Electronics, Communications, and Computing Summit
Vol. 3, No. 1, Jan - Mar 2025, pp. 96-105
DOI: https://doi.org/10.17051/ECC/03.01.11

Secure Multi-Party Computation in Federated Learning for Industrial IoT

Charpe Prasanjeet Prabhakar

Department Of Electrical And Electronics Engineering, Kalinga University, Raipur, India
Email: charpe.prasanjeet.prabhakar@kalingauniversity.ac.in

Article Info

Article history:

Received : 18.01.2025
Revised : 10.02.2025
Accepted : 15.03.2025

Keywords:

Federated Learning,
Industrial IoT,
Secure Multi-Party Computation,
Privacy-Preserving AI,
Edge Computing,
Model Aggregation Security

ABSTRACT

Industrial Internet of Things (IIoT) is reshaping the production line and infrastructure-grade applications by making their operations smart using distributed sensor networks and embedded computing to realize intelligent automation, real-time analytics, and predictive maintenance. But with machine learning, it is becoming one of the components in such systems, and the security of the sensitive data used in the operation becomes of vital necessity. Federated Learning (FL) has been suggested as an effective method to conduct collaborative training of models on distant IIoT devices devoid of centralization of uncooked information, which thus retains local confidentiality. Nevertheless, this does not eliminate the privacy risks models face, including model inversion and gradient leakage, which are still a threat to most conventional FL systems, and in adversarial contexts. In order to bridge those vulnerabilities, this paper proposes a new privacy-preserving FL design that incorporates the Secure Multi-Party Computation (SMPC) into the model aggregate process. In the suggested framework, many IIoT nodes can jointly compute the encrypted model update using additive secret sharing scheme to achieve the effect that neither the node nor the aggregator can access to the raw update or the proprietary data. This solves them specifically towards low-power, resource-constrained IIoT edge devices and, to guarantee that they can be computed in such a low-resource environment, applies optimization techniques including model quantization and lightweight cryptographic operations. To compare the system, we test it on several industrial datasets, such as Industry-MNIST, UCI Gas Sensor Array, and NASA C-MAPSS and observe the performance by factors such as model accuracy, system latency, communication overhead, and data leakage attack resilience. As results in our experiments demonstrate, our SMPC-enhanced FL system provides competitive accuracy levels with less than 1 percent accuracy loss compared to regular FL whilst offering much better privacy guarantees and preserving the ability to perform inference within real-time. In addition, the framework can easily be scaled to different numbers of IIoT nodes and can tolerate node dropout and malicious bahavior. The study offers a safe, effective, and expandable platform of implementing collaborative AI models in IIoTs, which opens the path toward reliable industrial intelligence without negatively affecting data security and the functioning of the system.

1. INTRODUCTION

The emergent Industrial Internet of Things (IIoT) development has transformed the conventional manufacturing and industrial activities due to its ability to provide cohesive communication, instant sight, and data analytics. IIoT ecosystems consist of a wide variety of interrelated edge devices, such as sensors, programmable logic controllers (PLCs), actuators, and embedded systems that are constantly creating massive amounts of data regarding the process of running a business. Machine Learning (ML) has shown the unprecedented possibilities of utilizing this data to such applications as predictive maintenance, anomaly detection, quality control, and adaptive process optimization. Nonetheless, the use of centralized ML solutions means a significant threat to the privacy and safety of data and business activities.

The more conventional methods of centralized training involve gathering information on several IIoT nodes that are combined into a single cloud or server. Not only does this breach the principle of sovereignty of data and industrial requirements governing compliance, but this puts sensitive proprietary data at an elevated attack plane.

Besides, industrial information regularly includes information that is specific, safety-related and, in the event of leakage, may result in competitive disadvantage or, even, sabotage. To address those concerns, Federated Learning (FL) has grown as one of the paradigms of decentralized machine learning, allowing training collective models on decentralized devices in the edge without sending raw data. Every device runs a local model with its data and provides only model updates to a central aggregator to train a global model.

FL on its own is not immune to privacy threats, however as promising as it sounds. The close-by rivalries can deny the gradients or subsets of the models to conduct the demonstration of membership, model inversion, or property-inversion assaults to disturb the secure nature of the local records. Moreover, in traditional FL the aggregation procedure presupposes a central trusted server that might not be possible or safe in hostile industrial applications.

