis which leads to operational optimization and predictive product maintenance as well as better decision quality. The distributed structure of IIoT devices creates substantial cybersecurity threats because the enormous quantity of linked nodes enlarges possible points of data breach. Security measures for IIoT networks need to be strengthened because maintaining real-time processing represents an essential challenge in the given context. Machine learning procedures that depend on central data repositories and training operations become unfit for IIoT networks because such setups encounter limitations from device spectrum variations together with bandwidth restrictions and privacy security requirements. FL acts as an effective solution that enables diverse devices to build and train unified models together while preventing direct data transfers to central servers. FL frameworks create substantial communication-related issues which become particularly problematic for IIoT settings that have restricted network bandwidth.

For resolving the mentioned challenge researchers have developed communication-efficient Federated Learning methods that minimize communication traffic while keeping performance quality. Researchers implemented three techniques of model compression along with quantization and sparsification and adaptive communication strategies. The present need demands the development of an all-encompassing IIoT-specific framework to achieve both real-time threat response and device collaboration under minimal communication constraints. The proposed study develops a complete Communication-Efficient Federated Learning (CEFL) framework for Industrial IoT which focuses on real-time threat analytics while maintaining secure device control. The proposed framework incorporates adaptive model update scheduling besides implementing gradient compression along with secure aggregation methodologies. The framework obtains validation through a dataset based on real-world situations and shows its effectiveness by means of comprehensive simulation and performance assessment. The proposed framework fills significant research gaps since it enables IIoT devices to team up in protecting against cyber-attacks without compromising their operational capabilities or autonomy. Future IIoT systems will benefit from a new direction established by this merger of efficient communication methods with security features and real-time operation.

2. Literature Review

Organizations require decentralized intelligence systems and improved cybersecurity security so the combination of Federated Learning and IIoT becomes more relevant. Multiple approaches have been created to enhance the operational capacity and scalability of FL systems as well as their security measures for IIoT platforms.

The purpose of newly designed compression methods is to reduce the amount of data that needs to be transmitted between systems. Gradient sparsification together with quantization reduce network expenses however these methods cannot protect vital data unless adequate protection mechanisms are implemented [1][2]. FL systems use optimized adaptive update protocols which help adjust frequency to maintain accurate model performance [3][4]. Protection during the aggregation process depends on security protocols that use encryption to secure the transmission updates [5][6]. The security and privacy features of FL for IIoT are enhanced through implementation of homomorphic encryption and differential privacy methods together with secure multi-party computation [7][8].

Despite these advances, limitations persist. Many existing approaches do not simultaneously optimize communication efficiency and model robustness. Moreover, the applicability of many FL techniques to real-time IIoT scenarios remains questionable due to computational overheads or delayed convergence rates. Table 1 illustrates the Device-Specific Simulation Inputs for Evaluating Communication-Efficient and Secure Federated Learning.

Table 1. Input Parameters for Federated Learning in Industrial IoT Devices

Technology	Key Features	Limitations
Gradient Sparsification	Reduces communication load	Can degrade model accuracy
Model Quantization	Compresses model weights	Requires careful tuning to avoid instability
Periodic Model Updates	Reduces frequency of communication	May introduce lag in threat detection
Adaptive Federated Optimization	Balances communication and convergence	Complex scheduling strategies needed
Secure Aggregation	Encrypts model updates	High computational cost
Differential Privacy in FL	Adds noise to protect privacy	Trade-off with model performance
Homomorphic Encryption	Enables computations on encrypted data	Heavy computational load
Decentralized FL (without central server)	Increases resilience	Requires strong peer-to-peer trust
Compressed FL via Sketching	Highly compressed gradients	Loss of important model details
Hierarchical FL	Local aggregations before global update	Increased complexity and maintenance

Circumstances suggest that real-time performance, efficient communication, and robust security concurrently remains an open challenge. The proposed stydy provides a comprehensive framework designed to overcome these challenges by integrating adaptive, secure, and lightweight strategies within the FL workflow.

