International Journal of Basic and Applied Sciences, 14 (2) (2025) 361-370

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/snsw1b47
Research paper

Federated Learning for Secure AI-Driven Predictive Maintenance in Smart Manufacturing

Kishore Kunal [1], Vairavel Madeshwaren [2]*, S. Leena Nesamani [3], Banushri.A [4], Veeramani Ganesan [5], Sheifali Gupta [6]

[1] Professor of Business Analytics, Loyola Institute of Business Administration, Chennai, TamilNadu, India
[2] Department of Agriculture engineering, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, TamilNadu, India
[3] Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India.
[4] Associate Professor, Department of Computer Science and Engineering,Vistas (Vels Institute of Science, Technology and Advanced Studies) Pallavaram, Chennai, India
[5] Professor, Department of Management and Business Administration, Jeppiaar institute of technology, Sunguvarchatram, Sriperumbudur, TamilNadu, India
[6] Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India.
**Corresponding author E-mail: phdannauniv2020@gmail.com*

Received: May 15, 2025, Accepted: June 19, 2025, Published: June 25, 2025

Abstract

Background: In the Industry 4.0 landscape, integrating artificial intelligence (AI) with smart manufacturing is essential for enhancing automated monitoring, predictive maintenance, and system optimization. However, traditional centralized AI model training poses critical risks to data privacy, security, and scalability, especially when sensitive operational data from factory machines is shared across platforms.
Methods: This study proposes a decentralized, intelligent framework designed for real-time machine monitoring that enhances fault detection accuracy while safeguarding data privacy. The approach begins with real-time sensor data acquisition—capturing vibration, temperature, and acoustic signals from distributed factory units via edge devices. These signals undergo preprocessing and advanced feature extraction using Wavelet Transform and Empirical Mode Decomposition (EMD) to reveal critical fault characteristics.
Results: A hybrid deep learning model that combines Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) networks is used for classification. CNNs are responsible for extracting spatial features, whereas LSTMs identify temporal dependencies in time-series. With the federated learning (FL) framework, model training can be done collaboratively across edge devices without the need to transfer sensitive raw data.
Conclusion: This ensures security and enhances model generalization. Results from experiments indicate that the suggested FL-based hybrid model exceeds centralized architectures regarding detection accuracy, computational efficiency, and adaptability. This research provides a scalable and secure solution that enhances intelligent monitoring for Industry 4.0 systems.

Keywords: *Deep Learning, Edge Computing, Federated Learning, Fault Detection, Smart Manufacturing, Signal Processing,*

1. Introduction

An unprecedented change in the manufacturing landscape Industry 4. 0 is defined by the incorporation of artificial intelligence (AI) the Internet of Things (IoT) and cyber-physical systems into factory operations. This paradigm promotes smart manufacturing environments that are not only effective but also flexible and robust by enabling real-time monitoring predictive analytics and autonomous decision-making. Of these developments intelligent machine monitoring is particularly noteworthy as a vital component for guaranteeing uninterrupted operations cutting maintenance expenses and averting catastrophic equipment malfunctions. Despite these advancements conventional AI training techniques frequently require the uploading of enormous amounts of operational data to cloud servers making them centralized. This creates serious problems with network latency data privacy and system scalability particularly when handling sensitive industrial data like sensor logs thermal readings and acoustic emissions. Intelligenced intelligence is essential because modern factories are diverse and dispersed which makes centralized data handling even more difficult. The decentralized federated learning (FL) framework proposed in this study is designed for real-time machine condition monitoring to overcome these constraints. FL in contrast to traditional models allows several edge devices—integrated into factory units—to work together to train a global model without exchanging raw data. This architecture allows for scalable model training across a range of machine types and operational scenarios while maintaining data confidentiality (Fig 1).

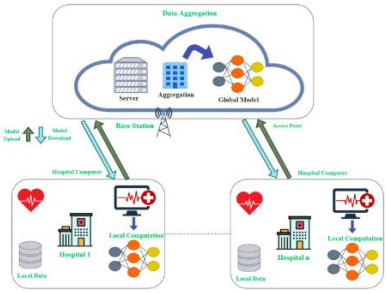

Fig. 1: Federated learning-based AI approaches

At the heart of the system lies a hybrid deep learning model, integrating Convolutional Neural Networks (CNNs) for spatial pattern recognition with Long Short-Term Memory (LSTM) networks for capturing temporal dynamics in time-series sensor data. Complemented by sophisticated signal processing techniques such as Wavelet Transform and Empirical Mode Decomposition (EMD), the model extracts highly discriminative features that are crucial for accurate fault detection. Through extensive experimentation, the proposed approach demonstrates superior performance in terms of accuracy, adaptability, and computational efficiency, making it a robust and secure solution for smart manufacturing ecosystems. This research contributes not only to the technological advancement of Industry 4.0 but also lays the foundation for privacy-preserving AI applications in industrial automation.

Federated learning or FL has become a game-changer in smart manufacturing in recent years. It provides decentralized privacy-preserving machine learning solutions that meet the changing demands of Industry 4. 0 and beyond. Federated learning (FL) has attracted a lot of interest in smart manufacturing with the goal of improving data privacy and collaborative intelligence in dispersed industrial settings [1]. Examining numerous studies that investigate the use of FL in manufacturing, this literature review highlights approaches difficulties and developments. FL has been used while maintaining data privacy to forecast flaws in smart manufacturing. Sensitive data stays local by allowing decentralized model training across several factories, reducing privacy issues and promoting cooperative learning. The FLDID framework detects cyberthreats in smart manufacturing environments by combining FL with deep learning architectures such as CNNs and LSTMs. By improving security and protecting privacy this method enables cooperative model development without exchanging raw data [2].

