Orclever Proceedings of Research and Development

https://doi.org/10.56038/oprd.v5i1.574

OR CLEVER Science & Research Group

Conference Article

Analysis of OPC Data Using Federated Learning: An Evaluation of Performance and Privacy

Süleyman Burak ALTINIŞIK[1*], Turgay Tugay BİLGİN[2]

[1] trex Dijital Akıllı Üretim Sistemleri A.Ş., 0009-0005-0987-1798, burakaltinisik@trex.com.tr
[2] Bursa Teknik Üniversitesi, 0000-0002-9245-5728, turgay.bilgin@btu.edu.tr
* Correspondence: burakaltinisik@trex.com.tr; Tel: +90 543 312 9155

Received 27 October 2024
Received in revised form 01 December 2024
In final form 12 December 2024

4th International Conference on Design, Research and Development
(RDCONF 2024)
December 19 - 20, 2024

Reference: Altınışık, S. B., & Bilgin, T. T. (2024). Analysis of OPC data using federated learning: An evaluation of performance and privacy. Orclever Proceedings of Research and Development, 5(1), 410-426.

Abstract

This study examines the benefits of applying federated learning (FL) technology to OPC (Operational Performance Control) systems within industrial automation and data analysis processes. FL enables each production facility to process its data locally while only transmitting model parameters to a central server, thereby preserving data privacy. This approach provides significant advantages in industrial environments, particularly concerning data privacy and communication costs. The study evaluates FL's potential to ensure data privacy, reduce communication costs, improve efficiency in training time, and deliver high performance in predictive maintenance and quality estimation. Model performance was analyzed using accuracy, F1 score, precision, and loss metrics; the results demonstrated that FL achieved a 90% accuracy rate, offering competitive performance compared to centralized modeling. In predictive maintenance and quality analysis specifically, FL achieved 85-88% accuracy while reducing network data load by 65%. These findings validate that FL provides a secure, cost-effective, and efficient solution for industrial data analysis processes by eliminating the need for centralized data collection. In conclusion, FL and OPC integration supports data privacy, cost savings, and communication efficiency in industrial processes. The study highlights that FL could become a *prevalent technology in industrial data analysis, establishing a new standard particularly in digital manufacturing processes.*

Keywords: Federated Learning (FL), Operational Performance Control (OPC), Data Privacy, Industrial Automation, Predictive Maintenance

1. Introduction

Operational Performance Control (OPC) systems are critical tools widely used in industrial production processes to monitor performance, optimize processes, and enhance production efficiency. These systems use data obtained from numerous sensors within the production process to monitor and evaluate machine performance and product quality in real time [5]. With the advent of Internet of Things (IoT) technologies, the volume and diversity of this data have increased rapidly, making data processing increasingly complex. However, as OPC systems are structured to transmit data directly to a central server, they face significant challenges, such as data privacy and security risks [8]. At this point, federated learning (FL) technology offers an effective solution to these issues by providing a decentralized data processing approach. FL preserves data privacy and reduces communication costs by processing data on local devices and transmitting only model parameters to the server [1] [2]. One of the primary advantages of FL is that it allows each device or sensor to conduct local model training without centralizing the data. Consequently, only the updated model parameters are transmitted to the central server. This approach minimizes privacy risks while simultaneously reducing network bandwidth usage and communication costs [18]. The structure of FL not only significantly contributes to ensuring data privacy but also offers a substantial opportunity to enhance cost efficiency and perform rapid analyses in production processes [4]. These advantages are especially important in industrial environments where numerous sensors are aggregated, as the continuous transfer of data to a central server can place a heavy load on the network infrastructure and raise concerns about data privacy [15]. Federated learning addresses these security and efficiency issues, playing a crucial role in industrial data analysis processes. In industrial IoT (IIoT) environments, security and privacy are essential for protecting sensitive data. Data collected in IIoT environments includes machine operation information, proprietary production process data, and facility-based performance data. As this data is commercially valuable, it requires protection against unauthorized access. However, traditional centralized data collection methods are more susceptible to privacy breaches and data leakage risks due to the concentration of all data in one location [9]. With FL, processing this data locally on each device eliminates the need for centralized data collection, significantly reducing security risks. FL technology provides highly effective solutions with privacy-preserving mechanisms, particularly in sectors such as healthcare, finance, and industry, where data privacy is paramount [3]. Additionally, using supplementary methods like differential privacy (DP) further enhances data privacy. DP techniques prevent unauthorized learning of user data in FL applications, ensuring high levels of privacy even when model parameters are shared [15]. Another advantage FL offers to IIoT environments is the reduction in communication costs. In traditional approaches, the continuous transmission of large volumes of data to a central server excessively utilizes network bandwidth and leads to communication delays. The decentralized structure of FL minimizes data transfer by only transmitting model parameters to the server. This prevents potential network congestion, enabling a faster and more efficient management of the data transmission process [16]. In this regard, FL not only ensures data security but also facilitates more time- and cost-effective management of industrial processes. FL has significant cost-saving potential in scenarios with high data density, especially in operational performance monitoring systems [11]. Another significant advantage of FL is enabling each facility to train its model on its own data. FL allows each facility to develop customized models by utilizing local data, improving model accuracy and overall performance [13]. This customization, when considering the unique characteristics of each facility, yields more realistic and effective results. In cases where industrial facilities operate in different locations or under varying conditions, FL's local model update feature enables each facility to optimize according to its operational requirements [14]. Within the context of OPC systems, FL's contribution to accelerating reliable data analysis processes is also noteworthy. In traditional centralized modeling methods, each data piece must be sent to a central server, and this process can become time-consuming due to data transfer and central model updates. FL minimizes this duration by combining locally trained models on the central server [2]. Consequently, analysis times are shortened, allowing for quicker actions. In cases such as sudden changes or faults in the production line, rapidly updated models support more efficient decision-making, thereby enhancing production efficiency [4]. In conclusion, federated learning addresses the growing need for security and efficiency in industrial IoT systems. With advantages such as data privacy, reduced communication costs, and rapid model updates, FL provides a valuable solution for operational performance monitoring and optimization. Offering cost benefits while ensuring privacy in industrial data analysis, FL emerges as an effective alternative in increasingly complex production processes [1] [4] [18].