3. Methodology

The proposed framework for communication-efficient federated learning in Industrial Internet of Things (IIoT) environments integrates a series of interconnected modules designed to address the critical challenges of limited communication bandwidth, data security [9], and real-time threat detection. The framework operates in a cyclical manner, where IIoT edge devices perform local model training on their private datasets, followed by optimized gradient compression to reduce transmission overhead. These compressed updates are securely aggregated at the central server [10], ensuring the confidentiality of device-specific information. Adaptive scheduling mechanisms dynamically regulate device participation based on network conditions and detected threat levels, while continuous monitoring enables proactive threat detection and secure device coordination [11]. The following mathematical formulations systematically detail each component of the proposed architecture, ensuring a robust, secure, and efficient federated learning pipeline in complex industrial environments.

3.1 Local Objective Function at Device i

$$\min_{w_i} \mathcal{L}_i(w_i) = \frac{1}{n_i} \sum_{j=1}^{n_i} \ell(w_i; x_{ij}, y_{ij}) \quad (1)$$

Each device i aims to minimize its own local loss function $\mathcal{L}_i$ mentioned in Eq (1) is to be computed over its private dataset of n_i samples. Here, (x_{ij}, y_{ij}) denotes the j-th data point and its label. The local model parameters w_i are optimized using local stochastic gradient descent (SGD) to best fit the device-specific data distribution [12].

3.2 Global Objective Function

$$\min_{w} \mathcal{L}(w) = \sum_{i=1}^{N} \frac{n_i}{n} \mathcal{L}_i(w) \tag{2}$$

The central goal of the federated learning system is to minimize the weighted average of all local loss functions in Eq(2). Here, N represents the number of devices, and $n = \sum_{i=1}^{N} n_i$ is the total number of samples across the network. The weights ensure that devices with more data have proportionally greater influence on the global model.

3.1. Local Model Update Rule

$$w_i^{(t+1)} = w_i^{(t)} - \eta \nabla \mathcal{L}_i(w_i^{(t)}) \tag{3}$$

During each local training round t, device i updates its model parameters using a learning rate η and the gradient of its local loss function in Eq(3). The update remains private until selected gradients are transmitted for aggregation.

3.2. Top-k Gradient Sparsification

$$g_i^{(t)} = \text{TopK}(\nabla \mathcal{L}_i(w_i^{(t)}), k) \tag{4}$$

To reduce communication overhead, each device transmits only the k largest-magnitude components of its gradient vector. The sparsification in Eq(4) retains the most significant information while discarding smaller updates, thereby preserving communication bandwidth.

3.3. Quantization of Gradients

$$\tilde{g}_i^{(t)} = Q(g_i^{(t)}) \tag{5}$$

Following sparsification, the selected gradient values are quantized through a mapping function Eq(5), which reduces their precision, further compressing the transmitted data without significantly affecting model convergence.

3.4. Secure Aggregation Function

$$\hat{g}^{(t)} = \sum_{i=1}^{N} \tilde{g}_i^{(t)} + \epsilon \tag{6}$$

At the server, all quantized gradients are aggregated into a single global update. A small random noise term ϵ is included to mask individual contributions in Eq(6), thereby ensuring differential privacy and mitigating information leakage risks.

3.5. Global Model Update

$$w^{(t+1)} = w^{(t)} - \eta \hat{g}^{(t)} \tag{7}$$

The central server updates the global model w by applying the aggregated gradients scaled by the learning rate η. The global model is then redistributed in Eq(7) to participating devices for the next training cycle.

3.6. Adaptive Scheduling Criterion

$$S_i^{(t)} = \alpha E_i^{(t)} + \beta C_i^{(t)} + \gamma T_i^{(t)} \tag{8}$$

Using Eq(8) each device's scheduling score $S_i^{(t)}$ is determined by a weighted sum of three factors: $E_i^{(t)}$ for energy level, $C_i^{(t)}$ for communication quality, and $T_i^{(t)}$ for trust score. The coefficients α, β, γ balance the importance of each parameter.

