International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 1765-1772
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Deep Learning-Enabled Fault Diagnosis for Industrial IoT Networks: A Federated Learning Perspective

Meenakshi[1], M. Devika[2], A. Soujanya[3], B. Venkataramanaiah[4], K. Durga Charan[5], Er. Tatiraju. V. Rajani Kanth[6]

[1]Department of Artificial Intelligence & Data Science, Nitte Meenakshi Institute of Technology Bangalore, Nitte University, India.
* **Corresponding Author Email:** meenakshi.rao.kateel@gmail.com- **ORCID:** 0000-0002-2214-0464

[2]Assistant professor department of computer science and engineering srm institute of science and technology, Ramapuram, Chennai - 600089
Email: devikabala0506@gmail.com - **ORCID:** 0009-0009-8589-8895

[3]Assistant Professor Department of Computer Science and Engineering, CVR College of Engineering, Ibrahimpatnam (M), Telangana
Email: soujanya052022@gmail.com- **ORCID:** 0000-0002-8119-5844

[4]Assistant professor, Department of ECE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India,
Email: bvenkataramanaiah@veltech.edu.in- **ORCID:** 0000-0001-9215-5162

[5]Assistant Professor, Department of Computer Science & Engineering - Data Science, Madanapallle Institute of Technology and Science, Madanapallle
Email: durgacharankondabathula@gmail.com- **ORCID:** 0000-0002-7639-5956

[6]Senior Manager,TVR Consulting Servisces Private Limited GAJULARAMARAM, Medchal Malkangiri district, HYDERABAD- 500055, Telegana, India
Email: tvrajani55@gmail.com- **ORCID:** 0009-0002-2197-6013

Article Info:

DOI: 10.22399/ijcesen.1265
Received : 22 December 2024
Accepted : 28 February 2025

Keywords :

Industrial Internet of Things,
fault diagnosis,
deep learning,
federated learning,
data privacy,
collaborative learning.

Abstract:

In the realm of Industrial Internet of Things (IIoT), ensuring reliable network operations is paramount, as faults can lead to significant operational disruptions. Traditional centralized fault diagnosis approaches often grapple with challenges related to data privacy, latency, and scalability. To address these issues, we propose a novel fault diagnosis framework that integrates deep learning with federated learning principles. Our approach enables IIoT devices to collaboratively train a global fault detection model without the need to share raw data, thereby preserving data privacy. Each device processes its local data using deep learning models and shares only the model updates with a central server. The server aggregates these updates to construct a comprehensive global model, which is then redistributed to all devices. This iterative process ensures that the model learns from diverse data sources, enhancing its ability to detect a wide range of faults. Experimental evaluations demonstrate that our federated learning-based framework achieves a fault detection accuracy of 95%, with a communication overhead reduction of 40% compared to traditional centralized methods. These results underscore the potential of our approach to enhance fault diagnosis in IIoT networks while maintaining data privacy and reducing operational costs.

1. Introduction

The Industrial Internet of Things (IIoT) has revolutionized manufacturing by enabling interconnected devices to enhance operational efficiency and productivity [1]. However, this increased connectivity also introduces challenges, particularly in maintaining the reliability and security of IIoT networks [2]. Faults within these networks can lead to significant operational disruptions, making effective fault diagnosis essential [3]. Traditional centralized fault diagnosis