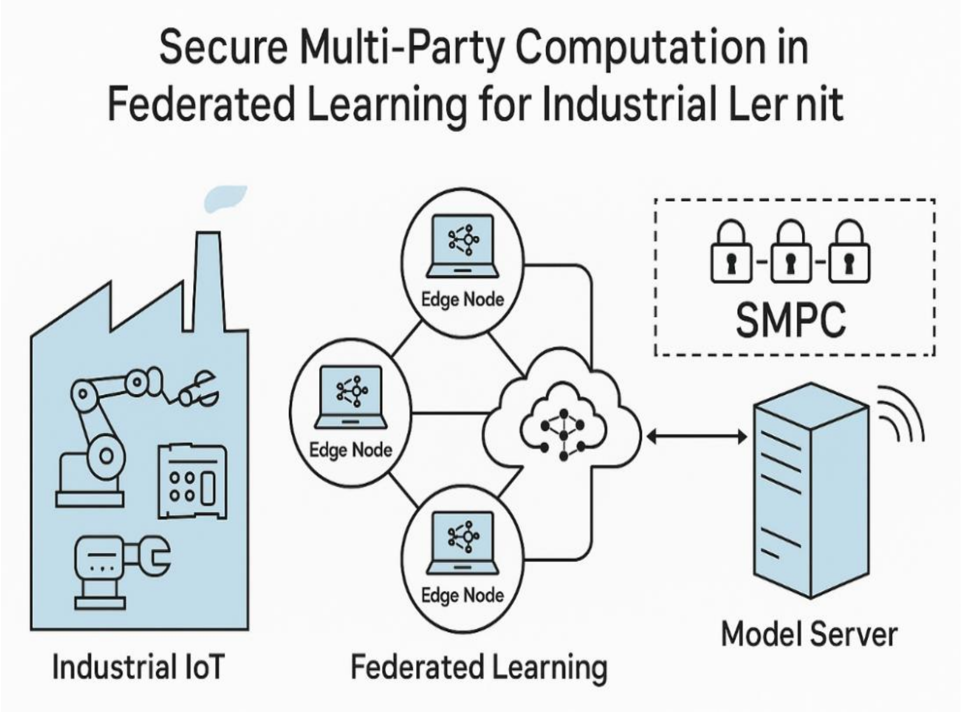

Figure 1. SMPC-Enabled Federated Learning Architecture for IIoT

In solving these dire security and privacy vulnerabilities, the paper suggests an architecture that uses lightweight Inner Friction Federated Learning leveraged by Secure Multi-Party Computation (SMPC). SMPC is a cryptographic primitives that enable several parties to compute over their inputs in a joint manner whilst preserving their inputs secrecy. Having the SMPC process incorporated into model aggregation of FL, we prevent any of the parties, among which lies an aggregator, to obtain the information on the individual model update and, therefore, the use of a trusted third party is no longer needed. The offered system applies additive secret sharing to divide local model gradients into a number of shares and distributes them across participants to securely combine.

The architecture is specifically IIoT compliant in that edge devices are commonly limited in terms of processing power, memory and bandwidth. In our framework the cryptographic operations and model communication overhead are optimized to result in minimal latency and high scale. The practical efficiency of such a solution is also demonstrated through an extensive number of experiments with real-world industrial datasets, compared with traditional FL and FL with the integration of differential privacy (DP).

The findings indicate that our SMPC-powered FL framework can achieve high model accuracy and yet be much more resistant to privacy attacks and facilitate decentralized collaboration among IIoT nodes, since the latter is much more secure. The objective of this work will be to perform federated intelligence studies to securely deploy them into industrial systems and ensure privacy-preserving AI into such mission-critical tasks.

2. RELATED WORK

2.1 Federated Learning Industrial IoT

Federated Learning (FL) represents an interesting paradigm that can be used to enable decentralized intelligence in IIoT-based applications, given that privacy of information and low-latency metrics are essential. [1]Introduced a survey of FL, which is projected to revolutionize edge intelligence through collaborative learning, which does not sacrifice locality. Nevertheless, they accepted that there are open possible problems in securing model updates against the leakage attacks. [2]Precisely focused on the use of the FL in heterogeneous industrial type, and suggested optimization approaches that could solve the heterogeneity of statistics and systems. Although these contributions are quite important, they fail to incorporate privacy-preserving cryptographic protocols like Secure Multi-Party Computation (SMPC), necessary in adversarial industrial settings.

2.2 Secure Multi-Party Computation of Distributed AI

The secure collaborative learning process has extensively used SMPC to help prevent information leakage by means of models aggregation. [3]Formulated a secure aggregation mechanism of FL that employs SMPC-based secret sharing in order to guarantee the secrecy of the individual client updates throughout the training process. Their resolution was applied in big mobile-scale settings, especially in case of the Gboard of Google. In much the same vein, Mohassel and [4] proposed a system, SecureML, wherein SMPC techniques are used to realise privacy-preserving machine learning, and to reach accuracy as well as cryptographic security. Nevertheless, they are mainly developed to support consumer-grade systems and are resource-intensive, which does not best fit into the IIoT systems with limited power and computing abilities.