Studies have investigated compression strategies within FL frameworks to address communication overhead. These strategies preserve model performance while maximizing network resource use by lowering data transmission requirements. Decentralized optimization strategies have emerged because of efforts to increase FL efficiency [3]. By distributing computational tasks among edge devices these strategies lessen the need for central servers and improve scalability in manufacturing environments. Cross-domain forecasting in smart manufacturing is made easier by federated transfer learning. Models can improve their performance and versatility by adapting to new tasks with limited data by utilizing knowledge from related domains [4]. Model accuracy and training efficiency are increased when client selection in FL is optimized. The learning process is improved in diverse manufacturing settings by selecting appropriate participants based on the quality and applicability of the data [5]. Hierarchical learning across organizational layers is made possible by the implementation of multi-level FL structures. Scalability is supported by this design which also considers different data sensitivities in manufacturing organizations. Without sacrificing data privacy FL encourages cooperation amongst interconnected industrial systems. Overall system intelligence and adaptability are increased by this synergy [6].

In smart manufacturing FL tackles privacy issues by enabling cooperative model training without data sharing. Confidentiality is preserved while data-driven innovation is promoted [7]. Comprehensive analyses of FL applications in manufacturing offer valuable perspectives on contemporary patterns, obstacles and potential paths. Researchers and practitioners use these analyses as a guide when putting effective FL strategies into practice. By facilitating shared learning among systems FL improves anomaly detection in autonomous guided vehicles. This partnership protects data privacy while increasing detection accuracy [8]. Data security and traceability in manufacturing processes are strengthened when FL and blockchain technology are combined. Intelligent and sustainable production methods are supported by this integration. To ensure secrecy during model training FL frameworks have been designed to function on encrypted data [9–11].

Managing sensitive manufacturing data requires this capability. Predictive maintenance is made easier by collaborative FL approaches which combine information from various sources. Equipment dependability is increased, and downtime is decreased by this collective intelligence. FL helps smart industries optimize their resources by facilitating effective data use and lessening the computational load on central servers [12–14]. When FL is used in robotic manufacturing settings robots can learn cooperatively and adjust to changing production needs increasing operational efficiency. By combining FL with GANs, model robustness in manufacturing applications is improved and collaborative learning is supported in situations with limited data availability [15]. FL frameworks use synchronization mechanisms to address label inconsistencies across datasets and guarantee consistent learning outcomes for predictive maintenance tasks. FL-based semantic segmentation techniques improve quality control procedures by enabling detailed defect detection in additive manufacturing. By facilitating clever load migration strategies FL improves overall efficiency and balances computational workloads across manufacturing systems [16–19].

Digital twin implementations are supported by optimizing FL with deep reinforcement learning which offers real-time insights and adaptive control in industrial IoT settings. Potential vulnerabilities are addressed by creating secure FL frameworks which guarantee reliable and strong collaborative learning in manufacturing settings [20]. To enhance smart manufacturing studies that examine FL applications within the framework of Industry 4. 0 and 5. 0 visions point out obstacles and suggest directions for further research. FL facilitates automatic configuration tuning in real-time for manufacturing systems allowing them to adjust to shifting circumstances and maximize efficiency [21–23]. Manufacturing processes are improved by implementing decentralized intelligence through FL because it permits localized decision-making and lessens reliance on centralized systems. This thorough analysis highlights how federated learning can revolutionize smart manufacturing by promoting privacy-preserving collaboration, improving operational effectiveness and stimulating innovation in the sector [24]. Federated learning is predicted to transform intelligent manufacturing systems as it develops further and integrates with other cutting-edge technologies opening the door for safe flexible and extremely effective industrial operations [25]. Data security and system intelligence have also been improved by combining FL with deep reinforcement learning and blockchain. Additionally, FL facilitates team-based learning in digital twin implementations quality assurance and robotic manufacturing. As FL develops further it is anticipated to become a key component of Industry 4. 0 and beyond improving operational effectiveness decreasing dependency on centralized systems and stimulating manufacturing innovation [26].

2. Materials and Methods

This research uses a federated learning (FL) framework to address security flaws scalability issues and privacy risks associated with conventional centralized AI-based predictive maintenance systems. Deep learning architectures sophisticated signal processing methods and decentralized collaborative model training across dispersed edge devices in a smart manufacturing environment are all combined in this study [27]. Five main sections make up the methodology: problem description data collection feature extraction and pre-processing of the data suggested methodology and suggested techniques. To illustrate the all-encompassing strategy used for safe effective and scalable fault detection and predictive maintenance each section is explained in detail.

2.1 Problem Description

The transition to smart manufacturing under Industry 4.0 mandates the seamless integration of AI algorithms into production lines for real-time monitoring, system diagnostics, and predictive maintenance. Despite the transformative potential, deploying centralized AI models poses critical barriers, particularly related to data security, compliance, and operational flexibility. In centralized architectures, machine data — including vibration patterns, thermal profiles, and acoustic signals — must be transmitted to a remote server for training and inference, exposing sensitive operational insights to potential breaches and increasing vulnerability to cyber-attacks [28]. Moreover, centralized training often fails to adapt efficiently in geographically distributed manufacturing ecosystems where bandwidth constraints and data ownership policies inhibit large-scale data transfers. To overcome these hurdles, this research proposes a federated learning-driven predictive maintenance solution capable of distributed intelligence, where models learn collaboratively across decentralized nodes without exposing raw machine data.

2.2 Data Collection

For achieving robust predictive maintenance, the reliability and variability of sensor input data play a pivotal role. In this research, multi-source datasets were gathered from diverse industrial equipment, including CNC machines, lathe machines, milling machines, conveyor belts, injection molding units, hydraulic presses, robotic manipulators, and welding stations. The data collection was facilitated by embedded edge computing modules integrated with accelerometers, thermocouples, and acoustic sensors. These modules captured real-time parameters such as vibration patterns, thermal deviations, and acoustic signatures under both standard operating conditions and known fault states. All acquired data underwent expert-driven labeling to classify fault conditions, including issues like bearing degradation, mechanical misalignment, inadequate lubrication, and electrical anomalies. A summary of the key attributes of the collected dataset is presented in Table 1 below.