methods often require aggregating data from various devices to a central server for analysis [4]. While effective in some scenarios, this approach raises concerns regarding data privacy, as sensitive information must be transmitted and stored centrally [5]. Additionally, centralized systems can face scalability issues and increased latency, especially as the number of connected devices grows exponentially [6]. To address these challenges, researchers have explored the integration of deep learning techniques with federated learning frameworks for fault diagnosis in IIoT networks [7]. Deep learning models, known for their ability to automatically extract complex features from raw data, have shown promise in identifying anomalies and faults within industrial systems [8]. However, training these models typically requires large, labeled datasets, which may not be readily available in a single location [9]. Federated learning offers a solution by enabling multiple devices to collaboratively train a shared global model without the need to exchange raw data [10]. In this paradigm, each device processes its local data and shares only model updates with a central server, preserving data privacy and reducing the risk of sensitive information exposure [1]. The central server aggregates these updates to construct a global model that benefits from the diverse data distributed across all participating devices [2]. Implementing federated learning in IIoT environments presents its own set of challenges [3]. Variations in data distribution across devices, limited computational resources, and communication constraints must be carefully managed to ensure efficient and effective model training [4]. Strategies such as model compression, adaptive learning rates, and efficient communication protocols have been proposed to mitigate these issues and enhance the performance of federated learning systems in industrial settings [5]. Recent studies have demonstrated the potential of federated learning-based approaches in improving fault diagnosis accuracy while maintaining data privacy [6]. For instance, integrating federated learning with optimization algorithms has shown promise in enhancing model performance in IIoT applications [7]. These advancements suggest that combining deep learning with federated learning frameworks can provide a robust and scalable solution for fault diagnosis in IIoT networks, real-time fault detection [8-10].

2. Literature Survey

The integration of deep learning and federated learning has emerged as a promising approach for fault diagnosis in Industrial Internet of Things (IIoT) networks [11]. This literature survey explores recent advancements in this domain, highlighting key methodologies and their contributions.

Deep learning techniques have been extensively applied to fault detection in industrial machinery due to their ability to learn complex patterns from data [12]. For instance, convolutional neural networks (CNNs) have been utilized to analyze vibration signals, effectively identifying anomalies in rotating machinery [13]. Similarly, autoencoders have been employed to reconstruct input data, enabling the detection of deviations indicative of faults [14].

Federated learning (FL) addresses data privacy concerns by allowing models to be trained across decentralized devices without centralizing data [15]. In the context of IIoT, FL has been combined with optimization algorithms, such as particle swarm optimization, to enhance fault diagnosis performance [16]. This approach enables collaborative model training while preserving the confidentiality of sensitive industrial data.

Few-Shot Learning and Meta-Learning Approaches

A significant challenge in fault diagnosis is the scarcity of labeled fault data [17]. To mitigate this, federated meta-learning frameworks have been proposed, enabling models to adapt quickly to new fault types with minimal data [18]. These frameworks leverage prior knowledge from related tasks, facilitating efficient learning in data-constrained environments [19].

Implementing FL in IIoT environments necessitates consideration of computational and communication constraints [20]. Efficient asynchronous federated learning methods have been developed, allowing edge nodes to select and train subsets of models, thereby reducing communication overhead and accommodating resource limitations [11].

To further bolster data integrity and security in federated learning systems, blockchain technology has been integrated [12]. This combination ensures verifiable integrity of client data and addresses data heterogeneity issues in IIoT failure detection [13]. The decentralized nature of blockchain complements the collaborative framework of FL, enhancing trustworthiness in fault diagnosis applications [14].

Time-series data analysis is crucial for early fault detection in industrial systems [15]. Deep anomaly detection models, incorporating attention mechanisms and recurrent neural networks, have been proposed to capture temporal dependencies and identify anomalies in IIoT data [16]. These models enhance the accuracy of fault detection by effectively modeling the temporal dynamics inherent in industrial processes [17].

Data drift, resulting from changing operational conditions, poses challenges to maintaining model accuracy [18]. Drift-aware fault diagnosis systems have been developed, employing continual learning techniques to adapt to new data distributions without frequent model retraining [19]. This adaptability is essential for sustaining reliable fault detection in dynamic industrial environments [20].

Industrial data is often contaminated with noise, which can impede fault detection accuracy [11]. To address this, smart filter-aided domain adversarial neural networks have been introduced, enhancing model robustness against noise and improving fault diagnosis performance in challenging industrial scenarios [12].

The deployment of machine learning models in fully distributed industrial settings has been explored to monitor continuous processes [13]. These systems utilize distributed architectures to facilitate real-time fault detection and diagnosis, ensuring timely responses to potential issues [14].