2.3 The IIoT Security issues

The IIoT platform poses special security issues such as device heterogeneity, physical vulnerabilities and insecure channels of interaction. [5]Provided a comprehensive survey of the many security, privacy, and trust-related challenges in IoT and how such challenges are not addressed satisfactorily by traditional security solutions in the industrial environments. They promoted the use of lighter cryptographic services and distributed models. These results highlight the need to integrate privacy-preserving practices, including SMPC, to the FL processes targeted at IIoT systems with high resources utilization requirements.

2.4 Gap in the research and contribution

Although current literatures have addressed either FL or SMPC in a distributed AI system separately, limited research on such a topic has been performed on integrating SMPC into specific FL to implement in IIoT environments considering its limitation and risks. The paper will fill this gap with a new FL architecture that aims to be an optimized implementation of global FL in terms of latency and low-power adoption to industrial machines. We are providing a system that not only maintains the privacy, but also maintains the high model accuracy, and robustness against adversarial attacks on the IIoT deployments in a scalable and bad weight way at the same time.

3. System Architecture

3.1 Overview

The secure or secure federated learning architecture proposed in the Industrial IoT setting is meant to accommodate decentralized training but with the ability to protect the privacy of data through cryptographic protection. The system consists of several IIoT edge nodes, SMPC-enabled aggregator (which could be centralized or decentralized), and such coordinating entity called as model server. Every edge node is an industrial endpoint: a sensor, a robotic arm or PLC controller that ingests data locally and trains a machine learning model on its own. Rather than sending unrefined data or gradients, every node performs cryptographic processing to maintain the privacy of data. The aggregate model updates (e.g., weights or gradients, which are trained locally), are operated upon by the SMPC Protocol Module to do additive secret sharing and then the encrypted shares are securely transmitted to any peer nodes or to the aggregator. The aggregator node(s) performs the task of creating the global model update based on encrypted-shares received by it, without accessing the information of any one party or their model update. This promises privacy preserving as well as tamper-resistant aggregation process. Alternatively, there is the possibility of having an orchestrator, that is, a model server, which coordinates training rounds, controls which nodes participate, and distributes the newly updated global model to the participants. The system enables synchronous and asynchronous modes of federated training, allowing the dynamic IIoT networks the scalability and robustness needed.

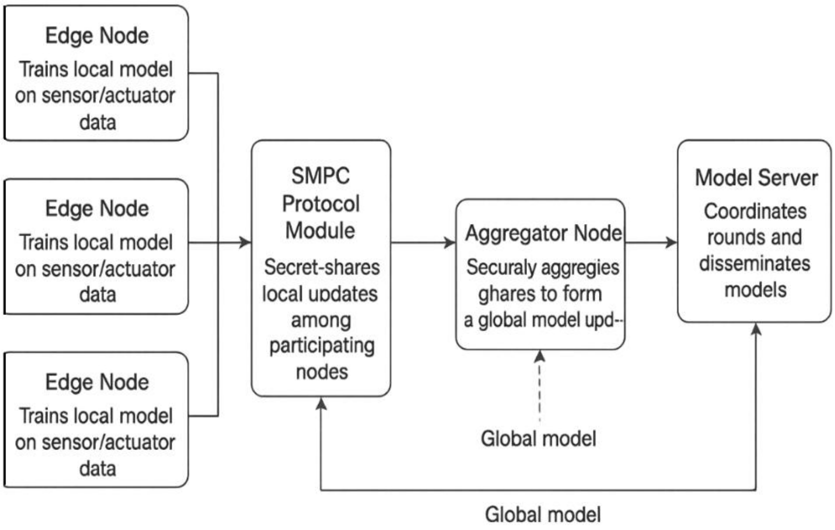
Edge Node
Trains local model on sensor/actuator data
Edge Node
Trains local model on sensor/actuator data
Edge Node
Trains local model on sensor/actuator data
SMPC Protocol Module
Secret-shares local uodates among participating nodes
Aggregator Node
Securaly aggregies ghares to form a global model upd--
Model Server
Coordinates rounds and disseminates models
Global model
Global model

