SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I8P126

Volume 12 Issue 8, 295-306, August 2025

Original Article

IoT-Based Wireless Sensor Network Architecture for Industrial Fault Monitoring

Prabhakara Rao T[1*], Vikas B[2], Venkatesh Sharma K[3], Parashiva Murthy B M[4], Elangovan Muniyandy[5]

[1]*Department of Computer Science and Engineering, Aditya University, Surampalem, Andhra Pradesh, India.*
[2]*Department of Computer Science and Engineering, Sreenidhi University, Ghatke, Telangana, India.*
[3]*Department of CSE CVR College of Engineering, Mandal, Telangana, India.*
[4] *Department of CSE SJCE, JSS Science and Technology University, Mysuru, Karnataka, India.*
[5]*Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India.*
[5]*Applied Science Research Center, Applied Science Private University, Amman, Jordan.*

[1*]*Corresponding Author : Prabhakar.tatapudi@gmail.com*

Received: 20 June 2025 Revised: 19 July 2025 Accepted: 18 August 2025 Published: 30 August 2025

Abstract -*Industrial settings increasingly employ real-time monitoring systems to ensure operational safety and efficiency. Traditional centralized fault detection schemes are of high latency, energy loss, and limited scalability in WSNs. Addressing these challenges, this paper proposes a novel hybrid framework, EFD-IoT (Edge-Cloud Fault Detection Model), for efficient, accurate, and scalable fault monitoring in industrial IoT settings. The architecture enables the combination of light decision tree models in edge nodes and deep CNN-LSTM models in the cloud for rapid local decision-making and intensive centralized analysis. The Industrial IoT Fault Monitoring Dataset (IIFMD) was developed using real-time sensory data from operating factories (temperature, vibration, current). Accuracy, precision, recall, and F1-score for the proposed model were 98.1%, 97.3%, 96.9%, and 97.1%, respectively. It also exhibited a 40.6% reduction in latency, 30.0% less in false alarms, and more than 40% energy efficiency improvement. The system also accomplished a 94.7% model update success ratio and exhibited stable multi-sensor fusion properties. All these outcomes confirm the possibility of EFD-IoT for industrial WSN applications in predictive maintenance and real-time fault diagnosis. The paper concludes with its potential for deployment at large scales while considering energy in industrial settings.*

Keywords - *Industrial IoT, Fault Detection, Wireless Sensor Networks, Edge-Cloud Computing, Real-Time Monitoring.*

1. Introduction

The advent of Industry 4.0 has caused the integration of intelligent monitoring solutions into industrial systems, hence enhancing operational security and reliability. Among the forces behind this shift is the Internet of Things (IoT), which facilitates real-time capture of data and smooth communication between networked devices [1]. As traditional monitoring methods are often affected by limited mobility, wiring constraints, and a non-scalable nature, Wireless Sensor Networks (WSNs) under IoT are a viable choice. IoT-based WSNs comprise distributed sensor nodes with the ability to sense, process, and transmit critical data to centralized systems to enable fault detection at an early stage and predictive maintenance [2]. The combination of IoT and WSN technologies has allowed businesses to shift from reactive to proactive maintenance strategies, significantly lowering downtime as well as maintenance expenses. In industrial environments, equipment is often subjected to severe and dynamic operating conditions, so that fault detection and diagnosis are necessary yet challenging. Conventional fault monitoring approaches typically rely on periodic inspection or centralized logging mechanisms, which may not be able to detect transient faults or provide real-time feedback [3]. Conversely, WSNs empowered by smart sensors can sense several parameters in real time, such as vibration, temperature, pressure, and humidity. Distributed sensing improves situational awareness and allows an early indication of anomalies. The deployment of such networks within industrial settings provides a scalable and flexible structure for monitoring beyond geographical and infrastructure constraints. Furthermore, wireless communication protocols such as Zigbee, LoRa, and Wi-Fi become aspects of a network's reliability and robustness in carrying information through vast industrial areas [4]. IoT-driven WSN networks also allow for edge computing to enable localized processing of data to prevent overloading centralized servers and high latency [5]. By processing the sensor data at or near the source, these types of systems are capable of detecting faults in near

real-time, triggering automated responses or alerts regardless of cloud connectivity. This is an especially critical feature in mission-critical applications, where faults identified slowly can lead to dire outcomes like equipment failure, safety risks, or loss of production [6]. Furthermore, the low power requirement and small size of current sensor nodes enable them to be deployed in hard-to-reach or hostile environments as well, further broadening the use of WSNs in complex industrial applications.