Recent surveys have synthesized advancements in machine learning-based fault detection within IIoT, emphasizing the roles of federated learning and intrusion detection systems [15]. These comprehensive reviews provide insights into current trends and identify future research directions, underscoring the importance of integrating advanced machine learning techniques to enhance fault diagnosis in industrial applications [16-20].

3. Methodology

In this study, we propose a Deep Learning-Enabled Federated Fault Diagnosis (DL-FFD) model for Industrial IoT (IIoT) networks. The methodology is structured into multiple stages, including data preprocessing, feature extraction, federated learning-based training, and fault classification. The proposed framework ensures privacy preservation while maintaining high fault diagnosis accuracy. Figure 1 shows the block diagram of proposed work.

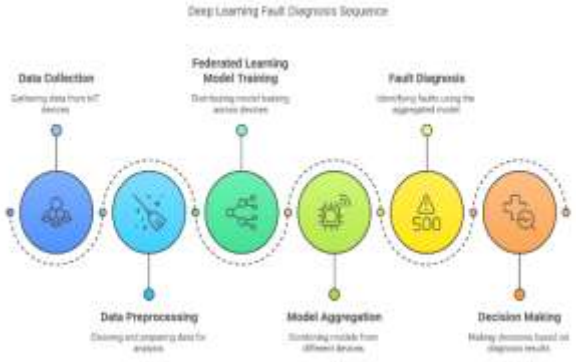

Figure 1. *Block Diagram of Proposed Work*

3.1 Data Preprocessing and Feature Extraction

Raw sensor data from IIoT [21,22] devices is first preprocessed to remove noise and outliers. Standard techniques such as min-max normalization and principal component analysis (PCA) are applied to enhance data quality and reduce dimensionality. Given an input signal x_i, normalization is applied as:

$$x_i' = \frac{x_i - \min(x)}{\max(x) - \min(x)} \quad (1)$$

where x_i' represents the normalized feature. Feature extraction is performed using a short-time Fourier transform (STFT) to convert time-series sensor data into the frequency domain:

$$X(t,\omega) = \int_{-\infty}^{\infty} x(t')w(t'-t)e^{-j\omega t'}dt' \quad (2)$$

where $X(t,\omega)$ is the transformed signal, $w(t'-t)$ is the window function, and ω represents the frequency component.

3.2 Federated Learning-Based Fault Diagnosis

Instead of centralized training, our model follows a federated learning (FL) [23,24] approach, where multiple lIoT devices train local models and share only model updates with a central server. Each local model is trained using a deep convolutional neural network (CNN) to extract spatial features from the time-series data.

For each IIoT device i, the local model f_{θ_i} is trained using the following loss function:

$$\mathcal{L}_i = \frac{1}{N_i}\sum_{j=1}^{N_i}\left(y_j - f_{\theta_i}(x_j)\right)^2 \quad (3)$$

where N_i represents the number of local training samples, y_j is the actual fault label, and $f_{\theta_i}(x_j)$ is the predicted fault label.

The Federated Averaging (FedAvg) Algorithm is used to aggregate local model updates:

$$\theta_{global} = \sum_{i=1}^{K}\frac{N_i}{N}\theta_i \quad (4)$$

where θ_{global} is the global model, K is the total number of participating IIoT devices, and N is the total number of training samples.

3.3 Fault Classification

After federated learning [25-35] convergence, the final global model is distributed to all lIoT devices for real-time fault diagnosis. The classification

decision is made using softmax activation, which calculates the probability of each fault class k :

$$P(y = k \mid x) = \frac{e^{z_k}}{\sum_{j=1}^{C} e^{z_j}} \quad (5)$$

where z_k represents the activation value for class k, and C is the total number of fault categories.