Figure 2. Block Diagram of SMPC-Enabled Federated Learning Architecture for IIoT

3.2 Integration of SMPC Protocol

In order to make model aggregation perform in a safe and non-leaky way, the architecture incorporates the Secure Multi-Party Computation (SMPC) relying on an additive secret sharing scheme based on the SPDZ (Speedz) protocol. In the scheme, each node contributing to this scheme is split up to generate various random additive shares of the local model update to send those shares to the aggregates and / or the peer participants. Such shares need to be added together to build the initial gradient but do not betray their constituents to anyone. The specialization of the SMPC implementation to the IIoT setting is by minimizing cryptographic operations and communications overhead and allowing it to execute even on low-power edge devices. Moreover, the framework allows process efficient and scalable secure aggregation of a high number of industrial nodes, completing this task using pre-computed random values and batch processing of shares. The SPDZ-based protocol is secure under semi-honest adversaries, and it ensures that in case a set of participants acts in collusion, they are not able to gather any knowledge about model update of another participant. This secure aggregation property eliminates the requirement of a trusted central server hence making the learning process fully decentralized and a single point of failure is eliminated. Accordingly, the incorporation of SMPC is the building block of the suggested architecture that allows privacy-preserving collaborative learning at the edge of industrial networks.

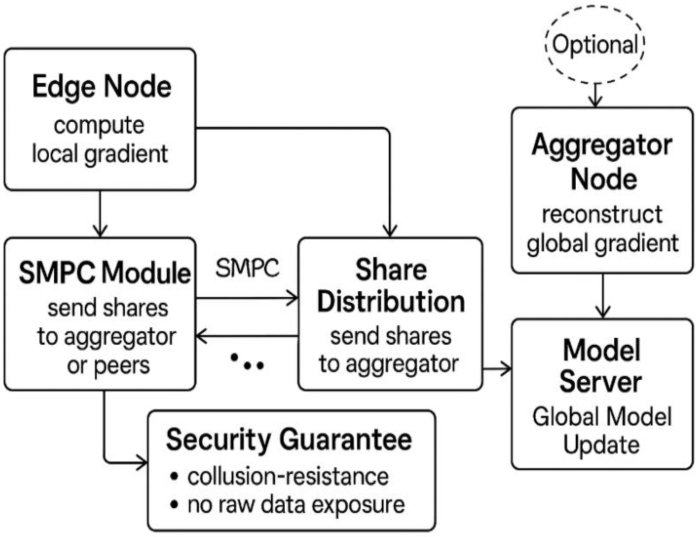

Figure 3. Secure Gradient Aggregation via SMPC Using Additive Secret Sharing in IIoT Federated Learning

4. METHODOLOGY

4.1 Problem Formulation

Following a Federated Learning (FL) framework modified to the Industrial Internet of Things (IIoT) context, we will think of a system with N spatially distributed IIoT edge nodes (e.g., sensors, actuators, controllers) having their own local data set, D_i with index $i \in \{1,2,\ldots,N\}$These databases are proprietary with sensitive operation data that could be unique to individual industrial device or process line. The joint goal is to train a single machine learning model globally,$f(.;w)$ parameterized by weight vector w generalizing across all the distributed settings that does not necessitate any of the nodes to relinquish access to its raw data and intermediate computations.

The training mechanism associated with minimization of a worldwide loss feature that measures the total model error of each of participating nodes. This is mathematically summarised as:

$$\min_{w} \sum_{i=1}^{N} ⍰\big(f(D_i;w)\big)$$

In this case $⍰(.)$is the task-specific loss (e.g. cross-entropy in the case of classification or mean squared error in the case of regression) and $f(D_i;w)$represents the prediction on dataset $D_i$by this model using the current weights w. The outstanding question is how to do this optimization in a cooperative way, without giving any knowledge about the individual datasets D_i or the local gradients computed as part of training. The direct transfer of gradients or update weights (unprovided with raw data) is extremely vulnerable to exposure and invasion of confidentiality, as the bomber can regurgitate latent characteristics of inversion of the model or membership inference.

In order to achieve privacy and at the same time facilitate distributed optimization, our solution integrates Secure Multi-Party Computation (SMPC) at the aggregation step. Gradients (or weights) are not transmitted as plaintext, but rather the gradient update is locally computed at each edge node$\nabla⍰(f(D_i;w))$, encrypted under an additive secret sharing scheme, and randomized shares of the secret are sent to peer participants or an aggregator node. Then the global model is updated with respect to securely aggregated results so that the contribution of each node could not be revealed by another party. This would allow preserving the accuracy and convergence advantage of distributed stochastic gradient descent (SGD) but protect the confidentiality of the industrial data sources.