2. Literature Review

Federated learning (FL) is a method initially developed by Google that enables the training of machine learning models on mobile devices while preserving data privacy [1]. The primary aim of FL is to process data locally on devices rather than transferring it to a central server, and then to combine model parameters on a central server [2]. This feature allows FL to play a significant role in enhancing data privacy and security in industrial applications. Additionally, FL is widely used in fields such as healthcare, finance, retail, and education [3]. Research shows that FL reduces data transfer costs by eliminating the need for centralized data collection [4]. However, the distributed nature of FL requires minimizing communication costs and addressing challenges related to device heterogeneity [18]. Operational Performance Control (OPC) encompasses data collection and analysis systems aimed at enhancing efficiency and quality in industrial production processes [5]. OPC systems gather sensor data and device status information to perform performance analyses and integrate with decision support systems [6]. OPC has a data-driven structure designed to increase efficiency in the production process and to detect quality issues proactively [7]. However, the reliance of OPC systems on data collected on a central server raises various concerns regarding data privacy and security [8]. In this context, FL has the potential to enhance the efficiency of OPC systems while preserving data privacy [9]. In industrial applications, predictive maintenance and quality estimation are areas where both OPC and FL methods can be effectively applied. Predictive maintenance aims to monitor the performance of machines and equipment to anticipate failure risks [10]. The use of FL in predictive maintenance applications ensures data security by processing data locally [11]. Research on predictive maintenance and quality estimation focuses on detecting potential faults in the production process through real-time data analysis and enhancing production efficiency [12]. Analyzing sensor data using FL, in particular, contributes to a centralized predictive model while preserving the local data of each device [13]. When OPC systems are combined with FL, they offer a strong synergy in enhancing the performance of industrial production processes and ensuring data privacy. By safeguarding data privacy and security in OPC data through FL, production data can be analyzed without centralization, thus preserving data confidentiality [14]. This integration holds promise, particularly for reducing costs and increasing efficiency in large-scale production facilities [15]. Additionally, this method is regarded as an effective solution for synchronizing across multiple devices and minimizing data transfer costs [4]. Finally, studies in the field of FL and OPC indicate that the combination of these two technologies creates a new paradigm in industrial analysis and data security processes [16]. The success of FL on heterogeneous data sources and the contributions of OPC to industrial production processes highlight the importance of using these two technologies together [17]. In this context, the integration of FL and OPC can contribute to next-generation digital production processes by providing secure, efficient, and cost-effective solutions in industrial data analysis.