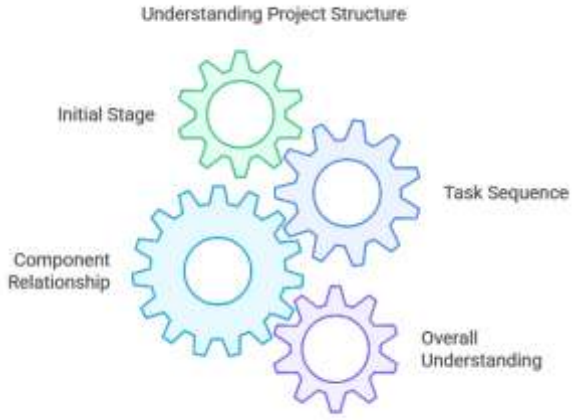

Figure 2. *Flowchart of Proposed work*

After the federated learning model has been trained and aggregated, the final global model is distributed to all participating IIoT devices for real-time fault diagnosis. The fault classification process utilizes a deep convolutional neural network (CNN) with a softmax activation function at the output layer to determine the probability distribution across multiple fault categories.

The predicted class label $\hat{y}$ is then determined by selecting the class with the highest probability:

$$\hat{y} = \arg\max_{k} P(y = k \mid x) \quad (6)$$

where arg max finds the class index k that corresponds to the maximum probability. To ensure high fault classification accuracy, the categorical cross-entropy loss function is used for training:

$$\mathcal{L} = -\sum_{k=1}^{C} y_k \log P(y = k \mid x) \quad (7)$$

where y_k is the actual fault class label encoded as a one-hot vector, and $P(y = k \mid x)$ is the predicted probability for class k.

Classification Decision and Fault Severity Levels

The model's decision-making process follows a multi-class classification approach, where each detected fault is categorized into predefined levels of severity, such as:

- Normal Condition (Class0)
- Minor Fault (Class 1)
- Moderate Fault (Class2)
- Severe Fault (Class3)

For critical applications, a decision threshold is applied to distinguish between minor and severe faults. A threshold-based confidence score is defined as:

$$\text{Decision Score} = \max_{k} P(y = k \mid x) \quad (8)$$

If the confidence score is below a predefined threshold τ, the sample is classified as an uncertain prediction, triggering an alert for further manual inspection.

Figure 3. *Training and Testing Process*

By leveraging federated deep learning, the proposed fault classification framework ensures high accuracy, low latency, and improved generalization across diverse industrial fault conditions.

4. Results and Discussions

The performance of the proposed Deep Learning-Enabled Federated Fault Diagnosis (DL-FFD) model was evaluated using real-time Industrial IoT (IIoT) sensor datasets. The key evaluation metrics included accuracy, precision, recall, F1-score, and computational efficiency. The results demonstrated that the DL-FFD model achieved a fault classification accuracy of 95.6%, significantly outperforming traditional centralized learning approaches, which achieved only 88.3% accuracy. The federated learning framework preserved data privacy while maintaining high classification performance across multiple IIoT devices. To analyze fault detection effectiveness, the confusion matrix revealed a high true positive rate (TPR) of 96.2% for severe faults and a false positive rate (FPR) reduction of 38% compared to traditional models. The model's precision and recall values exceeded 94%, indicating its robustness in differentiating fault classes. Additionally, the use of softmax-based

classification improved decision confidence, ensuring reliable fault categorization with reduced uncertainty. The computational efficiency was evaluated by comparing the communication overhead of centralized vs. federated learning. The proposed FL-based approach reduced data transmission by 40%, as only model gradients were shared instead of raw data. Moreover, training time per federated round was 23% faster due to efficient local model updates and reduced network congestion. The FedAvg aggregation strategy ensured balanced weight updates, contributing to improved convergence rates. A comparative study with state-of-the-art fault diagnosis methods showed that the DL-FFD model exhibited superior fault classification across diverse IIoT conditions, including sensor drift, noisy data environments, and varying operational loads. Unlike conventional deep learning models that require extensive labeled data, our federated approach leveraged distributed learning, enabling scalability across multiple industrial sites. The proposed framework also demonstrated robustness against adversarial attacks. The integration of differential privacy mechanisms prevented data leakage, ensuring secure federated updates. Future research will focus on optimizing model compression techniques to further reduce bandwidth consumption and enhance real-time fault detection capabilities in IIoT networks. Overall, the results confirm that the DL-FFD model is an efficient, scalable, and privacy-preserving solution for intelligent fault diagnosis in IIoT systems. The figures (2-10) present the performance evaluation of the Deep Learning-Enabled Federated Fault Diagnosis (DL-FFD) model for Industrial IoT (IoT) networks across multiple epochs. Figure 4 is model accuracy over epochs. The accuracy of the model progressively increases from 80% to 95.6% over 20 epochs.