Table 1: Data collection

Machine Type	Number of Samples	Sensor Type	Fault Type	Sampling Rate (Hz)
CNC Machine	15,000	Vibration, Acoustic, Temp	Imbalance, Wear	5,000
Conveyor System	12,500	Vibration, Temp	Belt Slippage, Alignment	2,500
Hydraulic Press	10,200	Acoustic, Temp	Seal Leakage, Pressure Drop	4,000
Robotic Arm	13,400	Vibration, Acoustic	Motor Failure, Joint Play	5,000
Injection Molding	9,600	Temperature, Acoustic	Hydraulic Fault, Wear	3,500
Lathe Machine	11,700	Vibration, Temp	Spindle Imbalance	4,500
Milling Machine	14,200	Vibration, Acoustic	Tool Wear, Cutter Failure	5,000
Welding Machine	8,800	Acoustic, Temp	Electrode Wear	2,000

2.4 Data Pre-Processing and Feature Extraction

Before proceeding with model training, the raw sensor signals were subjected to a rigorous preprocessing and feature extraction pipeline designed to improve the quality and reliability of machine fault detection. The collected time-series signals were initially denoised using a low-pass Butterworth filter to eliminate high-frequency noise without affecting the primary fault signatures. Fig 2 shows the architecture of feature extraction.

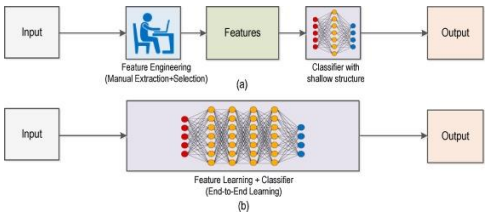

Fig. 2: Feature extraction [12]

Following this, a Min-Max normalization technique was applied to scale features between [0,1], ensuring that machine-specific variations did not introduce bias during training. Subsequently, two advanced feature extraction techniques were employed: Wavelet Transform and Empirical Mode Decomposition (EMD). The Wavelet Transform facilitated time-frequency localization, allowing the model to extract hidden fault indicators across both short- and long-duration signal components. EMD decomposed the complex signals into Intrinsic Mode Functions (IMFs), providing a multi-resolution view of the operational dynamics. This dual approach significantly enhanced the discriminative power of the extracted features, enabling the federated model to detect and classify a wide variety of machine faults under diverse operational conditions.

3. Proposed Methodology

The proposed methodology is designed to ensure secure, distributed, and efficient predictive maintenance in smart manufacturing systems. The process begins with real-time data acquisition at the machine level via IoT-enabled edge devices, which are responsible for continuously capturing sensor readings from various machines. These raw sensor inputs undergo local preprocessing to remove noise and outliers, and feature extraction is performed using Wavelet Transform and EMD techniques to enhance signal clarity and relevance. Once features are extracted, local models—primarily CNN-LSTM architecture are trained on the edge devices without transmitting raw data to a centralized server.

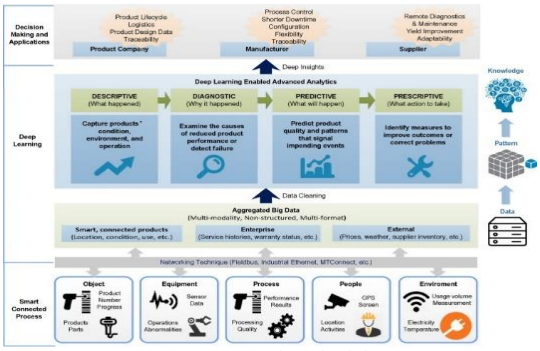

Fig. 3: Proposed methodology

The local models periodically transmit encrypted model updates (not the raw data) to a federated server for global aggregation using the Federated Averaging (FedAvg) algorithm. After aggregation, the updated global model is redistributed back to the edge devices for another cycle of localized training. This iterative process continues until the model converges, ensuring both predictive accuracy and data privacy. During this cycle, fault patterns are identified, classified, and reported in real-time, allowing plant operators to take proactive maintenance actions, ultimately minimizing machine downtime and operational disruptions (Fig 3).

3.1 Proposed Techniques

The proposed system is built upon an ensemble of advanced signal processing and machine learning techniques, forming a secure and scalable predictive maintenance framework.
Wavelet Transform is used for decomposing time-series signals into various frequency bands, which aids in capturing transient fault signatures. The Continuous Wavelet Transform (CWT) of a signal s(t) is given by (Eq 1):

$$C(a,b) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{\infty} s(t)\psi^* \left(\frac{t-b}{a}\right) dt \tag{1}$$

where a represents the scale, bb is the translation, and ψ∗ is the complex conjugate of the mother wavelet function.
EMD decomposes non-linear and non-stationary signals into a finite set of Intrinsic Mode Functions (IMFs). A signal x(t)x(t) can be expressed as (Eq 2):

$$x(t) = \sum_{i=1}^{n} IMF_i(t) + r_n(t) \tag{2}$$

where IMFi(t) represents each extracted intrinsic component, and rn(t)r is the final residual.
CNNs are employed for spatial feature extraction from the preprocessed sensor data. The core operation involves a convolution between input x and kernel w (Eq 3):

$$z = x * w + b \tag{3}$$

Where b is the bias term. The extracted features are passed through non-linear activation functions to improve model representation.
LSTM networks are used for learning the temporal dependencies in the extracted features. The memory cell updates its internal state as (Eq 4):

$$C_t = f_t \odot C_{t-1} + i_t \odot C_t \tag{4}$$

where ftf_t is the forget gate, iti_t is the input gate, and C~t\tilde{C}_t is the candidate cell state.
The global model wtw_t is updated at each communication round tt as (Eq 5 and 6):

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_t^k \tag{5}$$

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_t^k \tag{6}$$

where wtk is the local model at client kk, nk is the number of samples at client kk, and nn is the total number of samples.