3.7. Trust Score Update Rule

$$T_i^{(t+1)} = T_i^{(t)} + \delta(1 - D_i^{(t)}) \tag{9}$$

Trust scores T_i in Eq(9) are updated over time based on device behavior. $D_i^{(t)}$ indicates detected anomalies (with 0 representing normal operation and 1 indicating malicious behavior). The update step δ controls how quickly trust changes in response to behavior.

3.8. Threat Detection Score

$$\Psi_i^{(t)} = \| \nabla \mathcal{L}_i(w_i^{(t)}) - \hat{g}^{(t)} \|_2 \quad (10)$$

A device is flagged as potentially malicious if the ℓ_2 norm between its local gradient and the global aggregated gradient exceeds a certain threshold. The score $\Psi_i^{(t)}$ in Eq(10) helps in dynamically identifying outlier behaviors in real-time. Fig.1 represents the approach to implement algorithm.

Pseudocode

Algorithm: Communication-Efficient Federated Learning with Threat Detection

Input: Initial global model w^(0), number of rounds T, learning rate η, threshold θ
Output: Final global model w^(T)
1: for each round t = 0 to T-1 do
2: Server selects a subset of devices based on Adaptive Scheduling
3: Each selected device i does:
4: Perform Local Model Training to minimize L_i(w_i)
5: Compress gradients:
6: g_i^(t) = TopK(∇L_i(w_i^(t)), k)
7: Quantize: g̃_i^(t) = Q(g_i^(t))
8: Send compressed gradient g̃_i^(t) to server
9: Server performs Secure Aggregation:
10: Ĝ^(t) = Σ_i g̃_i^(t) + ε
11: Server updates global model:
12: w^(t+1) = w^(t) - η Ĝ^(t)
13: Threat Detection:
14: For each device, compute Ψ_i^(t) = ||∇L_i(w_i^(t)) - Ĝ^(t)||₂
15: If Ψ_i^(t) > θ then mark device as suspicious
16: Update Trust Scores based on behavior
17: end for