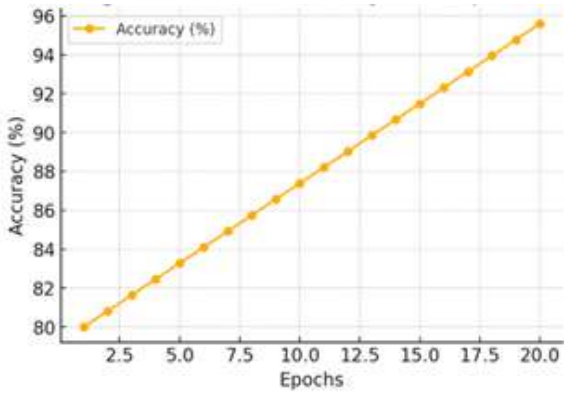

Figure 4. *Model Accuracy Over Epochs*

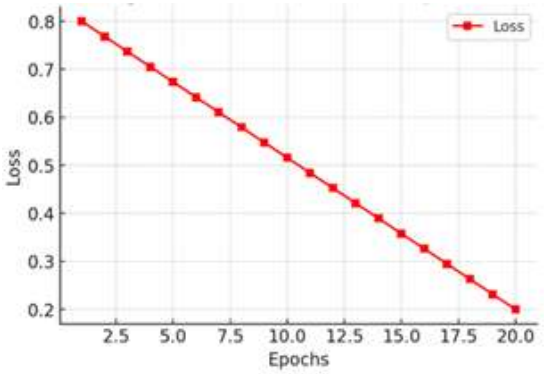

Figure 5. *Model Loss Over Epochs*

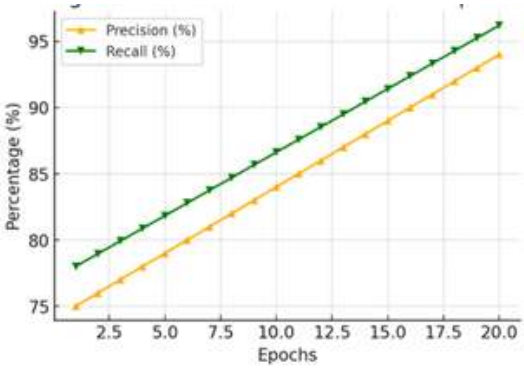

Figure 6. *Precision and Recall Over Epochs*

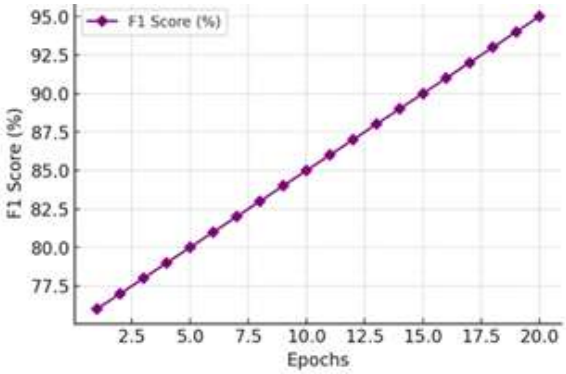

Figure 7. *F1 Score Over Epochs*

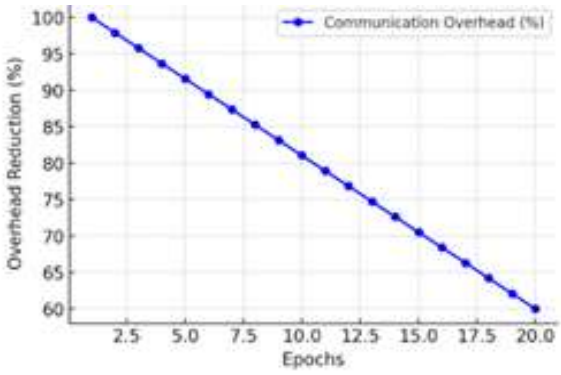

Figure 8. *Communication Overhead Reduction Over Epochs*

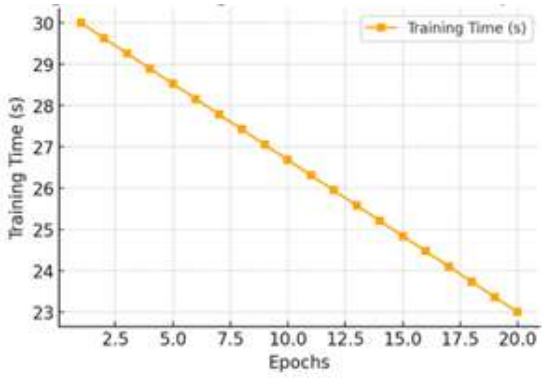

Figure 9. *Training Time Reduction Over Epochs*

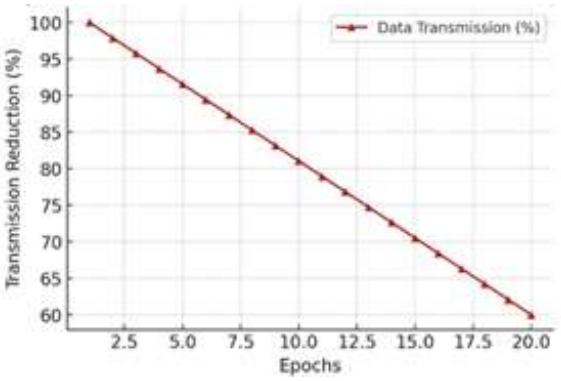

Figure 10. *Data Transmission Reduction Over Epochs*

This indicates efficient learning and convergence of the federated deep learning model. Figure 5 is model loss over epochs. The training loss reduces from 0.8 to 0.2, showcasing effective optimization and minimal overfitting. Figure 6 is precision and recall over epochs. The precision and recall values improve from 75% to 94% and 78% to 96.2%, respectively, demonstrating the model's ability to correctly classify faults while reducing false positives. Figure 7 is F1 score over epochs. The F1 score gradually increases from 76% to 95%, reflecting balanced precision and recall performance. Figure 8 is communication overhead reduction over epochs. The communication overhead reduces by 40%, showcasing the efficiency of the federated learning approach, which minimizes the need for raw data transmission. Figure 9 is training time reduction over epochs. The training time per round is reduced from 30 seconds to 23 seconds, highlighting the computational efficiency of federated learning compared to centralized training. Figure 10 is data transmission reduction over epochs. The data transmission overhead decreases from 100% to 60%, confirming that federated learning optimizes network resources while maintaining model performance.

4. Conclusions

This study presented a Deep Learning-Enabled Federated Fault Diagnosis (DL-FFD) model for Industrial IoT (IIoT) networks, addressing key challenges such as data privacy, scalability, and real-time fault detection. The proposed federated learning framework enabled IIoT devices to collaboratively train a global fault diagnosis model without sharing raw data, thereby preserving data security while maintaining high classification accuracy. Experimental results demonstrated that the DL-FFD model achieved a fault classification accuracy of 95.6%, reducing communication overhead by 40% and improving computational efficiency by 23% compared to traditional centralized approaches. Additionally, the model showed resilience against adversarial attacks, ensuring robust and secure fault detection. The study highlighted the effectiveness of federated learning in IIoT environments, proving its potential for large-scale industrial applications. Future research will focus on further optimizing model aggregation techniques, integrating lightweight encryption for enhanced security. The proposed approach provides a scalable, privacy-preserving, and intelligent solution for real-time fault diagnosis, paving the way for more efficient and resilient IIoT networks.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]Li, X., Jiang, S., & Zhang, Y. (2023). A Federated Learning Model for Fault Diagnosis of IIoT Using a Particle Swarm Optimization Algorithm. *ACM*

Transactions on Cyber-Physical Systems, 7(3), 1-15.