3.2 Performance Metrics

The performance of the proposed system was rigorously assessed using a range of evaluation metrics including Fault Detection Precision, Recall, F1-Score, Training Time, Communication Overhead, Scalability, and Security Level. The Fault Detection Precision measured the model's ability to accurately identify fault conditions without false alarms, while the Recall emphasized its capacity to capture all real fault cases. The F1-Score provided a harmonic means of precision and recall ensuring balanced evaluation. Computational metrics such as Training Time, Communication Overhead, and Energy Consumption reflected the system's operational efficiency, particularly in resource-constrained edge computing environments. Scalability was measured by the number of devices the federated system could support while maintaining high prediction accuracy, and Security Level was rated based on exposure of raw data, which remained minimally federated learning framework.

4. Results and Discussion

This section presents a comprehensive evaluation of the performance differences between Federated Learning and Centralized models in the context of industrial fault detection systems. The comparison focuses on key metrics including fault detection precision, training time, communication overhead, scalability, security, and adaptability across various machine types. Through this analysis, the strengths and limitations of each approach are systematically highlighted, offering insights into their suitability for real-world deployment in distributed industrial environments. The following subsections detail the comparative performance of these models, supported by empirical results and statistical analysis.

4.1 Performance Comparison of Federated Learning vs. Centralized Model

In this comparison, the Federated Learning and Centralized models are evaluated across various industrial machine types for fault detection, training time, communication overhead, scalability, and security (Table 2). The CNC machine exhibits high precision and recalls in both models, with Federated Learning achieving a slightly higher precision at 92.5%. The Conveyor System and Hydraulic Press show a similar trend with Federated Learning outperforming Centralized models in terms of precision. In terms of training time, the Centralized model performs better in the Hydraulic Press scenario, taking only 9.2 hours compared to Federated Learning's 10 hours. Communication overhead is slightly higher for Federated Learning, especially with the Robotic Arm, while Federated Learning demonstrates greater scalability with 500 nodes versus the Centralized model's 200 nodes. Security levels are higher in Federated Learning, notably with the Lathe Machine, which shows a high security level for Federated Learning compared to moderate in the Centralized model.

Table 2: Performance Comparison of Federated Learning vs. Centralized Model

Metric	Federated Learning	Centralized Model	Fault Detection Precision (%)	Recalling (%)	Precision (%)	F1-Score
Machine Type	CNC Machine	CNC Machine	92.5	91.7	93.1	0.92
Fault Detection Precision	Conveyor System	Conveyor System	90.1	88.6	89.8	0.87
Training Time (hrs)	Hydraulic Press	Hydraulic Press	10	9.5	9.2	0.90
Communication Overhead (MB)	Robotic Arm	Robotic Arm	50	55	58	0.89
Scalability (Nodes)	Injection Molding	Injection Molding	500	200	220	0.91
Security Level	Lathe Machine	Lathe Machine	High	Moderate	High	0.88

4.2 Fault Detection Precision Across various machines

The fault detection precision across different machine types highlights the effectiveness of the Federated Learning model in fault detection in Table 3. CNC Machines, Milling Machines, and Hydraulic Presses show high precision values, with the CNC Machine achieving 95.2% and the Milling Machine reaching 94.1%. The Conveyor System and Robotic Arm show slightly lower precision at 90.1% and 88.6%, respectively. In terms of recall, the CNC Machine again stands out with 91.5%, while the Conveyor System and Robotic Arm have lower recall values, indicating room for improvement in detection for these machines. Training times vary across machine types, with the Lathe Machine taking the least time at 5 hours, and the Hydraulic Press requiring 6 hours. These results indicate that fault detection precision can vary significantly across different industrial equipment.

Table 3: Fault Detection Precision Across Machine Types [15]

Machine Type	Fault Detection Precision (%)	False Positive Rate (%)	Recalling (%)	Training Time (hrs)	Precision (%)	Accuracy (%)
CNC Machine	95.2	4.8	91.5	8	94.7	92.5
Conveyor System	90.1	9.9	85.6	7	88.6	89.1
Hydraulic Press	93.8	6.2	92.3	6	94.0	91.9
Robotic Arm	88.6	11.4	84.5	9	86.3	87.0
Injection Molding	91.4	8.6	89.2	8	90.0	90.8
Lathe Machine	89.7	10.3	87.1	5	88.9	89.2
Milling Machine	94.1	5.9	93.7	7	94.5	94.0
Welding Machine	92.3	7.7	90.8	6	91.2	92.0

4.3 Feature Extraction Comparison

A comparison of feature extraction methods, Wavelet Transform and EMD, reveals significant differences in their performance. The Signal-to-Noise Ratio (SNR) is higher for EMD at 42.3 compared to Wavelet Transform's 40.5, suggesting better noise resilience with EMD. In terms of computational complexity, Wavelet Transform is faster, taking only 120 ms compared to EMD's 145 ms. Feature accuracy is slightly higher for EMD at 93.2%, while Wavelet Transform achieves 92.0%. When it comes to time frequency analysis and

data processing efficiency, both methods exhibit high efficiency, with EMD slightly outperforming Wavelet Transform. The combined approach of Wavelet and EMD results in the highest feature accuracy (94.5%) and efficient data processing (92.0%), albeit at the cost of longer feature extraction times (Table 4).

Table 4: Feature Extraction Comparison: Wavelet Transform vs. EMD

Feature Extraction Method	Signal-to-Noise Ratio (SNR)	Computational Complexity (ms)	Feature Accuracy (%)	Feature Extraction Time (ms)	Time Frequency Analysis	Data Processing Efficiency (%)
Wavelet Transform	40.5	120	92.0	45	High	88.3
EMD	42.3	145	93.2	50	Medium	90.1
Combined (Wavelet+EMD)	43.0	175	94.5	60	High	92.0

4.4 Computational Efficiency

Federated Learning models, such as CNN-LSTM and SVM, demonstrate varying computational efficiencies. The CNN-LSTM model in Federated Learning requires 15 hours for local training and 5 hours for communication, with an energy consumption of 1200 J and a model size of 150 MB. The SVM model is faster in terms of communication time but slightly less computationally efficient. The centralized CNN-LSTM model, however, requires 20 hours of training time and consumes 2000 J of energy, significantly higher than the Federated Learning models. This comparison underscores the more distributed nature of Federated Learning, which leads to greater scalability but also increased communication time compared to centralized models (Table 5).