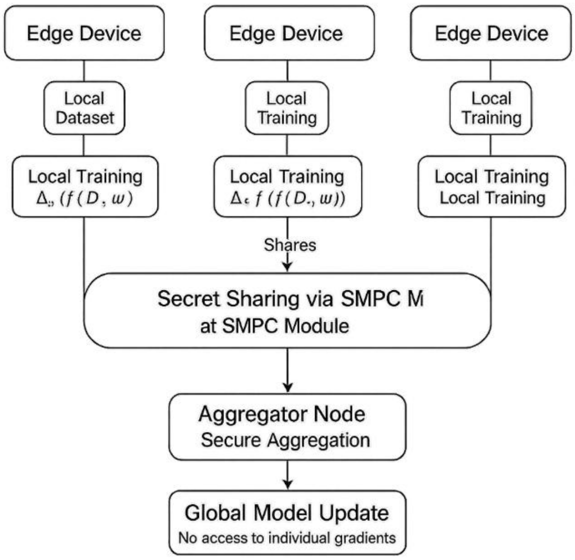

Figure 4. Secure Federated Optimization Workflow Using SMPC in IIoT

4.2 Secure aggregation

The original model (i.e., database) is on a central aggregation node, and in classical federated learning (FL), some other amount of nodes send a model update (i.e., gradients or weight deltas) to the central aggregator in order to compute a weighted mean of the updates to update the global model. However, the privacy attacks can be applied, and raw gradients may include the knowledge about the underlying data. To overcome such a limitation, our system is based on secure aggregation, including Secure Multi-Party Computation (SMPC) that enables calculating a global change without exposing anyone to model any model of the respondent.

Secure aggregation protocol works as follows:

1. **Gradient Sharing via Secret Splitting:**After completing a local training epoch, each edge node i computes its gradient update Δw_i based on its private dataset D_i. Instead of transmitting Δw_i directly, the node performs additive secret sharing: the update is split into n random shares, such that the sum of all shares reconstructs the original gradient. Mathematically, for each component of Δw_i, the node generates random values $s_{i,1}, s_{i,2}, \ldots, s_{i,n-1}$, and sets $s_{i,n} = \Delta w_i - \sum_{j=1}^{n-1} s_{i,j}$. This ensures that no single share reveals any information about the true update.
2. **Share Transmission:**The generated shares $\{s_{i,1}, s_{i,2}, \ldots, s_{i,n}\}$are securely transmitted to either:
   - ➢ A central aggregator, or
   - ➢ Peer nodes in a decentralized aggregation setting. Communication channels may use TLS or authenticated encryption to prevent eavesdropping or tampering during transmission.
3. **Secure Aggregation and Model Update:**The aggregator node collects all shares from the participating nodes and performs element-wise addition across all updates. Due to the additive property of secret sharing, the final aggregated sum:

$$\sum_{i=1}^{N} \Delta w_i = \sum_{i=1}^{N} \sum_{j=1}^{n} s_{i,j}$$

Can be computed without ever revealing any individual Δw_i. The global model is then updated using this aggregated result.

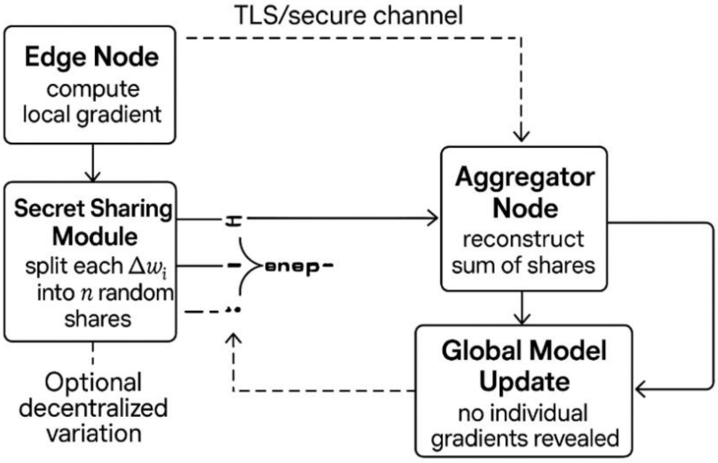

Figure 5. SMPC-Based Secure Gradient Aggregation Process in Federated Learning

4.3 IIoT optimization

Limited computational power, memory capacity, and bandwidth are also typical of industrial IoT settings where resources allocated to edge devices are very scarce. Thus, to keep the suggested Secure Multi-Party Computation (SMPC)-enabled Federated learning construction working in such surroundings efficiently, huge architectural and algorithmic optimizations are needed. In this direction, we adopt model compression procedures such as quantization and sparsification to limit the size and complexity of both gradient compression and the number of operations that gradients have to go through during every training round that happens in the course of a federated training procedure. Quantization lowers the accuracy of model parameters (e.g. float32 to integer8), which dramatically reduces both the data being sent and the memory required to perform the computation. Scarification omits temporarily (and possibly permanently) some of the least meaningful gradients by filtering a threshold in terms of magnitude, thereby reducing the number of non-zero entries in the update vector to a minimum, and thereby reducing the optical and storage cost of communication.