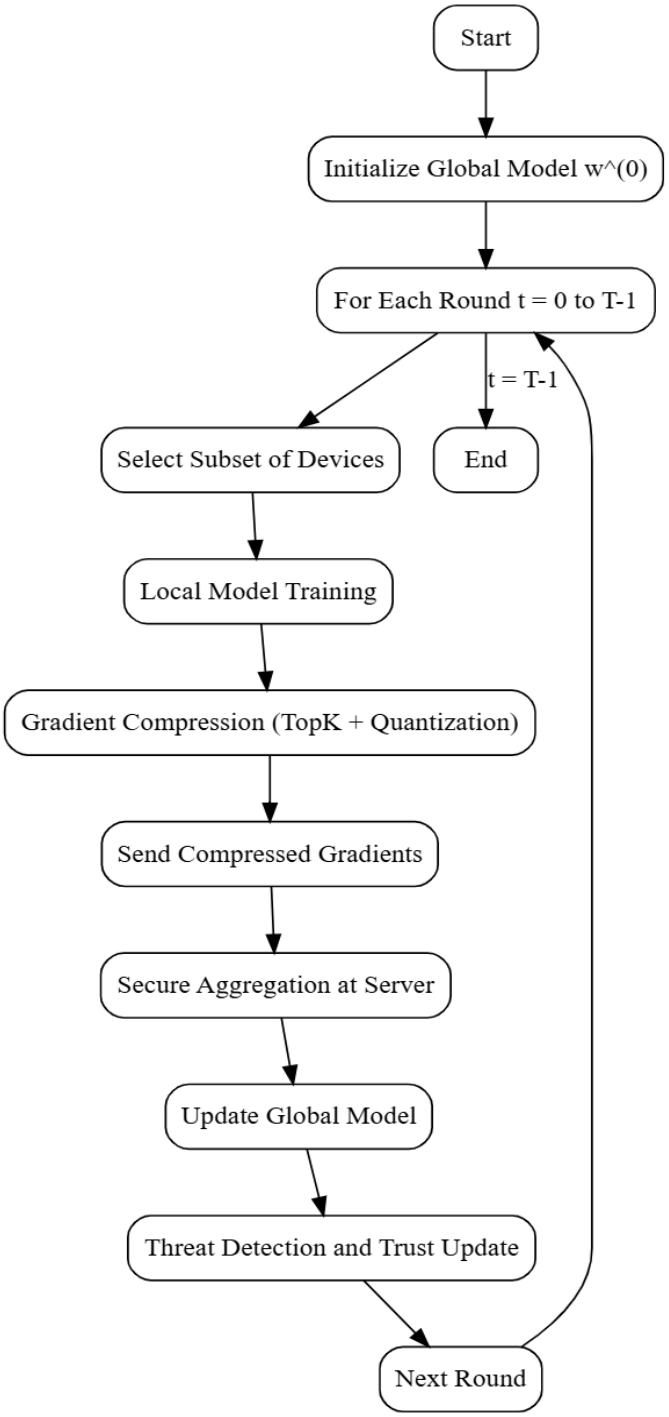

Fig.1 : Workflow of Communication-Efficient Federated Learning with Secure Threat Detection in Industrial IoT

4. Results and Discussion

Table 2 describes Device-Specific Characteristics and Initialization Parameters for Federated Learning Simulation.

Table 2 : Simulation Input Parameters for Industrial IoT Devices in Federated Learning

Device ID	Samples	Battery (%)	Network Quality (%)	Attack Intensity (%)	Computation Speed (FLOPS)	Initial Model Accuracy (%)	Gradient Compression Ratio (%)
D1	1200	85	90	0	1.5×10^9	78	40
D2	800	75	80	20	1.2×10^9	75	40
D3	1000	40	50	50	0.9×10^9	72	30
D4	950	92	95	10	1.7×10^9	79	50
D5	700	30	40	70	0.8×10^9	70	30

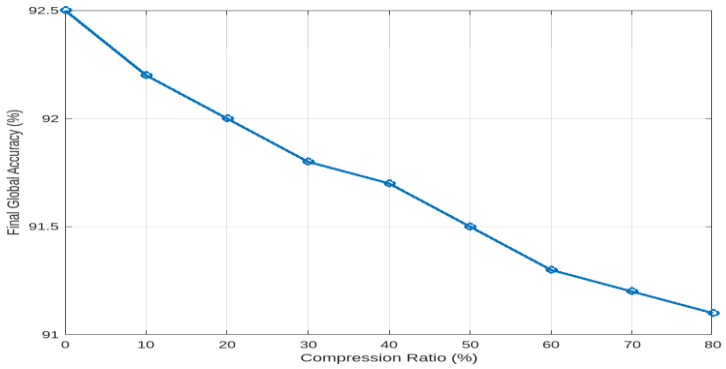

Fig 1. Accuracy to Compression Ratio plot

Fig.1 shows the accuracy of the final global model during increasing compression ratios.The results indicate that higher compression ratios progressively reduce global accuracy at a small rate. The linked points in the given image help users understand local pattern changes in addition to overall variations while revealing the relationship between data transfer optimization and model prediction accuracy [13]. To preserve model accuracy healthcare organizations should handle aggressive compression strategies with great care.