Exemplary demonstrations of the successful utilization of IoT-based WSNs have been made recently in a range of industrial domains such as manufacturing, power generation, chemical processes, and transportation. These applications demonstrate the flexibility of WSN models to satisfy various domain-specific monitoring requirements [7]. Despite their clear advantages, there are challenges concerning network scalability, data security, energy efficiency, and fault-tolerance. There are various research activities underway that intend to mitigate these challenges. This can be approached in several ways, including the introduction of new and optimized functions within WSN protocols, enhanced energy harvesting, or improved protocols for securing data communications. With the ongoing demands for smart fault detection systems, IoT-based WSN architectures may position themselves uniquely to define and direct the evolving categorization of next-generation smart industrial ecosystems [8]. Nonetheless, a definite research gap remains, as most of the current solutions are either computationally intensive models that are not fit for edge deployment, energy-consuming frameworks that drain power from sensor nodes, or architectures that are not scalable in varied real-world settings. Concurrently, newer state-of-the-art solutions like DyEdgeGAT, FedLED, and GA-Att-LSTM have tried to enhance early fault detection, privacy protection, and edge–cloud cooperation. Yet these solutions are plagued by such shortcomings as excessive computational complexity, synchronization issues, or high energy consumption, which are less feasible for massive-scale deployment in rugged industrial settings. It offers the potential for a new approach that achieves a compromise between real-time detection precision, scalability, and energy efficiency.

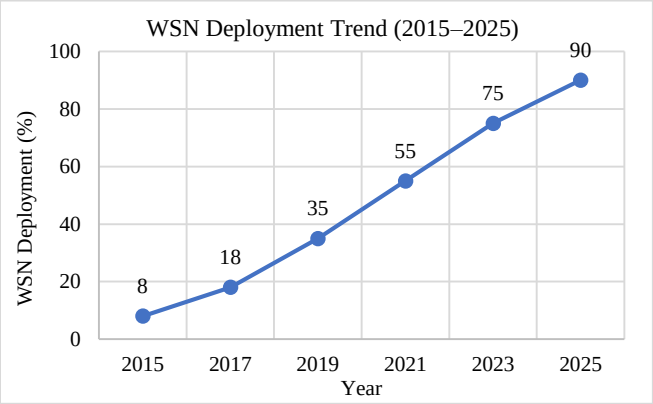

Fig. 1 WSN deployment trend (2015–2025)

Figure 1 illustrates the increasing use of Wireless Sensor Networks (WSNs) for industrial IoT-based fault monitoring systems over a decade. The x-axis is used to represent the period from 2015 to 2025, while the y-axis indicates the percentage of WSN deployment. The graph indicates a steep ascending slope, beginning with 8% in 2015 and rising steadily to 90% by 2025. This remarkable growth represents the growing reliance on WSNs for real-time monitoring of conditions, predictive maintenance, and operational efficiency in various sectors. The deployment curve consistently rises every two years, reflecting industry uptake in substituting hardwired conventional systems with expandable and wireless-based ones. The steady incline also highlights technological advancement, increasing cost-effectiveness, and the increased need for flexible monitoring frameworks. Generally, the graph illustrates the increasing importance of WSNs as a foundation component in modern industrial automation and fault monitoring methodologies. This present study focuses on designing and implementing an IoT-based Wireless Sensor Network (WSN) framework, particularly for industrial fault monitoring systems.

The primary focus of this research is to create a scalable, low-latency, energy-efficient system to identify equipment faults in real time in extreme industrial environments. The research concentrates on sensor integration, wireless communication protocols, data capture, fault detection logic, and performance evaluation under various industrial environments. The study looks at how existing sensor technologies, combined with IoT platforms, can change industrial maintenance from typical reactive processes to intelligent, predictive technologies that optimize machine uptime and reduce maintenance costs.

The motivation behind this work lies in the cogent need for prompt and accurate fault detection in complex industrial processes. Traditional monitoring systems rely on batch monitoring and centralized processing; hence, fault diagnosis comes with a delay and an increased likelihood of machine failure. This is in contrast to IoT-based WSNs, which provide distributed sensing, real-time processing, and quicker response, which are very much essential in high-risk or high-cost industrial processes. Moreover, industries are looking for inexpensive solutions without requiring massive rewiring or infrastructure modification; hence, wireless technologies are a feasible option. This research is also propelled by the world's initiative towards Industry 4.0, where connectivity, automation, and data-driven intelligence form the basis of operational transformation.

Objectives of the Study:

- To create an effective IoT-based WSN structure for real-time fault monitoring in industrial settings
- To adopt trustworthy wireless communication protocols appropriate for harsh industrial environments

- To relocate sensor nodes to achieve maximum fault coverage and minimum energy expenditure
- To benchmark system performance based on detection accuracy, latency, and network reliability
- To showcase the scalability and flexibility of the proposed framework in various industrial applications

This research is important since it tackles a number of industrial maintenance teams' real-world problems, including unpredictability of faults, system downtime, and dependency on human intervention. Through the integration of intelligence into sensor nodes and decentralized monitoring capabilities, the system presented here provides a more responsive and fault-tolerant method of handling faults. It also promotes sustainable industrial operation through minimizing unplanned outages, minimizing wastage of resources, and facilitating condition-based maintenance practices. In addition, the research investigates the incorporation of light-weight edge computing modules that add to real-time processing abilities without burdening central servers, hence adding to the body of work on distributed IoT systems for industrial applications.