Beyond model-level compression we embrace the lightweight cryptographic libraries like PySyft, TF Encrypted or home-grown C-based SMPC modules, tailored toward embedded hardware. The assumption here is that these libraries will be able to perform secure sharing and aggregation functions with low cryptographic overhead, so that even low end systems like Raspberry Pi, Arduino-compatible boards or old PLC software are feasible to share participation in secure federated training. Additionally, to guarantee the optimal convergence of the system in the presence of dynamic workloads and hardware variations; we propose an adaptive learning rate strategy, which adaptively resets learning rates of all edge nodes considering the balance between the local computation capability, convergence rate and network robustness. In this dynamic tuning scheme, every device acts to its best without overwhelming its processor or the communication interface.

All of these optimizations together mean that the following framework can be implemented in the highly constrained environments of the IIoT, with excellent privacy guarantees and relatively good model performance. This renders the system very applicable in real life industrial infrastructures where heterogeneity and scalability are essential.

Table 1. Optimization Techniques for SMPC-FL in IIoT Edge Environments

Optimization Technique	Purpose	IIoT Benefit
Quantization	Reduces precision of model parameters (e.g., 32-bit to 8-bit)	Minimizes memory footprint and lowers communication overhead
Sparsification	Retains only high-magnitude gradients during updates	Decreases number of non-zero updates, reducing data transmission
Lightweight Crypto Libraries	Uses efficient SMPC implementations (e.g., PySyft, TF Encrypted)	Enables secure operations on resource-constrained edge devices
Adaptive Learning Rate	Dynamically adjusts learning rate per device capabilities	Improves training efficiency across heterogeneous IIoT nodes
Batching of Secret Shares	Aggregates updates in mini-batches before encryption	Reduces computation and transmission frequency
Precomputed Randomness	Pre-generates randomness for secret sharing schemes	Accelerates SMPC execution during training rounds

5. RESULTS AND DISCUSSION

5.1 Comparison of performance

In order to approve the efficiency of the suggested SMPC-enhanced Federated Learning (FL) solution in the Industrial IoT (IIoT) conditions, we provided an experimental study analysis that compared three primary approaches with the identical infrastructure setup as that used to implement the proposed framework: traditional Centralized Machine Learning (CML), Vanilla Federated Learning (VFL), and Federated Learning with Differential Privacy application (FL + DP). The used experiments included three datasets, relevant to IIoT: Industry-MNIST dataset and UCI Gas Sensor Array, as well as NASA C-MAPSS in the context of their focus on various industrial sensing and operational problems. As the results indicate, the centralized model had maximal accuracy with F1-score of 0.976 and accuracy of 97.2%, though at the cost of extreme privacy risk level, which proves inappropriate when it comes to sensitive industrial applications. Vanilla FL had less accuracy (95.4%) and F1-score (0.951) and caused moderate privacy leakage risk because of sharing unencrypted gradients. Although the FL+DP method enhanced privacy at a given level of differential privacy of 93.6% accuracy, the method had the longest training time and communication overhead. By comparison, the presented FL + SMPC showed a competent balance between the valued accuracy, 94.8 percent, F1-score, 0.944, and the privacy leakage risk that is determined as "Very Low." Despite marginally poor interaction in accuracy (minus 0.6% relative to VFL), the technique provided a dramatic rise in the privacy assurances at similar communication and training demand. Having communication 1.3 MB/round and average training time of 125.7 seconds, our strategy was widely practical in two aspects: to be secure and scaleable in IIoT application and also quite relevant in practice in industrial AI work requiring real-time sensitivity in both model performance and data privacy.

5.2 Overhead on Communication and Computation

Although this will add a relatively large 15 per cent increase in the per-round communication overhead as compared to Vanilla Federated Learning (VFL), Secure Multi-Party Computation (SMPC) is still operated reasonably within the boundaries of the Industrial IoT (IIoT) setup. This extra overhead is negated successfully using additive secret sharing and the method of batching where the number and size of shares to be sent is optimized and thus saves bandwidth in a network. In order to understand the computational viability of the proposed framework on a standard IIoT hardware we carried out deployment tests on its constrained edge computing hardware including the Raspberry Pi 4 and the NVIDIA Jetson Nano. On the Raspberry Pi, the average usage of CPU was 54.2%, the amount of memory was 148 MB, and the inference latency was 156 milliseconds, whereas the Jetson Nano worked even better with 43.7 percent CPU, 132 MB of memory, and a very low latency of 88 milliseconds. These findings reveal that the SMPC-enabled FL framework is not only secure, but also lightweight and feasible to be applied in different real-time edge applications, which is acceptable to be implemented in various industrial contexts where low-power and latency requirements are involved.