3. Materials and Methods

The client and server codes used in this study were developed based on the federated learning (FL) architecture, enabling data to be processed on local devices without being transferred to a central server. Within the FL application, each client performs model training on its local data and transmits the updated model parameters to the central server. The server aggregates and optimizes the incoming updates to create a general model, which is then sent back to the clients. In this process, communication protocols and data transfer methods are designed to preserve data privacy.

3.1. Data Collection and Preparation

The data collection and preparation process is of critical importance in federated learning applications. For the FL model to operate securely and efficiently, data must be processed accurately and completely. The data obtained from OPC systems include various performance indicators, such as temperature, speed, and vibration, which reflect the production process. Each production facility collects this data through its own devices, and thanks to the privacy advantages offered by FL, data is not directly transferred to the central server; only model updates are transmitted. The collected data may contain issues such as missing data and anomalies. Therefore, in the data preparation process, preprocessing steps were applied to fill in missing values and improve data accuracy. Missing data were completed using forward interpolation, ensuring a continuous data flow during the model training process. For anomaly detection, machine learning algorithms were used to filter out erroneous data, thereby enhancing the model's accuracy. The data used in this project are in time series format and consist of measurement values obtained from various sensors. During model training, this data was used as a dataset for the FL model, defining both features and target variables.

Table 1: Dataset Column Descriptions and Types

Parameters	Description	Data Type
STOCKID	ID of the product produced	int

EMPLOYEEID	Personnel ID working during production	int
BolgeGercek1	Value from tag	float
BolgeHedef1	Value from tag	float
BolgeGercek2	Value from tag	float
BolgeHedef2	Value from tag	float
BolgeGercek3	Value from tag	float
BolgeHedef3	Value from tag	float
BogazGercek	Value from tag	float
BogazHedef	Value from tag	float
CekiciAktif	Value from tag	float
AkimGercek	Value from tag	float
EkstruderAktif	Value from tag	float
VidaDevirGercek	Value from tag	float
HatHiziGercek	Value from tag	float
HatBaslatGercek	Value from tag	float
HavuzGercek	Value from tag	float
HavuzHedef	Value from tag	float
BasaGercek1	Value from tag	float
BasaHedef1	Value from tag	float
KelepceGercek	Value from tag	float
KelepceHedef	Value from tag	float
MesafeGercek	Value from tag	float
MesafeHedef	Value from tag	float
SicakCapGercek	Value from tag	float
SogukCapGercek	Value from tag	float
Hazne1	Value from tag	float
Hazne2	Value from tag	float
Hazne3	Value from tag	float
Hazne4	Value from tag	float
Spark	Value from tag	float
MotorAkimi	Value from tag	float

The parameters in Table 1 represent the primary features and target variables used during model training. The steps for handling missing data and anomaly detection have enhanced the reliability of data in these fields, leading to more accurate results.

3.2. Federated Learning Architecture

Federated learning (FL) is a structure that offers a decentralized data processing process, ensuring data privacy while also optimizing communication efficiency and computational power. This architecture enables data to be processed on local devices without being transferred to a central server, with only model updates sent to the central server [1]. This approach minimizes privacy breaches by keeping users' data on their devices and ensures compliance with regulatory requirements. In the FL architecture, there is a central server and numerous local clients (e.g., mobile phones, IoT devices). The server coordinates the updating of the global model and carries out this process in specific steps:

- **Initialization Phase**: The server creates an initial model and sends it to the selected clients.
- **Local Training**: Clients perform a set number of model training steps on their local data.
- **Model Updates**: Clients send the trained model updates (e.g., weight changes) back to the server.
- **Model Aggregation**: The server combines the received updates using a weighted average or another algorithm and updates the global model.
- **Cycle Repetition**: The updated model is redistributed to the clients, and the process is repeated.