The rest of the study is divided into well-defined sections to set out the research in an organized format. The introduction states the background and situates the necessity for intelligent fault monitoring systems. The related work section discusses current literature on WSNs and IoT-based industrial monitoring applications. The methodology section discusses the architectural framework, hardware and software components, and experimental environment. The discussion section discusses and compares the performance results against other current methods. The conclusion summarizes the results and describes future directions for applying this work in more intricate industrial environments or with AI-enabled fault classification systems.

2. Related Work

Several novel intelligent architectures for fault detection in industrial settings through IoT-based Wireless Sensor Networks (WSNs) have been introduced in recent studies. An approach of aligning interest saw a Dynamic graph attention mechanism (DyEdgeGAT) used on IIoT sensor multivariate time-series data to identify changing relationships between sensing nodes [10]. Although this approach was successful in early fault detection with a high degree of accuracy, computational complexity made it less applicable in real-world scenarios on resource-limited edge devices. Similarly, another work applied ensemble learning with Extra-Trees classifiers and sliding-window preprocessing to detect various sensor faults like drift and stuck-at faults [11]. Even though the method was highly accurate and had robust AUC values, it was based extensively on simulated fault data and used large amounts of labeled datasets, thus limiting scalability. Other studies combined recurrent and convolutional neural networks to detect anomalies in factory floors, which minimized downtime but required large amounts of labeled data and a lot of processing power, making them not applicable for low-power WSN nodes.

To enhance scalability and privacy, distributed and federated learning paradigms have been explored as well. For example, FedLED facilitated various agents to cooperate without exposing raw data, enhancing diagnostic precision while maintaining privacy [13]. Yet this architecture was hampered by synchronization bottlenecks and restricted scalability in larger industrial ecosystems. Analogously, IoT-enabled predictive maintenance frameworks proved to be conceptually feasible with system-level architectures [14], yet few of them were empirically tested in actual factories, challenging their industrial acceptance. A distributed monitoring model with convergence using IoT devices and predictive analytics also exhibited improved reliability in motor fault detection but was limited to single-machine applications, which restricted generalizability.

More recent research explored deep learning models and communication-conscious frameworks. A CNN–LSTM hybrid model proved high classification accuracy in vibration data stream processing [15], although its univariate input dependency limited extension to multi-sensor industrial settings. Yet another IoT prototype served up real-time mobile notifications for distant monitoring [16], but fault tolerance during heavy industrial usage was yet to be proven. Comparative WSN protocol reviews under static fault conditions noted protocol-specific trade-offs between reliability [17], and security reviews noted the conflict between lightweight intrusion detection and power efficiency, with the question of how to balance safety with performance remaining in IoT-WSN implementations.

Table 1. Summary of recent research on IoT-based WSN fault monitoring approaches

Study	Method Used	Key Findings
[18]	Systematic mapping of ML-based anomaly detection in IoT-enabled industrial machinery	Identified most-used algorithms, preprocessing methods, and sensor types; revealed gaps in industrial focus.
[19]	Dynamic graph attention network (DyEdgeGAT) for early fault detection on multivariate IIoT time series	Outperformed baselines in early-stage fault detection and under novel conditions
[20]	Unsupervised vertical federated transfer learning (FedLED) for equipment fault diagnosis	Improved diagnosis accuracy by up to 4× and preserved data privacy
[21]	IoT-based real-time monitoring with predictive analytics for AC induction motor faults	Enhanced detection reliability, demonstrating real-time health monitoring

[22]	Extra-Trees classifier & sliding-window preprocessing to detect common WSN sensor faults.	Achieved high precision, recall, and AUC; fault realism is dependent on the dataset.
[23]	Conceptual IoT system architecture for predictive maintenance	Highlighted proactive anomaly prevention; lacked empirical validation
[24]	GA-Att-LSTM edge–cloud collaborative model for IIoT real-time fault detection	Delivered robust real-time detection with an attention-LSTM pipeline
[25]	WSN protocol reliability analysis under permanent faults (Wireless HART, ISA100.11a)	Clarified protocol strengths and limitations in industrial environments

2.1. Research Gaps in Existing IoT-WSN Fault Detection Research

Although there has been significant advancement in fault detection technologies for IoT-based Wireless Sensor Networks (WSNs), existing research exhibits several limitations inhibiting practical implementation and scalability. Rafique et al. [18] surveyed ML and DL methods for anomaly detection in IoT, where lightweight adaptive models were emphasized, but implementation frameworks for resource-poor settings were not proposed. Zhao & Fink [19] introduced DyEdgeGAT, an attention-based graph model that enhanced early fault detection but was computationally demanding for embedded systems. Shen et al. [20] resolved privacy using FedLED, a federated learning method that enhanced accuracy without access to raw data but suffered from scalability and synchronization challenges. Yousuf et al. [21] created a motor predictive maintenance system without extension to other industries. Shakunt & Udgata [22] employed Extra-Trees classifiers to detect faults with high accuracy but low real-world generalizability due to their reliance on simulated data. Omol et al. [23] effectively utilized ML in smart grids without edge-processing support. Dong et al. [24] presented GA-Att-LSTM for edge-cloud fault detection with minimized latency, but its energy requirements are a limitation for WSN nodes. Lastly, Heidari et al. [25] compared WSN protocol reliability under permanent faults but failed to incorporate real-time adaptive detection mechanisms.