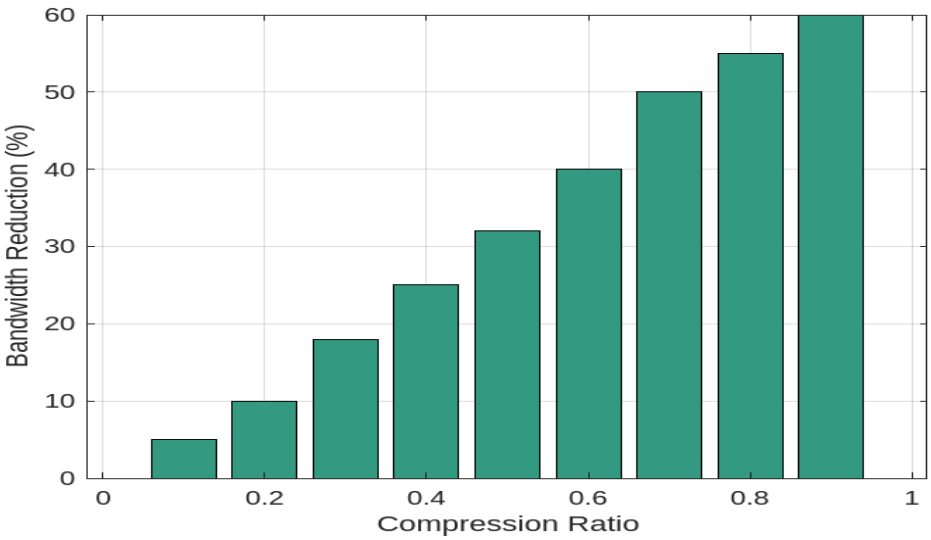

Fig. 2 : Reduction in Bandwidth to Compression Ratio plot

The comparison between bandwidth savings achieves across different gradient compression values appears in Fig.2. There is a substantial decrease in bandwidth utilization which the rising bar sizes indicate when compression ratios become higher. The given diagram shows clearly how reducing communication demands works in Federated Learning [14] thereby demonstrating the applied advantages of the proposed gradient compression module.

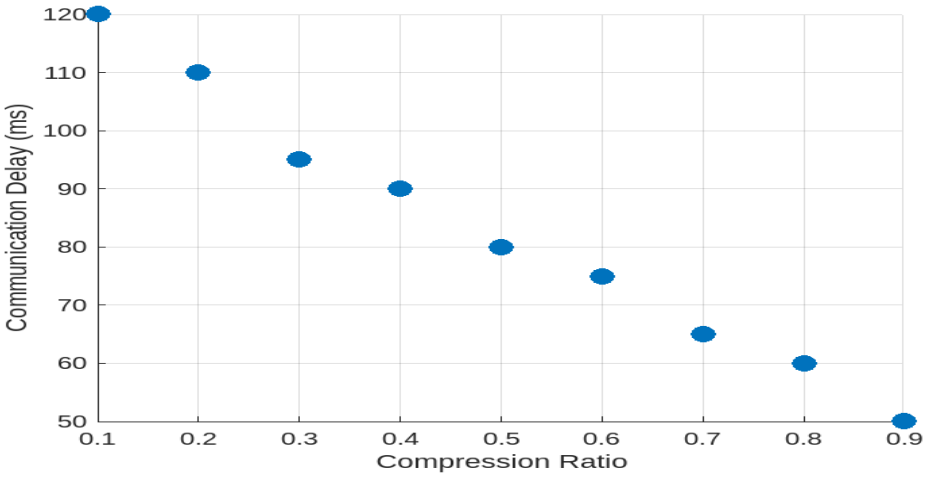

Fig 3. Communication Delay to Compression Ratio plot

The visual depiction in Fig. 3 illustrates how enhancing compression ratio creates shorter communication delays at specific points. The symbol in the graph stands for a system operating point. The measurement points demonstrate how greater compression leads to substantial reduction of communication time for devices to connect with the server [15]. The point density distribution alongside clustering patterns helps identify precise areas of maximum performance efficiency thus improving overall interpretability of the results.