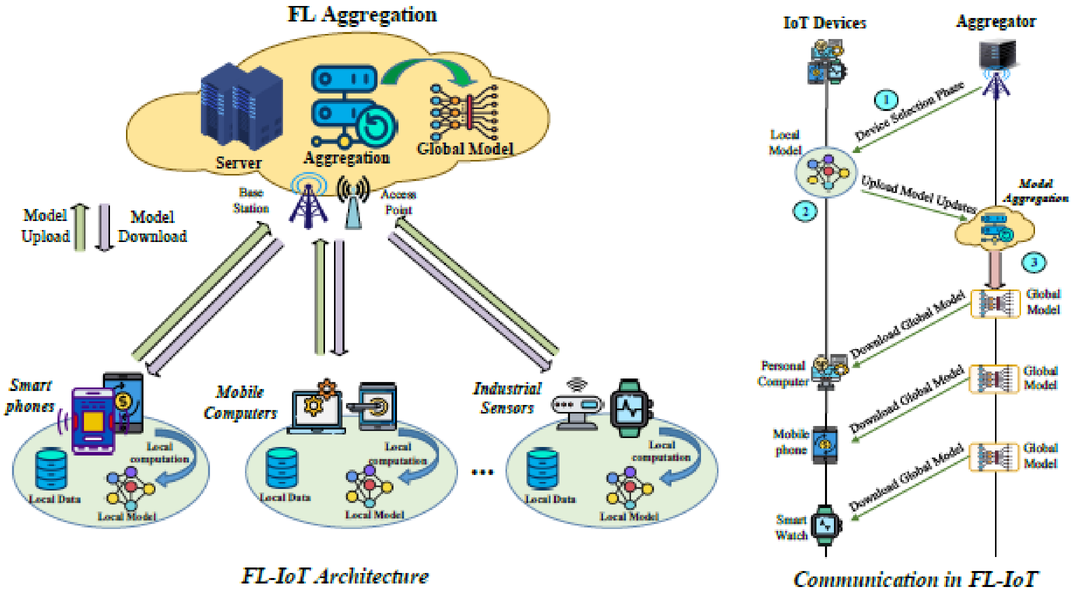

Figure 1: Federated Learning Architecture in General

As shown in Figure 1, the Federated Learning architecture is implemented step by step in this manner. There are three main types of this architecture:

3.2.1. Horizontal Federated Learning

Horizontal FL, as shown in Figure 2, is used in scenarios where devices representing different users participate with the same data features. For example, model training conducted on the phones of different users using the same mobile application is an instance of horizontal FL. In this scenario, the dataset on each client contains similar features, but the data is spread across different users.

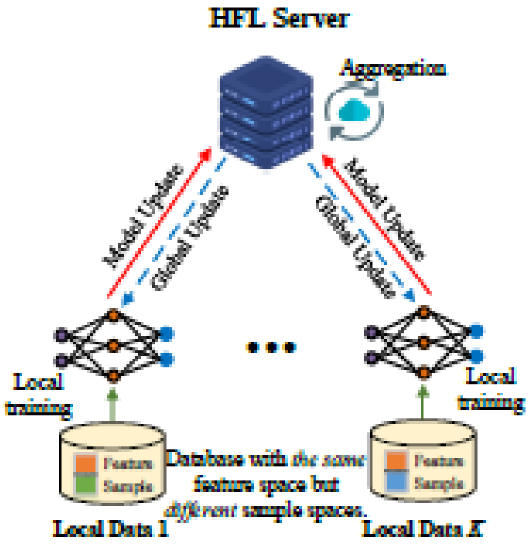

Figure 2: Horizontal Federated Learning Architecture

3.2.2. Vertical Federated Learning

Vertical FL, as shown in Figure 3, enables model training among organizations representing the same users but with different data features, without sharing data. In this architecture, each participant holds different types of data. For example, joint model training between a bank's customer financial information and a retail company's shopping information for the same customers is an instance of vertical FL. This approach provides richer data representation and allows the model to make more complex predictions.