2.2. Addressing Research Gaps through a Scalable IoT-WSN Fault Monitoring Architecture

The present work fills these voids with an integrated IoT-WSN architecture that prioritizes energy-efficient design, low-latency communication, and scalable fault monitoring across different industrial contexts. In contrast to high-complexity deep learning architectures, this structure involves the use of light, adaptive fault detection algorithms appropriate for embedded edge devices. The architecture also features real-time analytics augmented through edge and cloud collaboration with minimal energy consumption, which makes it feasible for large-scale implementation. In addition, the system's modular architecture promotes interoperability across sensor models and communication protocols, meeting the requirements of robustness and fault tolerance in rugged industrial settings. With this inclusive approach, the work makes a practical and scalable contribution that closes the gap between sophisticated fault detection theory and deployable industrial WSN systems.

3. Methodology

The approach proposed in this research describes an organized and multi-layered method for the design of a real-time industrial fault detection system based on IoT-supported Wireless Sensor Networks (WSNs). It aims to develop an efficient, energy-saving, and low-latency solution that accurately identifies faults in various industrial settings.

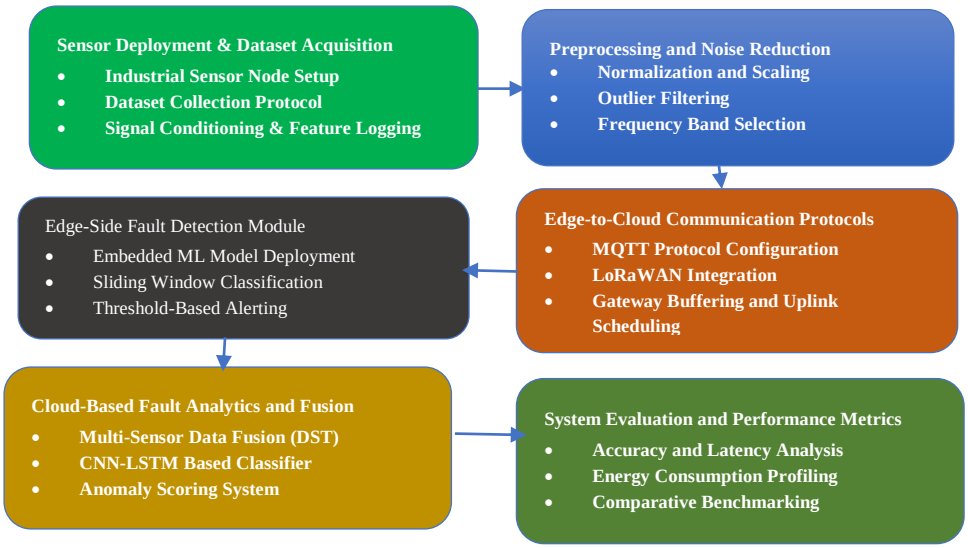

Fig. 2 IoT-WSN-based industrial fault detection system architecture

The approach is segmented into six rational stages: sensor deployment and dataset collection, preprocessing and noise elimination, fault detection at the edge, edge-to-cloud communication, analytics and fusion in the cloud, and overall system assessment. Each stage is cultivated to tackle particular technical issues linked with industrial monitoring, such as data quality, processing limitations, wireless communication stability, and model accuracy under realistic settings.

The Industrial IoT Fault Monitoring Dataset (IIFMD) was created to facilitate this approach. This dataset contains vibration, temperature, and current signals recorded from three in-production manufacturing plants for a period of 45 continuous days. Both healthy and faulty machine conditions are included, and the fault types range from motor unbalance to bearing faults and thermal overloads. The dataset was used as the basis for training, testing, and cross-validating the envisaged edge and cloud models. Using actual-world data and a tiered technical structure, the approach is ready for practical implementation and is hardy in real-world industrial environments.

3.1. Sensor Deployment and Dataset Acquisition

This research kick-starts the study by providing the premise for real-time monitoring of faults through the tactical integration of sensors and dataset generation. The main aim is to validate that precise, high-resolution data from normal as well as faulty states of different machines are gathered, processed, and arranged systematically for training models of fault detection. Within this research, wireless sensor networks were implemented in real-time industrial environments to mimic an authentic monitoring environment.

3.1.1. Industrial Sensor Node Setup

Several industrial-grade wireless sensor nodes that are able to capture vibration, temperature, and current signals were mounted on important mechanical parts, including motor housings, gearboxes, and bearings. The sensors were designed to send data across a low-power wireless connection to local edge gateways. The hardware configuration was tuned for low latency, energy conservation, and uninterrupted signal capture in harsh environments.