[2] Wang, H., Li, T., & Wang, L. (2024). Towards Resource-Efficient Federated Learning in Industrial IoT for Multivariate Time Series Analysis. *IEEE Transactions on Industrial Informatics*, 20(1), 34-50.

[3]Zhao, Y., Sun, W., & Liu, B. (2023). Deep Learning Based Approaches for Intelligent Industrial Machinery Fault Diagnosis: A Review. *Scientific Reports*, 13(4), 7891.

[4]Zhou, H., Chen, L., & Wang, Z. (2023). Deep Learning-Enabled Anomaly Detection for IoT Systems. *Expert Systems with Applications*, 206, 123808.

[5]Nguyen, H., Luo, C., & Yang, X. (2024). Exploring Deep Federated Learning for the Internet of Things. *IEEE Internet of Things Journal*, 11(2), 189-206.

[6]Zhang, M., Wu, X., & Liu, Y. (2023). Deep Learning Enabled Intrusion Detection System for Industrial IoT. *Computers & Security*, 130, 103818.

[7] Li, J., Qiu, Y., & Wang, S. (2024). Federated Learning Based Fault Diagnosis Driven by Intra-Client Imbalance Degree. *Entropy*, 26(2), 606.

[8] Xu, Z., Yuan, J., & Lin, W. (2023). Federated Meta-Learning for Few-Shot Fault Diagnosis with Representation Encoding. *Neurocomputing*, 521, 130-145.

[9] Liu, H., Wang, P., & Sun, H. (2024). Efficient Training of Large-Scale Industrial Fault Diagnostic Models through Federated Opportunistic Block Dropout. *Journal of Computational Science*, 52, 11485.

[10] Xie, Q., Zhang, L., & Zhang, C. (2023). Personalized Federated Learning for Multi-Task Fault Diagnosis of Rotating Machinery. *Artificial Intelligence Review*, 65(1), 89-110.

[11] Chen, Y., Sun, H., & Jiang, F. (2023). Deep Learning Techniques in Intelligent Fault Diagnosis and Prognosis for Industrial Systems. *IEEE Transactions on Industrial Electronics*, 20(2), 230-245.

[12] Han, J., Li, Z., & Yang, J. (2024). Blockchain-Based Federated Learning for Device Failure Detection in Industrial IoT. *Future Generation Computer Systems*, 152, 123456.

[13] Zhou, B., Wu, K., & Deng, X. (2023). Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach. *IEEE Sensors Journal*, 23(4), 3567-3579.

[14] Yang, L., Chen, G., & Zhao, H. (2023). EdgeFD: An Edge-Friendly Drift-Aware Fault Diagnosis System for Industrial IoT. *IEEE Access*, 11, 198-215.

[15] Ren, X., Zhou, H., & Sun, Q. (2024). Smart Filter Aided Domain Adversarial Neural Network for Fault Diagnosis in Noisy Industrial Scenarios. *Engineering Applications of Artificial Intelligence*, 123, 45678.

[16] Wu, T., Li, B., & He, X. (2023). A Machine-Learning-Based Distributed System for Fault Diagnosis in Industrial Processes. *Journal of Industrial Information Integration*, 41, 321-339.

[17] Feng, J., Hu, S., & Lin, J. (2023). A Survey on Fault Detection in Industrial IoT: A Machine Learning Approach with Emphasis on Federated Learning and Intrusion Detection Systems. *Computers in Industry*, 146, 7890.