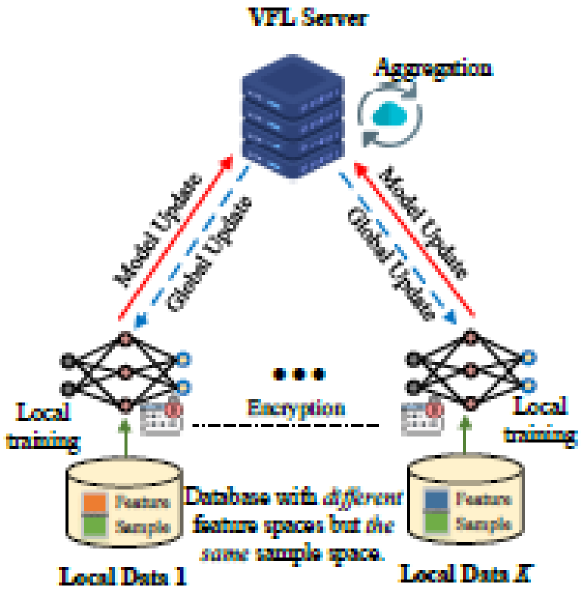

Figure 3: Vertical Federated Learning Architecture

3.3.3. Transfer Federated Learning

Transfer FL, as shown in Figure 4, is an architecture that facilitates the sharing and transfer of knowledge between different tasks. In this method, a model previously trained on one dataset or problem is adapted to another dataset and task. It is particularly useful in situations with limited data or where heterogeneous data exists.

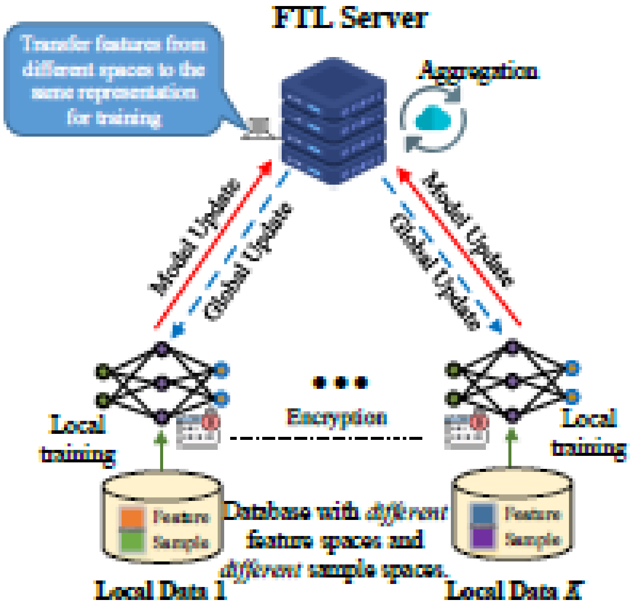

Figure 4: Transfer Federated Learning Architecture

In this study, horizontal FL is adopted. Each facility performs independent model training using local data and only transmits the updated model parameters to the server. The central server aggregates parameter updates from all clients to create a general model. The client and server codes used in the project enable clients to train models on local devices and transmit only the model parameters to the server. This architecture enhances data security by processing data without centralization and reduces communication costs [4]. The code used in the project's client and server structure includes transmitting model updates from the client side to the server and aggregating parameters on the server side to update the global model. The following methods summarize this process:

- **Local Model Training**: Each client performs independent model training using local data.
- **Transmission of Model Parameters to the Server**: After training, clients transmit the updated model parameters to the server.