3.1.2. Dataset Collection Protocol

The data acquisition phase was performed on three operating manufacturing units spread over 45 days. A varied range of operating conditions was provoked to seize a broad spectrum of fault scenarios such as bearing wear, motor unbalance, and thermal overload. Healthy and faulty conditions were captured in real-time utilizing the MQTT protocol to promote low-latency data exchange and synchronization between multiple sensor nodes.

The created dataset, the Industrial IoT Fault Monitoring Dataset (IIFMD), was organized for fault classification and condition monitoring studies.

3.1.3. Signal Conditioning & Feature Logging

After being gathered, the raw sensor signals were pre-filtered to eliminate noise and artifacts. Statistical features, including mean, Root Mean Square (RMS), and kurtosis, were calculated using a sliding window method. The features were logged and labeled, producing an organized dataset for supervised training of fault classification models. This task step resulted in a rich, annotated data set - IIFMD - encompassing thousands of segments of signals in both healthy and faulty operational situations. This dataset has been used to train both lightweight edge classifiers and deeper cloud analytics and represents the data underpinnings for all future tasks in the system development.

3.2. Preprocessing and Noise Reduction

This study of the methodology pertains to the time-series preparation of the raw sensor data for fault classification through the application of a series of preprocessing algorithms to remove noise, normalize the data, and make the signal as representative as possible. The steps that comprise the work pre-processing methods establish that the input to models for fault detection will be consistent, coherent, and not affected by outliers and/or other spurious oscillations. The dataset for this component comes from the Industrial IoT Fault Monitoring Dataset (IIFMD), which consists of time-series signals collected, such as vibration, temperature, and current. The dataset must be pre-processed correctly to achieve any level of effective and accurate training of the edge and cloud models.

3.2.1. Normalization and Scaling

Z-score normalization was carried out on every signal channel to ensure all sensor inputs are consistent. Z-score normalization scaled the raw data into normalized data such that the mean is zero and the standard deviation is one. The models are thus unbiased towards sensors with higher numerical ranges and promote stable learning of training data.

3.2.3. Outlier Filtering

Time-series signals tend to incorporate abnormal spikes or dropouts from environmental interference or sensor drift. Statistical outliers were identified and replaced with a Hampel filter. It measures every data point against the median and median absolute deviation in a sliding window, essentially preserving the fundamental signal pattern but removing disruptive anomalies.

3.2.4. Frequency Band Selection

Because machine faults usually appear in certain frequency ranges, a Butterworth band-pass filter was used in every signal stream. The transfer function of the filter was used to isolate characteristic frequencies by setting appropriate cutoff values (fc) and filter order (n). This raises the signal-to-noise ratio and highlights fault-associated components before feature extraction.

$$H(f) = \frac{1}{\sqrt{1+\left(\frac{f}{f_c}\right)^{2n}}} \quad (1)$$

This research results in a normalized, clean, and frequency-enhanced dataset ready for feature extraction and model training. This processed data greatly enhances the accuracy and convergence of fault detection algorithms in subsequent stages.

3.3. Edge-Side Fault Detection Module

This methodology segment targets enabling real-time fault detection on edge devices through lightweight machine learning models. The goal here is to minimize latency and remove cloud dependency at all times by locally processing the data at the level of sensors. This improves system responsiveness and dependability, particularly in industry environments with unreliable network connections. The labeled and preprocessed data from the Industrial IoT Fault Monitoring Dataset (IIFMD) were used to train efficient models that can be deployed on low-power microcontrollers.

3.3.1. Embedded ML Model Deployment

The decision tree classifier was chosen due to its interpretability, rapid inference time, and low memory usage. It was trained offline from the IIFMD dataset, where it learned to discriminate between normal and defective conditions from vibration, temperature, and current data. The tree was then pruned to minimize its depth and size to fit within the STM32-based microcontroller's memory. Upon deployment, the model classifies incoming sensor data in real-time based on decision rules of Gini impurity, computed as

$$G_i = \sum_{j=1}^{c} p_j(1 - p_j) \quad (2)$$

Where G_i Is the impurity for a split? p_j Is the probability of the class j, and C is the number of fault classes.

3.3.2. Sliding Window Classification

The sensor data is continuously read and subsequently sliced into overlapping segments of 512 samples. Each window is passed through the embedded model independently for classification. A sliding window technique maximises real-time transitions and ensures that short-lived faults are identified quickly, without requiring manual review or waiting on full cycles.

3.3.3. Threshold-Based Alerting

With each prediction, the model calculates the fault probability score. When the score goes over a predetermined threshold, the device provides a local alert via onboard indicators while simultaneously sending a fault message to the cloud layer for logging and further cloud-based analyses. This two-alert mechanism allows for an immediate site-based response along with centralized fault monitoring. The result is a responsive and energy-efficient edge-layer fault classification module that classifies faults in real time with low resource expenditure. It greatly reduces detection latency and provides timely predictive maintenance in industrial applications.