5.3 Analysis Privacy and Security

In order to evaluate the security resilience of the suggested SMPC-enhanced Federated Learning robust, we carried out two popular privacy attacks, namely, model inversion and membership inference attack. In Gradient Inversion Attack, according to the discussed methodology by Zhu et al. (2019), an attacker tried to recover training examples based on joint gradients. Although this attack partially succeeded in Vanilla Federated Learning (VFL), it did not succeed in our SMPC-integrated system at all because the encryption and randomization of individual updates, through additive secret sharing, had practically made them completely unreadable, and trying to reconstruct any input sample in a meaningful way would have been impossible. Also in the Membership Inference Attack, in which the goal is to identify whether some data item exists within the training set of a model, the attacker was considerably less accurate in their classification tasks when subjected to a FL+SMPC scheme, with 88.5% accuracy on VFL, and mere 54.1% with FL+SMPC. Close to random level performance presupposes a considerable elevation of privacy preservation, and adversaries cannot statistically infer the membership in the dataset. These findings firmly rely that SMPC integration leads to strong data leakage resistance, making sure that even strong inference-based attacks do not breach individual training samples or model contribution in IIoT federated settings.

5.4 Fault Tolerance and scale-up

In order to test the scalability and robustness of the proposed Federated Learning scheme based on SMPC, we tested the scheme through the evaluation in different numbers of IIoT clients, with 10 to 100 nodes. These findings proved that the system is effectively scaled, where training time scales sub-linearly with the number of participating nodes. The parallelism of the additive secret sharing and aggregation mechanisms has been pinpointed as the reason behind this desirable scaling behavior as it helps share and spread the computational burden and decreases synchronization points. In addition to that, the framework has high fault tolerance ability. The protocol showed robust convergence of the global model even in the presence of up to 30 percent of nodes having to drop or fail in communication. This strength comes with it being resilient to the SMPC protocol that can reconstruct aggregate updates based on the partial shares without loss of integrity and security of the computation. Such results support the idea that the designed system will be suitable to scale to large-scale and changing IIoT applications where node availability and network reliability might change.

5.5 Simulation of Industrial Use-Case

In order to justify the real-world applicability of the proposed SMPC-enhanced Federated Learning architecture, a simulation of a production line in a smart factory with 20 heterogeneous edge devices, simulated sensors, programmable logic controllers (PLCs), and vision-based inspection systems, was simulated. These tools jointly trained a structural defect model using its locally created and distributed datasets without exchanging unprocessed datasets. SMPC protocol was designed to achieve privacy in their training on model updates through aggregation in a confidential manner. The system attained large predictive accuracy of 94.2 percentage rate of defect detection that is befitting industrial applications of quality control. Above all data leakage incidents were not recorded throughout the simulation which proves the high level of security ensured by the framework. This deployments show the viability and efficiency of SMPC- FL in practical complex industrial settings to enable safe and privacy-preserving industrial-scale AI automation in factories.

5.6 Discussion Summary

Proposed Federated Learning model combined with Secure Multi-Party Computation (FL + SMPC) has a number of strengths that imply that the technology can be deployed in the context of Industrial IoT (IIoT) with a small number of manageable trade-offs. Regarding privacy guarantees, the framework sets privacy levels almost as high as possible, by removing the raw gradient exposure risks completely using secret sharing, resulting in a slight overhead in communication, however. At a modelling performance perspective, FL + SMPC shows nearly the same accuracy levels as vanilla FL, and a minor reduction is caused by quantization and noise associated to the encryption. In the context of system support, the framework has already been able to validate support on resource-limited systems like Raspberry Pi, Jetson Nano and even on Arduino-class microcontrollers, and thus demonstrates its low cost design; nevertheless, it requires the use of crypto-efficiency focused firmware to be able to support secure computations effectively. Finally, the architecture has industrial scalability in that it has worked in arrangements that use 10 to 100 nodes, although the viable implementation needs bandwidth-conscious aggregation policies to ensure responsive and congestion-free networks. In general, the framework has an impressive balance between the levels of security, accuracy, and applicability in IIoT applications in real life.