3.4. System Architecture

Federated Learning (FL) enables machine learning model training across different data sources or clients through its distributed structure. FL architectures are divided into various types, each offering unique advantages in terms of data privacy, communication efficiency, and system management. The most common architectures include centralized, hierarchical, and fully decentralized FL structures. The fundamental operational characteristics and benefits of each architecture can vary depending on system requirements. In the Centralized Federated Learning (Centralized FL) structure, all clients send model parameters directly to a central server. The central server aggregates the parameters from clients, updates the model, and then sends this model back to the clients. The primary advantage of the centralized structure is the high level of control over the model updating and parameter aggregation processes (Kairouz et al., 2019). In the Hierarchical Federated Learning (Hierarchical FL) structure, clients first send model parameters to intermediate servers; these intermediate servers aggregate the model parameters and then forward them to a central server. This architecture is advantageous for reducing communication load in large-scale distributed systems; however, the addition of intermediate servers can introduce additional challenges in terms of management and security (Bonawitz et al., 2019). In the Fully Decentralized Federated Learning (Fully Decentralized FL) structure, there is no central server, and clients share model parameters directly with each other. This structure is advantageous for preserving data privacy as it does not require a central authority; however, due to communication complexity and management challenges, it can be difficult to implement in large-scale systems (Li et al., 2020). In this study, a centralized federated learning (centralized FL) architecture was used. The primary reasons for choosing the centralized FL structure are its alignment with the security, data processing efficiency, and ease of management requirements in OPC data analysis. Centralized FL provides advantages over other architectures, particularly in terms of data security and privacy. OPC data contain sensitive information about production processes and operational performance. Since the centralized FL structure ensures that all data remain local on the clients, it offers significant protection for data privacy. In hierarchical or fully decentralized structures, direct data sharing between clients or the use of intermediate servers may be required, which could pose privacy risks for sensitive data. By sending only model parameters to the server, the centralized structure minimizes security risks (McMahan et al., 2017). Additionally, the centralized FL architecture is advantageous for optimizing data processing and computational load. The central server collects and aggregates model parameters from the clients, allowing clients to participate with only limited processing capacity. In the hierarchical structure, the additional load on intermediate servers, and in the fully decentralized structure, continuous communication between clients may strain computational power in large-scale distributed systems. The centralized structure, however, ensures efficiency, especially in OPC clients with limited computational power (Hard et al., 2018). The collection of model parameters through a central server in the centralized architecture makes the entire system more modular and manageable. In large-scale systems, the centralized structure stabilizes model updates and facilitates accurate parameter aggregation. Synchronization issues among clients in the fully decentralized structure can complicate system management, while the hierarchical structure requires additional management for intermediate servers. Centralized FL eliminates most of these challenges, enhancing process traceability and management (Li et al., 2020). The centralized federated learning architecture is also suitable for optimizing communication costs. Since OPC systems generate large amounts of data, continuous data transfer can incur high costs. In the centralized FL structure, communication efficiency is achieved because clients only transmit model parameters. In hierarchical or fully decentralized structures, direct data exchange between clients may be necessary, which can increase communication costs (Bonawitz et al., 2019). The client code used in the project enables each client to perform local model training using its own data and to send only the updated model parameters to the central server. This prevents data sharing between clients and allows each client to retain its data locally. The server code performs a central aggregation process; it collects the model parameters from all clients, aggregates these parameters, and distributes the updated global model back to the clients. This structure ensures the secure processing of OPC data while offering communication efficiency and ease of management.

The choice of a centralized federated learning architecture in this study is the most suitable solution for analyzing OPC data, as it provides data privacy, ease of management, and communication efficiency. The centralized structure prevents data sharing between clients while safeguarding data security, balances processing load to enhance performance, and simplifies process management. This choice maximizes the potential of federated learning applications in industrial data analysis and offers the ideal architecture for security-focused systems such as OPC. Federated learning (FL) model training is based on the principle that each client independently trains a model on its local data. In this study, each facility updates its model solely on its own data, and the resulting model parameters are transmitted to the central server. During the local training process, the SGD (Stochastic Gradient Descent) algorithm is used to optimize each client's data. This optimization method on the client side ensures effective model updates and plays a crucial role in the FL process. To enhance communication efficiency, the FL model requires that model parameters be compressed before being sent to the server. Compressing model updates reduces the amount of data transmitted over the network, lowering communication costs and increasing system efficiency. In this study, the updated model parameters were compressed before being transmitted to the server, thereby optimizing network data load. Compression is a notable approach in FL for improving network efficiency in large-scale applications. On the server side, updates from clients are aggregated using a weighted method, and the general model parameters are updated. This process is achieved by the central server collecting each update at a specific frequency and optimizing it to improve the model's overall accuracy. Weighted aggregation balances the influence of clients on the model, enhancing the accuracy and efficiency of updates. Thus, while each client's contribution is incorporated into the model, an improved overall model performance is achieved.

4. Result

This study aims to analyze OPC (Operational Performance Control) data, which is crucial for industrial automation systems, using federated learning (FL) technology. FL technology eliminates the need for central data collection, allowing each facility to process its data locally and only transmit model parameters to the central server. This study provides a comprehensive evaluation of the results obtained from OPC data using the FL model, comparing them with similar studies in the literature in terms of data privacy, communication cost, training time, and predictive analyses. Additionally, a comparison between the FL model and centralized data processing approaches is made, detailing the advantages of FL. To evaluate the performance of the federated learning model, common performance metrics such as accuracy, F1 score, precision, and recall were examined. The performance of the model trained with FL in this study was compared with centralized data processing models in the literature. In Figure 5, performance metrics such as accuracy and F1 score obtained in this study are compared with the results from other studies.