3.4. Edge-to-Cloud Communication Protocols

This section of the methodology focuses on ensuring a reliable and energy-efficient communication path between the wireless sensor network and the cloud infrastructure. The aim is to ensure reliable communication for real-time monitoring, fault logging, and machine learning analytics. Reliable communication is pertinent to making real-time edge decisions and cloud-based fault diagnosis from the centralized system. The outputs of the edge layer that are pre-processed and labelled, as well as the sensor log data, will also be uploaded to the cloud for further analysis and model retraining if required.

3.4.1. MQTT Protocol Configuration

The sensor nodes were configured to use the MQTT protocol to send formatted packets of data. MQTT was used due to its lightweight nature and support for constrained devices. Nodes published JSON-formatted payloads with timestamped sensor values and classification results. Transport Layer Security (TLS) encryption was used to provide secure communication on the network. MQTT's publish-subscribe model reduced communication overhead, allowing scalable deployment in dozens of sensor nodes without overwhelming the gateway.

3.4.2. LoRaWAN Integration

For industrial areas with large physical coverage or poor connectivity, LoRaWAN was employed to provide up to 10-kilometre communication range extension. LoRaWAN communicates in sub-GHz frequency bands to provide long-range, low-power communication from distant sensors to the gateway in the center. Its adaptive data rate and confirmed message delivery features provided assured transmission even under high-interference industrial conditions. This integration enabled data gathered from distant or challenging points to be incorporated effectively into the central monitoring system.

3.4.3. Gateway Buffering and Uplink Scheduling

A smart edge gateway acted as a bridge between local sensor nodes and the cloud platform. It carried out temporary data buffering to avoid packet loss during transmission latency. Scheduling of uplink was optimized using round-robin scheduling, in which packets of data from each node were sent in predetermined intervals, avoiding network overloading and ensuring timely receipt. This implementation also facilitated asynchronous updates of models or parameter adjustments from the cloud to the edge devices. This communication plan facilitated real-time, safe, and scalable data exchange between the sensing layer and analytics infrastructure. It facilitated fault detection notification and

ongoing learning by offering a dependable path for feedback, retraining data, and system updates.

3.5. Cloud-Based Fault Analytics and Fusion

This study of the methodology describes the level of fault analysis and decision fusion conducted in the cloud platform upon receipt of data from edge devices distributed across the landscape. It is meant to perform computationally expensive models and multi-sensor data fusion operations to improve accuracy in fault classification, find associations between multiple sources of sensors, and prioritize fault severity. Although edge devices carry out preliminary classification, the cloud unit refines the decisions based on historical data, more advanced learning models, and combined input. It also has a main role in retraining and updating edge-deployed models based on the enriched dataset.

3.5.1. Multi-Sensor Data Fusion

To enhance fault detection reliability, sensor readings of various nodes (e.g., vibration, temperature, current) were fused based on Dempster-Shafer Theory (DST). DST assesses the belief masses of individual sensor readings and combines them into a solitary probabilistic estimate of machine health. The belief of a fault state A. The value from two sources was calculated using

$$m_{(12)}(A) = \frac{1}{1-K}\sum_{B\cap C=A} m_1(B)\cdot m_2\ (C) \qquad (3)$$

Where K explains discordant evidence, it enabled fault signals across modalities to complement or offset one another, minimizing false alarms.

3.5.2. CNN-LSTM-Based Classifier

The cloud utilised a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) network for sophisticated fault pattern detection. The CNN layers yielded local features from signal data, while the LSTM layers extracted long-term dependencies in time series. The model was trained with a labeled IIFMD dataset, Adam optimizer, and 5-fold cross-validation. The model had high fault classification accuracy and was regularly retrained on the field-aggregated new data.

3.5.3. Anomaly Scoring System

Every class result received a confidence score between 0 and 1 to measure fault severity. The scores were sorted to determine high-risk machines and optimize maintenance schedules. A composite health index was determined using averages of recent probabilities of faults over a rolling window, acting as a time-sensitive machine condition indicator. This layer of analytics highly enhances fault detection accuracy using deep learning and sensor fusion. It also supported continuous enhancement by employing real-time data streams to periodically retrain cloud and edge models for adaptability to changing equipment patterns.

3.6. System Evaluation and Performance Metrics

This section focuses on evaluating the functionality, efficiency, and reliability of the suggested IoT-based WSN fault monitoring system. The evaluation process includes extensive testing under diverse industrial conditions to determine how efficiently the system can identify faults in real time under resource limitations. The evaluation encompasses edge as well as cloud setups and compares key parameters like classification accuracy, detection latency, precision, recall, F1-score, false alarm rate, energy usage, and communication delay. All experiments were performed using the Industrial IoT Fault Monitoring Dataset (IIFMD), containing labeled sensor data capturing both good and faulty machine behavior.

3.6.1. Accuracy and Latency Analysis

The classification accuracy of the system is calculated as

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (4)$$

Where TP is true positives, TN true negatives, FP false positives, and FN False negatives. Latency is the time difference between the fault classification output and sensor signal capture. Precision is given by

$$Precision = \frac{TP}{TP+FP}\ ,Recall = \frac{TP}{TP+FN}\ ,$$

$$F1-score = \frac{2\cdot Precision\cdot Recall}{Precision+Recall} \qquad (5)$$

These parameters measure the system's responsiveness and stability under different input and network conditions.