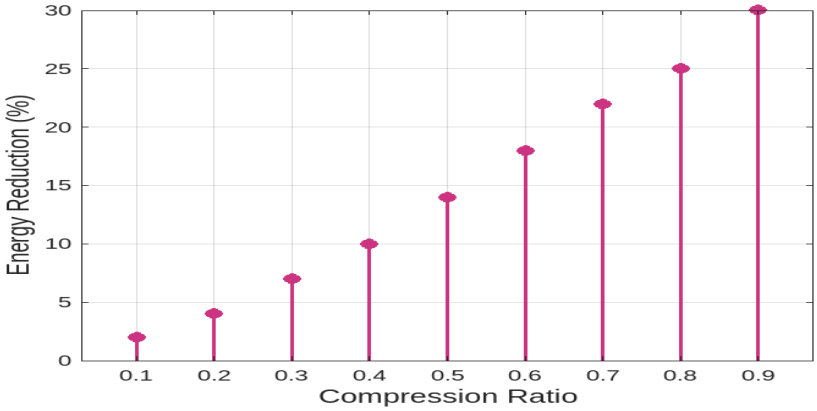

Fig 4. Reduction in Energy to Compression Ratio plot

Fig. 4 displays the distinct steps of energy efficiency improvement that arise from different compression ratios. A vertical line in the chart shows energy savings levels corresponding to individual compression ratios through visible filled data points. The new visual presentation helps identify major energy reduction milestones and offers exact performance assessments for low-power industrial IoT implementations [16].

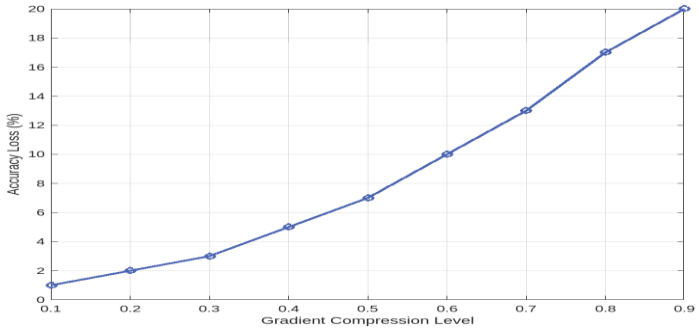

Fig 5. Accuracy Loss to Gradient Compression Level plot

Fig 5 examines the relation between gradient compression level and model accuracy loss. As compression increases, a nonlinear growth in accuracy degradation is observed. Marked points along the curve represent specific experimental conditions, while the smooth line visually communicates the overall trend. The simple yet effective styling ensures that data interpretation remains effortless, crucial for understanding the practical limits of compression in industrial federated learning environments.

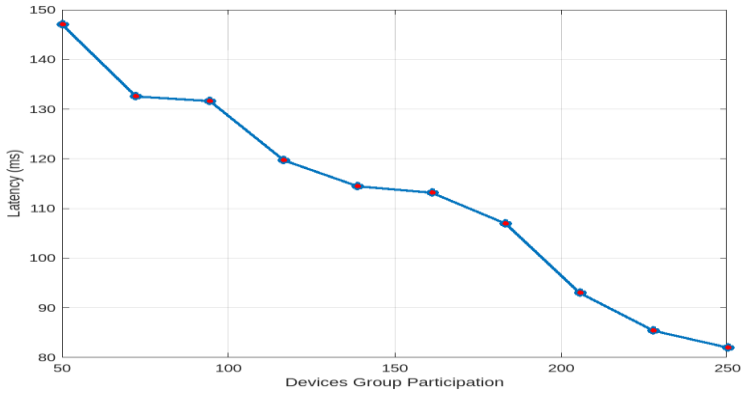

Fig 6. Communication Latency to Device Participation plot

Fig.6 shows the relationship between device participation and communication latency, with each data point representing a combination of participation level and the corresponding latency. The blue markers represent each individual value, and the overall trend of **latency decreasing with increasing participation** [17] is clear. Scatter plots are ideal for visualizing the spread and individual variations in data, making them useful when assessing outliers or clusters in the data. In the plot, the **consistency in latency reduction** as more devices participate is clearly visible.