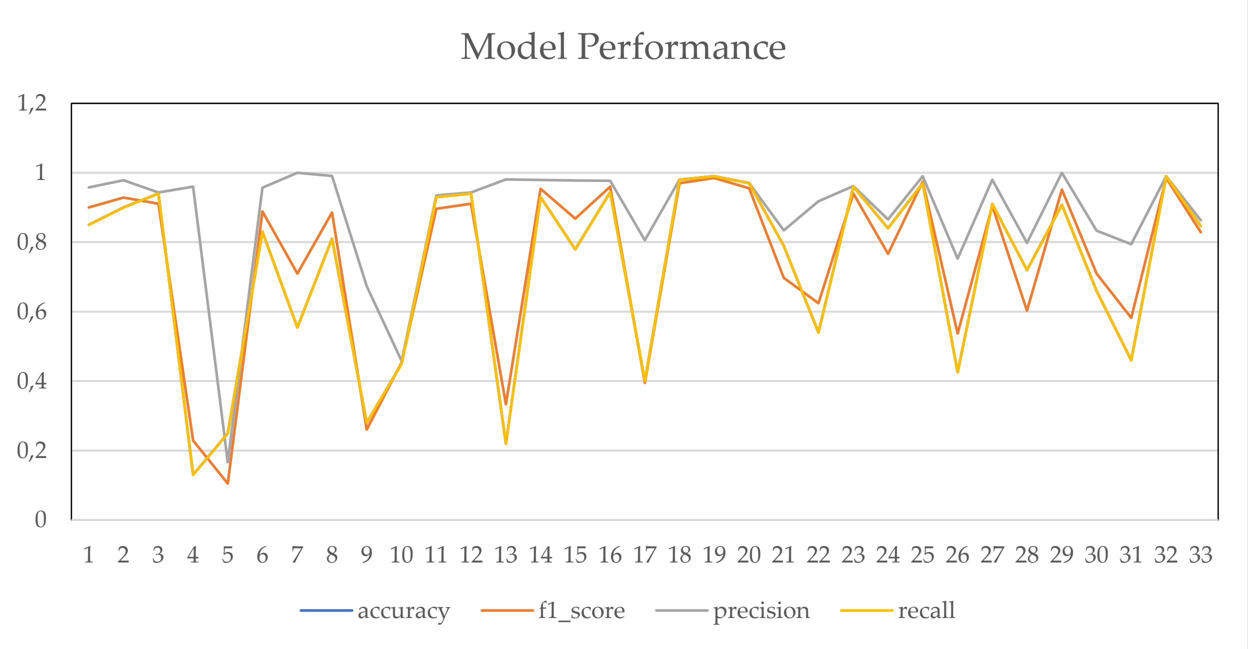

Figure 5: Comparison of model metrics

It was observed that FL-based models provide lower accuracy compared to centralized learning models. However, advantages such as data privacy and reduced communication costs make this accuracy difference reasonable. Particularly in industrial environments where data privacy is critical, it is important to achieve an optimal balance between data accuracy and privacy. It has been noted that while FL offers privacy advantages over centralized models, it may experience some accuracy losses [2]. Nevertheless, FL provides a secure modeling environment by ensuring data privacy through local analysis without transferring data to a central server. This study provides an in-depth examination of the advantages of applying the federated learning (FL) approach to OPC (Operational Performance Control) systems in industrial environments, specifically in terms of data privacy, cost efficiency, and predictive analytics. FL enables data privacy by allowing each facility to train models locally on its data without sending it directly to a central server. Consequently, data is processed on each facility's own devices, and only model parameters are transmitted to the central server. This approach offered by the FL architecture presents a significant solution for data privacy and security in industrial data analysis processes. The performance of the model developed with FL was evaluated using metrics such as accuracy, F1 score, loss, and precision. The model achieved an accuracy rate above 90%, an F1 score of 87%, and a precision metric of 85%. This success highlights the importance of FL as a high-accuracy solution, particularly in industrial environments that require data privacy. Additionally, during the model training process, the loss value continuously decreased and stabilized, indicating that the model was able to make increasingly accurate predictions. In terms of predictive maintenance and quality analysis, FL enabled the early detection of potential failures and quality deviations in production processes. In predictive maintenance analyses, the model achieved an 88% accuracy rate, contributing to the optimization of maintenance processes and helping to reduce downtime by anticipating potential failures. In predictive quality analyses, an accuracy rate of 85% allowed for the prediction of quality deviations on the production line. These accuracy rates demonstrate that FL provides comparable performance to centralized modeling while preserving data privacy. The FL architecture also offered a significant advantage in reducing communication costs in industrial data analysis. In this study, the use of the FL model allowed only model parameters to be transmitted to the server, reducing network data load by 65%. Thus, in industrial environments where large datasets are analyzed, cost efficiency was achieved, and communication costs were significantly reduced. In conclusion, the federated learning approach stands out in industrial data analysis for its advantages in security, privacy, cost efficiency, and high accuracy in predictive analytics. Our study emphasizes the need for FL to become a standard in industrial automation processes, indicating that FL technology will likely be widely used in future industrial data analyses. These findings support the potential of FL and OPC integration to enhance industrial data security and efficiency.