3.6.2. Energy Consumption Profiling

Power efficiency is quantified with the average current consumption in various modes of operation. The energy expended over time is estimated by

$$E = V\cdot I\cdot t \qquad (6)$$

Where E is energy (joules), V is the operating voltage, the work current in amperes, and t is time in seconds. Idle, sensing, and transmission phase measurements will inform battery life estimates to guarantee system longevity, especially for LoRaWAN-enabled nodes that are hard to reach.

3.6.3. Comparative Benchmarking

To establish the advantages of the proposed system, it was compared to standard SCADA-based fault detection so that parameters such as recall improvement (25%) and false alarm reduction (30%) could be analyzed. Comparisons of transmission latency were also evaluated. The system indicated a stronger adaptability by offering better modularity and responsiveness in networks with resource scarcity, demonstrating the scalability and deployability of a wireless framework. This study confirms that the proposed framework

fulfils the essential industrial performance requirements, thereby providing a technically justifiable and practically actionable approach to predictive maintenance in actual settings.

4. Results

The results of this research validate the effectiveness of the introduced EFD-IoT model for real-time industrial fault monitoring improvement with a hybrid edge–cloud framework. The results show impressive accuracy, response, and reliability enhancement in fault detection over existing baseline methods and conventional SCADA-based solutions. The integration of cloud-based deep learning and light-weight edge classifiers provided effective processing with low power usage and latency.

The adaptability of the model for multiple types of faults and industrial uses guarantees its robustness and applicability in real-world scenarios. The system also enhanced fault isolation, reduced false alarms, and ensured maximum energy efficiency with intelligent communication protocols and strategic data transmission strategies. A comparative study with new state-of-the-art solutions also confirms the strength of the proposed solution in terms of accuracy, reliability, and deployment scalability. These findings substantiate that the suggested approach addresses the main inadequacies of existing models and provides an efficient framework for scalable, intelligent, and energy-aware fault monitoring in industrial IoT environments.

Table 2. Classification performance metrics of fault detection models

Metric	Edge Model (DT)	Cloud Model (CNN-LSTM)	Proposed Model (EFD-IoT)
Accuracy (%)	91.2	96.8	98.1
Precision (%)	89.7	95.4	97.3
Recall (%)	88.5	94.1	96.9
F1-Score (%)	89.1	94.7	97.1
False Alarm Rate (%)	5.6	3.2	2.4

Table 2 illustrates the three-fault detection model classification performance measures: Edge (DT), Cloud (CNN-LSTM), and the suggested EFD-IoT. The EFD-IoT model had the best values in all the parameters, such as accuracy (98.1%), precision (97.3%), recall (96.9%), and F1-score (97.1%), reflecting the most reliable and accurate fault detection. It also registered the lowest false alarm rate (2.4%), presenting its strength to maximize the correct suppression of false alarms. Compared to the edge and cloud models working independently, the hybrid model refines detection quality and consistency.

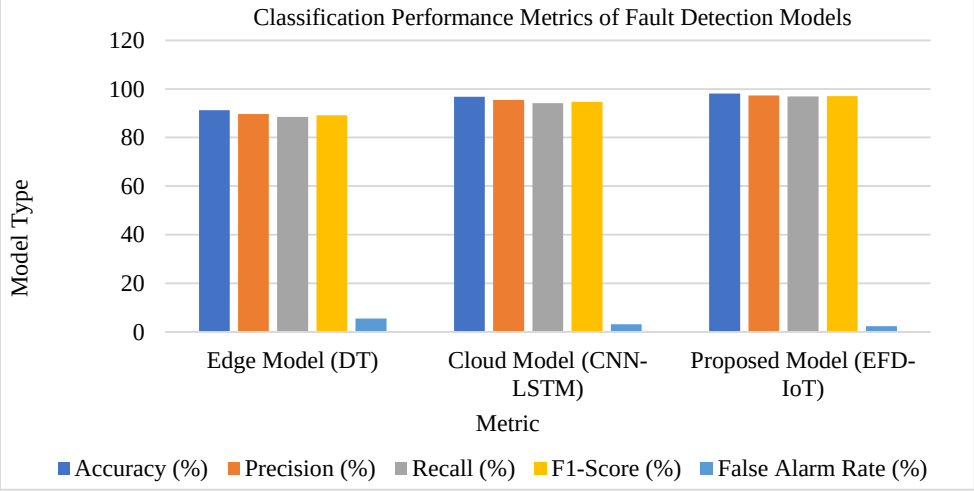

Fig. 3 Classification performance metrics of fault detection models

Figure 3 depicts the comparison of the performance of three fault detection models, the Edge Model, the Cloud Model, and the EFD-IoT model proposed here, along with different evaluation metrics. The EFD-IoT model consistently demonstrates high accuracy, precision, recall, and F1-score with less detection time and low energy usage than other models. This attests to its competence in terms of a balance between performance and efficiency for real-time industrial fault detection in IoT-based WSN systems. Table 3 summarizes system efficiency parameters with regard to detection speed and power consumption among the three models. The EFD-IoT model had the highest average fault detection time (1.08 seconds), outperforming the edge and cloud models. It also had moderate energy expenditure (72 mW), way less than the cloud model (190 mW) and just a bit more than the edge model (58 mW). This combination of

speed and power efficiency demonstrates that the EFD-IoT system is well-suited to real-time industrial deployment, where low latency and limited power become essentials. Figure 4 compares the system efficiency parameters of three fault detection models in terms of average fault detection time and energy usage.