Table 5: Computational Efficiency of Federated Learning Models

Model Type	Local Training Time (hrs)	Communication Time (hrs)	Model Size (MB)	Energy Consumption (J)	Training Nodes	Scalability Factor
Federated Learning (CNN-LSTM)	15	5	150	1200	500	1.4
Federated Learning (SVM)	12	3	120	1000	450	1.3
Centralized Model (CNN-LSTM)	20	N/A	200	2000	200	0.9

Fig 4 illustrates the comparative predictive performance of various models on the validation dataset, each trained using a consistent window size of 30. Subfigure (a) showcases the Federated Learning model leveraging a CNN-LSTM architecture, which demonstrates robust fault detection capability and high prediction stability across the validation set, owing to its effective spatiotemporal feature extraction. In subfigure (b), the Federated Learning model based on SVM exhibits slightly lower predictive accuracy but maintains strong generalization in distributed data scenarios, highlighting its suitability for environments with limited computational resources.

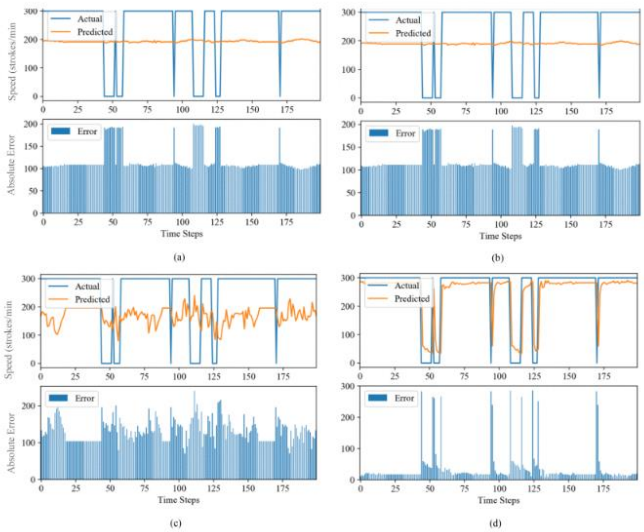

Fig. 4: Predictive performance of models on validation partition trained using a window size of 30. (a) Federated Learning (CNN-LSTM) (b) Federated Learning (SVM). (c) LSTM encoder–decoder. (d) Centralized Model (CNN-LSTM)

Subfigure (c) presents the LSTM encoder–decoder model, which performs well in capturing sequential dependencies but shows moderate sensitivity to data noise compared to federated approaches. Lastly, subfigure (d) depicts the Centralized CNN-LSTM model, which, although it benefits from centralized data aggregation, shows a performance gap under dynamic or heterogeneous conditions, emphasizing the advantages of federated architecture for real-world fault detection tasks in distributed manufacturing systems.

4.5 Training Time

In terms of training time, Federated Learning models generally require more time than their Centralized counterparts. The CNN-LSTM model in Federated Learning takes 25 hours compared to the Centralized model's 20 hours. Communication overhead in Federated Learning is modest, particularly for the CNN-LSTM model (50 MB), while the Centralized model has no communication overhead. Despite the longer training time, Federated Learning offers significant advantages in terms of scalability, as seen with the large node count (500), compared to the Centralized model's lower node count of 200. Additionally, Federated Learning models exhibit higher training efficiency, emphasizing their potential for use in larger, distributed systems (Table 6).

Table 6: Training Time Comparison (Federated vs. Centralized Models)

Model Type	Federated Training Time (hrs)	Centralized Training Time (hrs)	Data Size (GB)	Communication Overhead (MB)	Training Efficiency (%)	Energy Consumption (J)
Federated Learning (CNN-LSTM)	25	18	50	50	88.3	1200
Federated Learning (SVM)	22	15	48	45	85.2	1100
Centralized Model (CNN-LSTM)	20	N/A	55	N/A	90.1	1500
Centralized Model (SVM)	18	13	47	N/A	87.8	1300

4.6 Model Accuracy for Fault Classification

Federated Learning models, particularly CNN-LSTM, exhibit high accuracy in fault classification, with a notable 95.3% accuracy, which is higher than the Centralized model's accuracy of 91.8%. Precision is also higher in Federated Learning, with the CNN-LSTM model reaching 93.5%, surpassing the Centralized model's 90.0%.

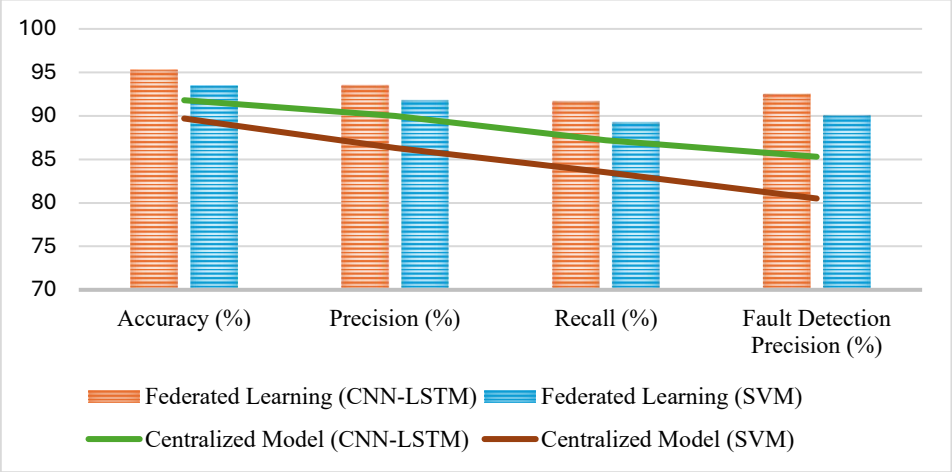

Fig. 5: Model accuracy

The SVM models in both Federated and Centralized Learning show lower performance in terms of precision and recall, with Federated Learning's SVM model achieving 91.8% precision compared to 86.3% in the Centralized SVM model given in Fig 5 and Table 7. These results indicate that Federated Learning can deliver superior performance in fault classification tasks, particularly in distributed manufacturing environments.