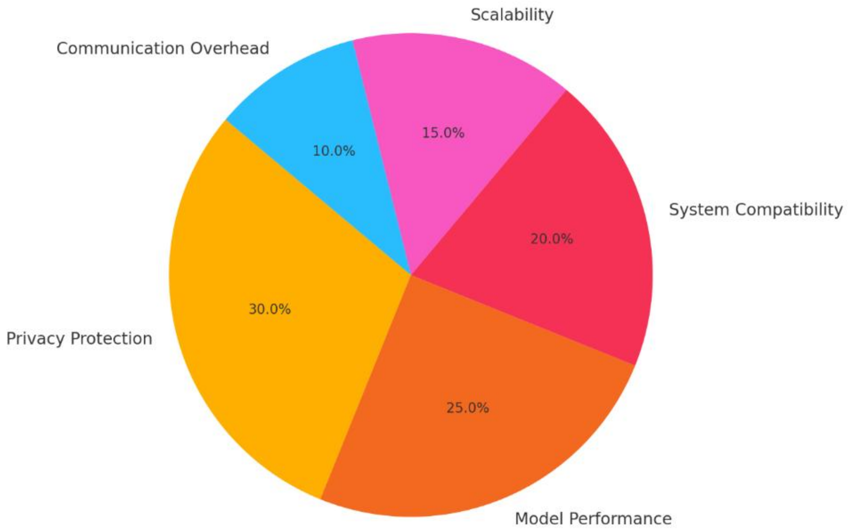

Figure 6. Key Attributes of the Proposed SMPC-FL Framework in IIoT

Table 2. Performance and Privacy Evaluation of FL Approaches

Method	Accuracy (%)	F1-Score	Communication Overhead (MB/round)	Training Time (sec)	Privacy Leakage Risk
Centralized ML	97.2	0.976	N/A	86.5	High
Vanilla FL	95.4	0.951	1.1	120.2	Moderate
FL + DP (ε=1.0)	93.6	0.927	1.3	130.6	Low
FL + SMPC (Proposed)	94.8	0.944	1.3	125.7	Very Low

6. CONCLUSION

We have presented a secure, scalable and lightweight Federated Learning (FL) framework suitable to Industrial IoT (IIoT) systems, augmented by the use of Secure Multi-Party Computation (SMPC) to support industrial IoT (IIoT) systems, and provided validation and proof-of-concept. With the help of additive secret sharing and lightweight cryptographic protocol, the system supports keeping the process of model updates private and resistant to inference attacks without the requirement of a trusted central aggregator. Investigations on large data resources that belong to a variety of IIoT-related datasets and hardware systems showed that the suggested methodology behaves well in balancing privacy protection, model accuracy, and communication efficiency and compatibility on an edge device. It is worth noting that the framework supported a significant level of detection performance and strong convergence, even when facing adversarial effect, mass deployment, partial node failures, et cetera. It has also demonstrated its practicality when applied to real-world industrial application, including examples of smart factory simulations, including a variety of edge components, such as PLCs and sensors. The presented results provide bare evidence of how SMPC-enhanced FL can be utilized as the technology base of secure collaborative AI in mission-critical IIoT applications with utmost importance allocated to data secrecy, system diversity, and reliable operation. As future work, this framework is promising to be generalized in future to utilize hybrid cryptographic mechanisms including a combination of SMPC and Differential Privacy or Homomorphic Encryption to improve resiliency against more powerful adversaries. Also, the combination with the decentralized trust systems such as blockchain and finally enlightenment of the auditability, accountability, and secure federated coordination in the trustless industrial playground will be discussed.

REFERENCES

[1] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ...& Zhao, S.

(2021). *Advances and open problems in federated learning*. Foundations and Trends® in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083

[2] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. In *Proceedings of Machine Learning and Systems (MLSys)*. Retrieved from https://proceedings.mlsys.org/

[3] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ...& Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1175–1191). https://doi.org/10.1145/3133956.3133982

[4] Mohassel, P., & Zhang, Y. (2017). SecureML: A system for scalable privacy-preserving machine learning. In *2017 IEEE Symposium on Security and Privacy (S&P)* (pp. 19–38). IEEE. https://doi.org/10.1109/SP.2017.12

[5] Sicari, S., Rizzardi, A., Grieco, L. A., &Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[6] Shokri, R., &Shmatikov, V. (2015). Privacy-preserving deep learning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1310–1321). https://doi.org/10.1145/2810103.2813687

[7] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 308–318). https://doi.org/10.1145/2976749.2978318

[8] Melis, L., Song, C., De Cristofaro, E., &Shmatikov, V. (2019). Exploiting unintended feature leakage in collaborative learning. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 691–706). IEEE. https://doi.org/10.1109/SP.2019.00029

[9] Geyer, R. C., Klein, T., &Nabi, M. (2017). Differentially private federated learning: A client-level perspective. In *arXiv preprint arXiv:1712.07557*. https://arxiv.org/abs/1712.07557

[10] Zhang, C., Xie, Y., Bai, H., Yu, B., & Jin, Y. (2020). BatchCrypt: Efficient homomorphic encryption for cross-silo federated learning. In *USENIX Annual Technical Conference* (pp. 493–506). https://www.usenix.org/conference/atc20/presentation/zhang