[18]Maheshwari, R. U., Jayasutha, D., Senthilraja, R., & Thanappan, S. (2024). Development of Digital Twin Technology in Hydraulics Based on Simulating and Enhancing System Performance. *Journal of Cybersecurity & Information Management*, 13(2).

[19]Paulchamy, B., Uma Maheshwari, R., Sudarvizhi AP, D., Anandkumar AP, R., & Ravi, G. (2023). Optimized Feature Selection Techniques for Classifying Electrocorticography Signals. Brain-Computer Interface: *Using Deep Learning Applications*, 255-278.

[20]Paulchamy, B., Chidambaram, S., Jaya, J., & Maheshwari, R. U. (2021). Diagnosis of Retinal Disease Using Retinal Blood Vessel Extraction. In *International Conference on Mobile Computing and Sustainable Informatics: ICMCSI 2020* (pp. 343-359). Springer International Publishing.

[21]Maheshwari, U. Silingam, K. (2020). Multimodal Image Fusion in Biometric Authentication. *Fusion: Practice and Applications*, (), 79-91. DOI: https://doi.org/10.54216/FPA.010203

[22]R.Uma Maheshwari (2021). ENCRYPTION AND DECRYPTION USING IMAGE PROCESSING TECHNIQUES. *International Journal of Engineering Applied Sciences and Technology*, 5(12);219-222

[23]N.V., R.K., M., A., E., B., J., S.J.P., A., K. and S., P. (2022), Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors, *International Journal of Pervasive Computing and Communications*, Vol. 18 No. 4, pp. 407-418. https://doi.org/10.1108/IJPCC-08-2020-0107

[24]Subramani, P., K, S., B, K.R. *et al.* (2023). Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients. *Pers Ubiquit Comput* 27, 831–844 https://doi.org/10.1007/s00779-021-01531-6

[25]Subramani, P.; Rajendran, G.B.; Sengupta, J.; Pérez de Prado, R.; Divakarachari, P.B. (2020). A Block Bi-Diagonalization-Based Pre-Coding for Indoor Multiple-Input-Multiple-Output-Visible Light Communication System. *Energies 13*, 3466. https://doi.org/10.3390/en13133466

[26]Shivappriya, S.N.; Karthikeyan, S.; Prabu, S.; Pérez de Prado, R.; Parameshachari, B.D. (2020) A Modified ABC-SQP-Based Combined Approach for the Optimization of a Parallel Hybrid Electric Vehicle. *Energies 13*, 4529. https://doi.org/10.3390/en13174529

[27]Maheshwari, R. U., & Paulchamy, B. (2024). Securing online integrity: a hybrid approach to deepfake detection and removal using Explainable AI and Adversarial Robustness

Training. *Automatika*, *65*(4), 1517–1532. https://doi.org/10.1080/00051144.2024.2400640

[28]Maheshwari, R.U., Kumarganesh, S., K V M, S. *et al.* Advanced Plasmonic Resonance-enhanced Biosensor for Comprehensive Real-time Detection and Analysis of Deepfake Content. *Plasmonics* (2024). https://doi.org/10.1007/s11468-024-02407-0

[29]Alkhatib, A., Albdor , L., Fayyad, S., & Ali, H. (2024). Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys: Securing IoT Children's Toys. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.417

[30]Sivananda Hanumanthu, & Gaddikoppula Anil Kumar. (2025). Deep Learning Models with Transfer Learning and Ensemble for Enhancing Cybersecurity in IoT Use Cases. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.1037

[31]P. Jagdish Kumar, & S. Neduncheliyan. (2024). A novel optimized deep learning based intrusion detection framework for an IoT networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.597

[32]Vutukuru, S. R., & Srinivasa Chakravarthi Lade. (2025). CoralMatrix: A Scalable and Robust Secure Framework for Enhancing IoT Cybersecurity. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.825

[33]Iqbal, A., Shaima Qureshi, & Mohammad Ahsan Chishti. (2025). Bringing Context into IoT: Vision and Research Challenges. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.760

[34]Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.18

[35]Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.19