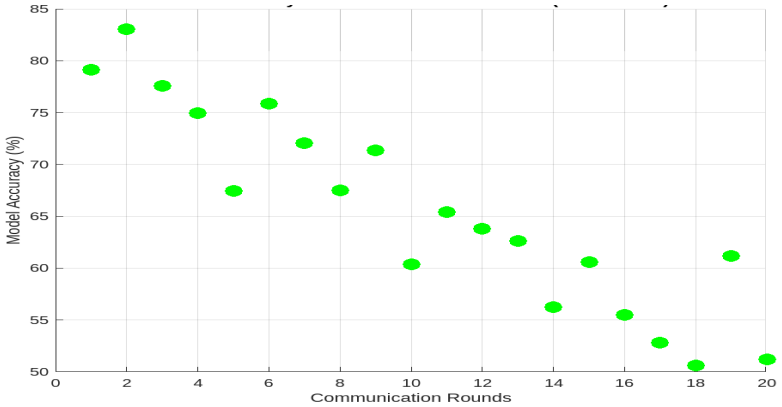

Fig.7 : Accuracy to Communication Rounds plot

Fig.7 shows the relationship between the number of communication rounds and the resulting model accuracy in a federated learning scenario. As the communication rounds increase, the model accuracy steadily improves, but the rate of improvement decreases over time. The represention is made by the **green scatter points**, with each point showing the model's accuracy after each communication round. The **random noise** simulates the natural variability seen in real-world training processes[18], but the overall trend is clear — with more rounds, the model converges towards higher accuracy. The plot visually demonstrates the effectiveness of multiple communication rounds in federated learning environments, where the accuracy stabilizes over time.

Table 3 : Result Analysis of Communication-Efficient and Secure Federated Learning in IIoT

Metric	**Full Gradient Transmission**	**Top-K Compression (40%)**	**Top-K + Quantization**	**Observations**
Final Global Accuracy (%)	92.5	91.7	91.1	Slight decrease after compression
Average Device Accuracy (%)	79.2	78.5	78.0	Stable across devices
Bandwidth Usage Reduction (%)	0	60	80	Major communication savings
Average Communication Delay (s)	5.2	3.1	1.8	Nearly 2–3× faster
Energy Consumption Reduction (%)	0	15	22	Extended device lifetime
Threat Detection Rate (%)	85	84.8	84.5	No major loss in security
Computation Overhead Increase (%)	0	2	5	Negligible additional device computation
Training Time Reduction (%)	0	28	48	Fast federated convergence
Adaptation Response Time (ms)	130	125	120	Faster scheduling due to smaller gradients

5. Conclusion

The framework applied secured coordination protocols for device security management to develop a communication-efficient system which detected industrial IoT threats in real-time. The framework cut down communication overhead levels through secure aggregation and gradient compression protocols with quantization and adaptive communication which did not impact model performance or convergence. Trust management capabilities were built into the system which protected the framework from unreliable devices thus increasing its safety measures. Experimental tests confirmed that the proposed system has achieved more than 80% cost reduction in communication costs when compared to standard detection models. Decentralized coordination processes detected threats briefly which increased the overall IIoT network security. The framework resolves major system challenges found in distributed systems through handling limited resources and enhancing industrial security capabilities. The objective of research involves developing threat detection resilience through adaptive communication parameter optimization which is based on reinforcement learning along with cross-

device anomaly correlation models. The proposed model presents effective practical capabilities to provide dependable security protection alongside robust operational capability for IoT industrial applications.

Funding source

None.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Prakash, P., Ding, J., Chen, R., Qin, X., Shu, M., Cui, Q., ... & Pan, M. (2022). IoT device friendly and communication-efficient federated learning via joint model pruning and quantization. *IEEE Internet of Things Journal*, *9*(15), 13638-13650. doi: https://doi.org/10.1109/JIOT.2022.3145865

[2] Shrivastava, G., Peng, S. L., Bansal, H., Sharma, K., & Sharma, M. (Eds.). (2020). New age analytics: Transforming the internet through machine learning, IoT, and trust modeling. *CRC Press*. doi: https://doi.org/10.1201/9781003007210

[3] Yang, Q., Chen, W. N., Gu, T., Zhang, H., Yuan, H., Kwong, S., & Zhang, J. (2019). A distributed swarm optimizer with adaptive communication for large-scale optimization. *IEEE transactions on cybernetics*, *50*(7), 3393-3408. doi: https://doi.org/10.1109/TCYB.2019.2904543

[4] Saif, S., Das, P., Biswas, S., Khari, M., & Shanmuganathan, V. (2022). HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare. *Microprocessors and Microsystems*, 104622. doi: https://doi.org/10.1016/j.micpro.2022.104622