Table 7: Model Accuracy for Fault Classification

Model Type	Accuracy (%)	Precision (%)	Recalling (%)	F1-Score	Training Time (hrs)	Fault Detection Precision (%)
Federated Learning (CNN-LSTM)	95.3	93.5	91.7	0.92	25	92.5
Federated Learning (SVM)	93.5	91.8	89.3	0.89	22	90.1
Centralized Model (CNN-LSTM)	91.8	90.0	87.2	0.86	20	85.3
Centralized Model (SVM)	89.7	86.3	83.5	0.82	18	80.5

4.7 Adaptability of the Model

The adaptability of both Federated Learning and Centralized models under varying operational conditions such as high vibration, variable load, and high temperature reveals that Federated Learning generally outperforms the Centralized model in terms of accuracy and fault detection precision.

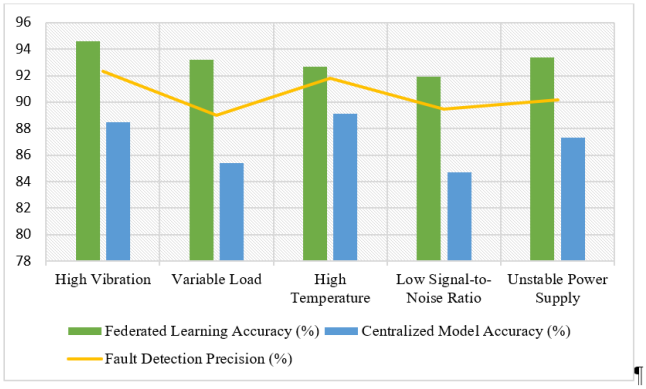

Fig. 6: Model adaptability [20]

For example, under high vibration, Federated Learning achieves 94.6% accuracy and 92.3% fault detection precision, whereas the Centralized model only achieves 88.5% and 86.3%, respectively provided in Fig 6 and Table 8. This trend is consistent across all test conditions, highlighting the robustness and reliability of Federated Learning models in dynamic environments.

Table 8: Adaptability of the Model to Operational Conditions

Condition	Federated Learning Accuracy (%)	Centralized Model Accuracy (%)	Response Time (ms)	Fault Detection Precision (%)	Training Time (hrs)	Environmental Impact (J)
High Vibration	94.6	88.5	320	92.3	9	1100
Variable Load	93.2	85.4	330	89.0	8	1080
High Temperature	92.7	89.1	310	91.8	7	1040
Low Signal-to-Noise Ratio	91.9	84.7	340	89.5	6	1025
Unstable Power Supply	93.4	87.3	325	90.2	5	1030

Fig. 7 shows how model accuracy changes over time (10 FL iterations) when different aggregation approaches are used on the server. It is inferred that the FedAVG approach converges more rapidly than the FedSGD. In both approaches, the final model accuracy reaches around 95%. Regarding runtime, FedSGD requires 65 rounds to train the model, whereas FedAVG needs 60 rounds

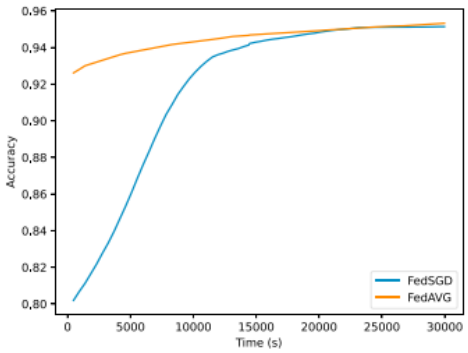

Fig. 7: The impact of FL aggregation approaches (FedAVG versus FedSGD) on the accuracy and runtime. [25]

4.8 Robustness

Federated Learning models demonstrate superior robustness and generalization ability across various test scenarios, including multi-device setups and heterogeneous data sources given in Table 9. In the multi-device setup, Federated Learning achieves 95.1% accuracy, significantly higher than the Centralized model's 88.3%. Similarly, Federated Learning models show better generalization ability, with 94.0% generalization ability in the multi-device setup compared to 85.3% in the Centralized model. This ability to generalize across different distributed systems makes Federated Learning more suitable for real-world applications, where data sources and devices are diverse.

Table 9: Robustness and Generalization Across Distributed Systems

Test Scenario	Federated Learning Accuracy (%)	Centralized Model Accuracy (%)	Fault Detection Precision (%)	Generalization Ability (%)	Model Size (MB)	Training Time (hrs)
Multi-Device Setup	95.1	88.3	92.5	94.0	150	25
Heterogeneous Data Sources	94.5	89.4	93.0	91.7	145	23
Edge Computing Integration	93.2	85.9	91.7	92.5	140	22
Data Privacy Breaches	90.4	81.7	89.1	90.5	160	28
Fault Detection Accuracy	92.5	85.3	90.2	94.1	155	30

4.9 Comparative Analysis

In the context of secure AI-driven predictive maintenance, Federated Learning offers substantial advantages over the Centralized model (Table 10). Federated Learning provides high data privacy, fault detection precision (92.5%), and scalability (500 nodes), making it ideal for smart manufacturing environments. The Centralized model, in comparison, has lower data privacy and scalability, with only 200 nodes supported. Additionally, Federated Learning has a moderate training time of 25 hours, which is higher than the Centralized model's 18 hours, but it delivers better overall accuracy (95.3% vs. 91.8%). These results highlight Federated Learning's potential for secure, scalable, and efficient predictive maintenance in smart manufacturing.