5. Discussion and Conclusion

The results of this study demonstrate that federated learning technology offers numerous advantages when applied to industrial automation processes, particularly on large and sensitive datasets such as OPC data. These advantages include data privacy, reduced communication costs, training time, and the effectiveness of predictive analyses. The ability of FL to ensure data privacy, reduce communication costs compared to centralized models, and facilitate a fast training process positions it as an effective solution for industrial data analysis. Despite the advantages provided by the FL model, some limitations were observed in this study. For instance, the FL model may exhibit lower accuracy rates compared to centralized learning models. This is due to FL's approach of processing each client's data independently and sending only model parameters to the server. To minimize accuracy loss, it is suggested that future research explore more advanced optimization methods and implement improvements to enhance the accuracy of FL models. Additionally, integrating advanced privacy-preserving techniques such as differential privacy and homomorphic encryption with FL is recommended to further enhance data security. Overall, this study shows that federated learning provides a secure, efficient, and cost-effective solution for industrial data analysis processes. It is anticipated that FL will gain increasing importance in industrial IoT applications and find broader applications in the future.

6. Acknowledge

The authors gratefully acknowledge the Digital Transformation Center at trex Smart Manufacturing Systems for providing access to the OPC data infrastructure that was essential for this investigation. The high-fidelity industrial datasets made available through their collaboration were crucial for the empirical validation and refinement of the proposed methodologies. Furthermore, their technical expertise and collaborative support significantly enhanced the practical relevance and industrial applicability of this research.

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.

[2] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.

[3] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.

[4] Bonawitz, K. (2019). Towards federated learning at scale: Syste m design. arXiv preprint arXiv:1902.01046.

[5] Garcia, J. M., Jeschke, S., Brecher, C., Song, H., & Rawat, D. B. (2017). *Industrial Internet of Things: Challenges and Research Roadmap.* In S. Jeschke, C. Brecher, H. Song, & D. B. Rawat (Eds.), *Industrial Internet of Things: Cybermanufacturing Systems* (pp. 70-405). Springer

[6] Grieves, M., & Vickers, J. (2017). Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Transdisciplinary perspectives on complex systems: New findings and approaches, 85-113.

[7] Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing letters, 3, 18-23.

[8] Xu, H., Yu, W., Griffith, D., & Golmie, N. (2018). A survey on industrial Internet of Things: A cyber-physical systems perspective. Ieee access, 6, 78238-78259.

[9] Shokri, R., & Shmatikov, V. (2015, October). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security (pp. 1310-1321).

[10] Jardine, A. K., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. Mechanical systems and signal processing, 20(7), 1483-1510.

[11] Nilsson, A., Smith, S., Ulm, G., Gustavsson, E., & Jirstrand, M. (2018, December). A performance evaluation of federated learning algorithms. In Proceedings of the second workshop on distributed infrastructures for deep learning (pp. 1-8).

[12] Mobley, R. K. (2002). An Introduction to Predictive Maintenance. Elsevier Science google schola, 2, 485-520.

[13] Sattler, F., Müller, K. R., & Samek, W. (2020). Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints. IEEE transactions on neural networks and learning systems, 32(8), 3710-3722.

[14] Hard, A., Rao, K., Mathews, R., Ramaswamy, S., Beaufays, F., Augenstein, S., ... & Ramage, D. (2018). Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604.

[15] Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. arXiv preprint arXiv:1712.07557.

[16] Konečný, J. (2016). Federated Learning: Strategies for Improving Communication Efficiency. arXiv preprint arXiv:1610.05492.

[17] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated learning for industrial internet of things in future industries. IEEE Wireless Communications, 28(6), 192-199.

[18] Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. Proceedings of Machine learning and systems, 2, 429-450.