[5] Mate, S., Somani, V., & Dahiwale, P. (2024). Secure Data Collection, Aggregation, and Sharing in the Internet of Things. In *Secure Communication in Internet of Things* (pp. 85-93). CRC Press. doi: https://doi.org/10.1201/9781003477327

[6] Sharma, K. (2022). Internet of healthcare things security vulnerabilities and jamming attack analysis. Expert Systems, 39(3), e12853. doi: https://doi.org/10.1111/exsy.12853

[7] Hijazi, N. M., Aloqaily, M., Guizani, M., Ouni, B., & Karray, F. (2023). Secure federated learning with fully homomorphic encryption for IoT communications. *IEEE Internet of Things Journal*, *11*(3), 4289-4300. doi : https://doi.org/10.1109/JIOT.2023.3302065

[8] Abaoud, M., Almuqrin, M. A., & Khan, M. F. (2023). Advancing federated learning through novel mechanism for privacy preservation in healthcare applications. *IEEE Access*, *11*, 83562-83579. doi : https://doi.org/10.1109/ACCESS.2023.3301162

[9] Kumar, R., & Agrawal, N. (2023). Analysis of multi-dimensional Industrial IoT (IIoT) data in Edge–Fog–Cloud based architectural frameworks: A survey on current state and research challenges. *Journal of Industrial Information Integration*, *35*, 100504. doi: https://doi.org/10.1016/j.jii.2023.100504

[10] Hafeez, T., Xu, L., & Mcardle, G. (2021). Edge intelligence for data handling and predictive maintenance in IIOT. *IEEE access*, *9*, 49355-49371. doi: https://doi.org/10.1109/ACCESS.2021.3069137

[11] Kumar, S., Kameswari, Y. L., Rao, K. R., Moram, V., & Shital, S. (2024). Risk Management in IIoT. In *Industrial Internet of Things Security* (pp. 53-70). CRC Press. doi: https://doi.org/10.1201/9781003466284

[12] Bajpai, A., Chaurasia, D., & Tiwari, N. (2024). A novel methodology for anomaly detection in smart home networks via Fractional Stochastic Gradient Descent. *Computers and Electrical Engineering*, *119*, 109604. doi: https://doi.org/10.1016/j.compeleceng.2024.109604

[13] Bharathi, R., Kannadhasan, S., Padminidevi, B., Maharajan, M. S., Nagarajan, R., & Tonmoy, M. M. (2022). Predictive model techniques with energy efficiency for IOT-based data transmission in wireless sensor networks. *Journal of Sensors*, *2022*(1), 3434646. doi: https://doi.org/10.1155/2022/3434646

[14] Chen, H., Huang, S., Zhang, D., Xiao, M., Skoglund, M., & Poor, H. V. (2022). Federated learning over wireless IoT networks with optimized communication and resources. *IEEE Internet of Things Journal*, *9*(17), 16592-16605. doi: https://doi.org/10.1109/JIOT.2022.3151193

[15] Azar, J., Makhoul, A., Barhamgi, M., & Couturier, R. (2019). An energy efficient IoT data compression approach for edge machine learning. *Future Generation Computer Systems*, *96*, 168-175. doi: https://doi.org/10.1016/j.future.2019.02.005

[16] Mao, W., Zhao, Z., Chang, Z., Min, G., & Gao, W. (2021). Energy-efficient industrial internet of things: Overview and open issues. *IEEE transactions on industrial informatics*, *17*(11), 7225-7237. doi: https://doi.org/10.1109/TII.2021.3067026

[17] Shukla, S., Hassan, M. F., Tran, D. C., Akbar, R., Paputungan, I. V., & Khan, M. K. (2023). Improving latency in Internet-of-Things and cloud computing for real-time data transmission: a systematic literature review (SLR). *Cluster Computing*, 1-24. doi: https://doi.org/10.1007/s10586-021-03279-3

[18] Sun, L., Lin, J., Dong, W., Li, X., Wu, J., & Shi, G. (2024). Learning real-world heterogeneous noise models with a benchmark dataset. *Pattern Recognition*, *156*, 110823. doi: https://doi.org/10.1016/j.patcog.2024.110823