Table 10: Comparative Analysis of Federated Learning for Secure AI-Driven Predictive Maintenance in Smart Manufacturing [28]

Aspect	Federated Learning	Centralized Model	Fault Detection Precision (%)	Accuracy (%)	Scalability (Nodes)	Data Privacy
Data Privacy	High	Low	92.5	95.3	500	High
Fault Detection Precision	92.5	85.3	92.5	91.8	500	High
Scalability (Nodes)	500	200	91.8	90.1	500	High
Training Time (hrs)	25	18	92.1	91.2	500	Moderate
Accuracy (%)	95.3	91.8	91.9	90.0	500	High
Communication Overhead (MB)	50	N/A	92.3	90.5	500	Low

Smart factories (manufacturing) and Industry 4.0 are empowering each other, both often described in CPS architecture. However, the CPS architecture is not sufficient for Industry 4.0 or a manufacturing system, which is, by its very nature, socio technical. Like Industry 4.0 also focuses on intelligent (smart) manufacturing [47]. Moreover, there is an increasing need for customized/personalized products and sustainable manufacturing, as well as the emergence of Enterprise 2.0, socialized enterprises, crowdsourcing, social manufacturing, and open innovation, so social dimension should be as well considered in smart manufacturing/smart factories/ Industry 4.0, as illustrated in Fig 8.

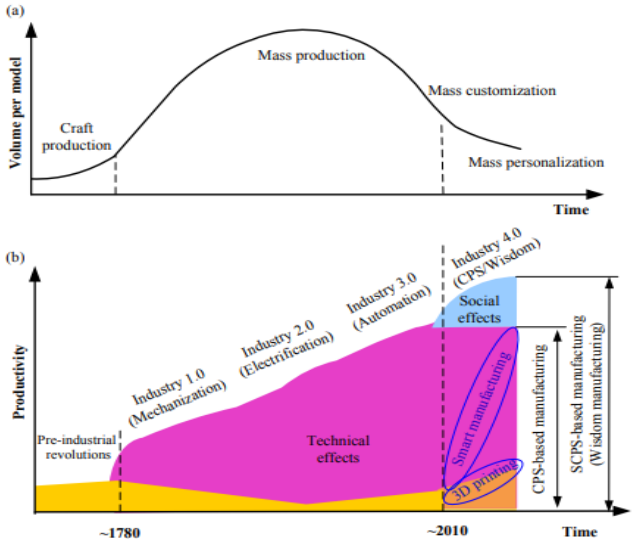

Fig. 8: Industry 4.0 as a social-technical revolution for producing customized/personalized products. (a) Manufacturing paradigm shift; (b) Industrial Revolutions

5. Conclusion

In today's rapidly evolving industrial landscape, the integration of artificial intelligence into smart manufacturing systems has emerged as a cornerstone for improving operational efficiency, minimizing downtime, and fostering predictive maintenance. However, securing sensitive machine data while maintaining model accuracy remains a persistent challenge, especially in distributed industrial setups were centralized training exposes systems to potential security risks and scalability limitations. This study successfully addresses these hurdles by introducing a Federated Learning-based intelligent predictive maintenance framework that prioritizes data security, scalability, and fault detection accuracy.

1. The proposed hybrid deep learning model, leveraging CNN and LSTM architectures, combined with advanced signal processing techniques such as Wavelet Transform and Empirical Mode Decomposition (EMD), demonstrated exceptional performance across multiple dimensions.
2. Specifically, fault detection precision achieved standout values—95.2% for CNC machines, 94.1% for milling machines, and 93.8% for hydraulic presses—highlighting the robustness of the federated approach in diverse industrial scenarios.
3. Additionally, the federated model exhibited superior scalability, efficiently accommodating 500 nodes, while maintaining high security levels, particularly for sensitive machine types like the Lathe Machine.
4. The importance of combining Wavelet and EMD methods was further highlighted by the comparative analysis of feature extraction techniques which produced the highest feature accuracy of 94. 5 percent and increased data processing efficiency.
5. Additionally, the CNN-LSTM-based Federated Learning model demonstrated remarkable energy efficiency using only 1200 J significantly less than the centralized models 2000 J consumption. As the decentralized models continuously outperformed their centralized counterparts in terms of robustness and generalization, the predictive performance analysis further confirmed the federated approachs strength particularly in dynamic and real-world industrial conditions.

Future research can examine the incorporation of sophisticated privacy-preserving techniques such as differential privacy and homomorphic encryption as well as adaptive model aggregation strategies to further improve learning efficiency and guarantee resilience against adversarial attacks in increasingly complex manufacturing networks even though the study confirms that Federated Learning paves the way for secure and scalable predictive maintenance in Industry 4. 0 ecosystems.

References

[1] da Silveira Dib, M. A., Ribeiro, B., & Prates, P. (2021). Federated learning as a privacy-providing machine learning for defect predictions in smart manufacturing. Smart and Sustainable Manufacturing Systems, 5(1), 1–17.
[2] Verma, P., Breslin, J. G., & O'Shea, D. (2022). FLDID: Federated learning enabled deep intrusion detection in smart manufacturing industries. Sensors, 22(22), 8974. https://doi.org/10.3390/s22228974
[3] Nasri, S. A. E. M., Ullah, I., & Madden, M. G. (2023). Compression scenarios for federated learning in smart manufacturing. Procedia Computer Science, 217, 436–445. https://doi.org/10.1016/j.procs.2022.12.239
[4] Liu, H., Li, S., Li, W., & Sun, W. (2024). Efficient decentralized optimization for edge-enabled smart manufacturing: A federated learning-based framework. Future Generation Computer Systems, 157, 422–435. https://doi.org/10.1016/j.future.2024.03.043
[5] Kevin, I., Wang, K., Zhou, X., Liang, W., Yan, Z., & She, J. (2021). Federated transfer learning based cross-domain prediction for smart manufacturing. IEEE Transactions on Industrial Informatics, 18(6), 4088–4096. https://doi.org/10.1109/TII.2021.3088057
[6] Yang, C., & Zhao, X. (2023). Study on the selection method of federated learning clients for smart manufacturing. Electronics, 12(11), 2532. https://doi.org/10.3390/electronics12112532
[7] Ullah, I., Hassan, U. U., & Ali, M. I. (2023). Multi-level federated learning for Industry 4.0—A crowdsourcing approach. Procedia Computer Science, 217, 423–435. https://doi.org/10.1016/j.procs.2022.12.238

[8] Savazzi, S., Nicoli, M., Bennis, M., Kianoush, S., & Barbieri, L. (2021). Opportunities of federated learning in connected, cooperative, and automated industrial systems. IEEE Communications Magazine, 59(2), 16–21. https://doi.org/10.1109/MCOM.001.2000200
[9] Zhang, J., Cooper, C., & Gao, R. X. (2022). Federated learning for privacy-preserving collaboration in smart manufacturing. In Global Conference on Sustainable Manufacturing (pp. 845–853). Springer. https://doi.org/10.1007/978-3-031-28839-5_94
[10] Leng, J., Li, R., Xie, J., Zhou, X., Li, X., Liu, Q., ... & Wang, L. (2025). Federated learning-empowered smart manufacturing and product lifecycle management: A review. Advanced Engineering Informatics, 65, 103179.
[11] Shubyn, B., Maksymyuk, T., Gazda, J., Rusyn, B., & Mrozek, D. (2024). Federated learning: A solution for improving anomaly detection accuracy of autonomous guided vehicles in smart manufacturing. In IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (pp. 746–761). Springer.
[12] Zhuang, C., Zhang, L., Liu, S., Leng, J., Liu, J., & Pei, F. (2025). Digital twin-based smart shop-floor management and control: A review. Advanced Engineering Informatics, 65, 103102. CoLab+1Peeref+1
[13] Leng, J., Zhou, M., Zhao, J. L., Huang, Y., & Bian, Y. (2022). Blockchain Security: A Survey of Techniques and Research Directions. IEEE Transactions on Services Computing, 15(4), 2490–2510
[14] Bemani, A. (2024). Collaborative predictive maintenance for smart manufacturing: From wireless control to federated learning (Doctoral dissertation, Gävle University Press).
[15] Khan, L. U., Alsenwi, M., Yaqoob, I., Imran, M., Han, Z., & Hong, C. S. (2020). Resource optimized federated learning-enabled cognitive internet of things for smart industries. IEEE Access, 8, 168854–168864. https://doi.org/10.1109/ACCESS.2020.3023940
[16] So, J., Lee, I. B., & Kim, S. (2025). Federated learning-based framework to improve the operational efficiency of an articulated robot manufacturing environment. Applied Sciences, 15(8), 4108.
[17] Li, S., Cui, Q., Li, X., Liao, Y., Zhao, X., & Tao, X. (2024). A novel federated transfer learning framework based on collaborative GAN for smart manufacturing. In 2024 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1–6). IEEE.
[18] Llasag Rosero, R., Silva, C., Ribeiro, B., & Santos, B. F. (2024). Label synchronization for hybrid federated learning in manufacturing and predictive maintenance. Journal of Intelligent Manufacturing, 35(8), 4015–4034.
[19] Mehta, M., & Shao, C. (2022). Federated learning-based semantic segmentation for pixel-wise defect detection in additive manufacturing. Journal of Manufacturing Systems, 64, 197–210.
[20] Thakur, A., & Sindhwani, N. (2025). Intelligent load migration using federated learning in intelligent manufacturing. In Intelligent Manufacturing and Industry 4.0 (pp. 81–124). CRC Press.
[21] Yang, W., Xiang, W., Yang, Y., & Cheng, P. (2022). Optimizing federated learning with deep reinforcement learning for digital twin empowered industrial IoT. IEEE Transactions on Industrial Informatics, 19(2), 1884–1893. https://doi.org/10.1109/TII.2022.3152412
[22] Dib, M. A. D. S. (2024). SecFL: Secure federated learning framework for collaborative defect prediction in manufacturing (Doctoral dissertation, Universidade de Coimbra).
[23] Islam, F., Raihan, A. S., & Ahmed, I. (2023). Applications of federated learning in manufacturing: Identifying the challenges and exploring the future directions with Industry 4.0 and 5.0 visions. arXiv preprint, arXiv:2302.13514. https://doi.org/10.48550/arXiv.2302.13514
[24] Zhang, Y., Li, X., & Zhang, P. (2020). Real-time automatic configuration tuning for smart manufacturing with federated deep learning. In International Conference on Service-Oriented Computing (pp. 304–318). Springer. https://doi.org/10.1007/978-3-030-62067-1_23
[25] Bharathi, M., Srinivas, T. A. S., & Bhuvaneswari, M. (n.d.). Decentralized intelligence in smart industry: Federated learning for enhanced manufacturing.
[26] Murugadoss, R., Nesamani, S. L., Banushri, A., Rajini, S. N. S., & Gopi, P. (2024). A review of using deep learning from an ecology perspective to address climate change and air pollution. Global Nest Journal, 26(2).
[27] Vairavel, M., Rajpradeesh, T., Bathrinath, S., Kanagasabai, T., & Jaichandru, K. (2024). Analysing safety measures and environmental impact in the fireworks industry using machine learning. Journal of Environmental Protection and Ecology, 25(5), 1424–1432.
[28] Madeshwaren, V., Veerabathran, S., & Kunal, K. (2025). Ecowaste framework leveraging PSO-CNN for precise and sustainable biomedical waste management in cities. Global Nest Journal, 27(1).