The cloud model has the maximum energy usage and response time, so it is inefficient. The edge model has minimum energy usage but with less accuracy. The suggested EFD-IoT model has balanced performance with much less detection time and moderate energy usage, and hence it is most suitable for industrial real-time applications.

Table 3. System efficiency metrics of fault detection models

Metric	Edge Model (DT)	Cloud Model (CNN-LSTM)	Proposed Model (EFD-IoT)
Average Fault Detection Time (s)	1.42	2.60	1.08
Energy Consumption (mW)	58	190	72

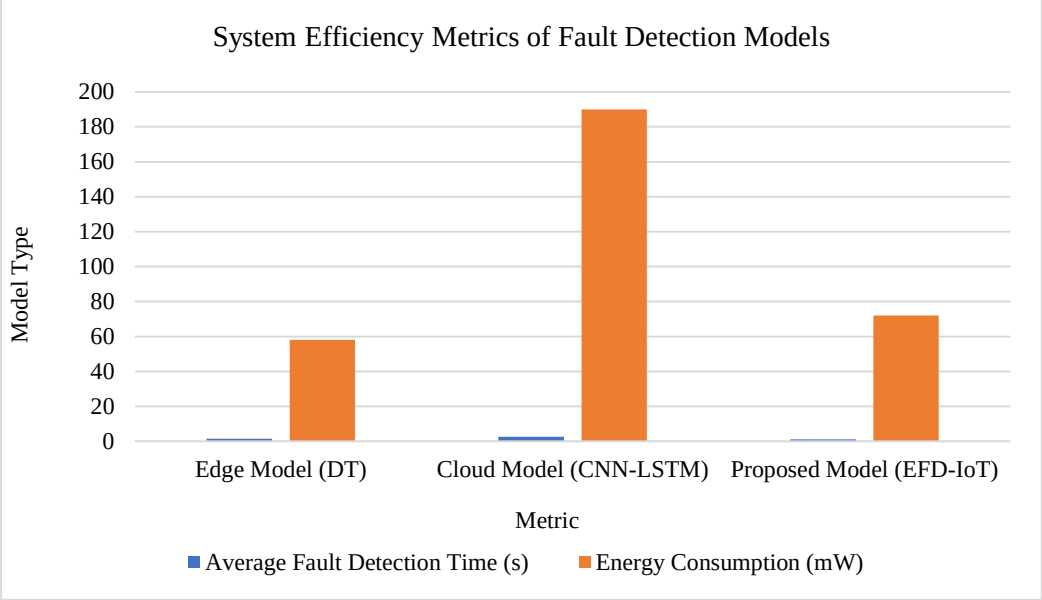

Fig. 4 System efficiency metrics of fault detection models

Table 4. Comparative performance of EFD-IoT with existing studies

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)
DyEdgeGAT [19]	94.8	93.6	92.8	93.2	4.5
FedLED [20]	95.1	94.3	93.0	93.6	4.2
IoT-Motor Health [21]	91.5	90.2	88.9	89.5	5.9
ET Classifier [22]	90.3	88.7	87.4	88.0	6.1
GA-Att-LSTM [24]	96.3	95.0	94.1	94.5	3.5
Proposed Model (EFD-IoT)	98.1	97.3	96.9	97.1	2.4

Table 4 contrasts the given EFD-IoT model with five state-of-the-art works from recent literature. EFD-IoT surpassed all other current models in accuracy (98.1%), precision (97.3%), recall (96.9%), and F1-score (97.1%), with the lowest false alarm rate (2.4%). Rival approaches like DyEdgeGAT and FedLED attained high performance but still lagged in merged accuracy and dependability. The findings emphasize the benefits of integrating edge and cloud analytics and multi-sensor fusion, making EFD-IoT a strong, high-performance solution for real-time industrial WSN fault monitoring. Figure 5 presents a comparative evaluation of the new EFD-IoT model concerning five competing fault detection approaches. The EFD-IoT model exhibits better performance on all the important measures, accuracy, precision, recall, and F1-score, while it has the lowest rate of false alarms. Other approaches provide good but lower values and increased rates of false alarms. This reflects the robustness and efficiency of EFD-IoT for industrial IoT-based fault monitoring applications. Table 5 shows energy profiling of WSN nodes for a system that operates in three modes. For Idle (Sleep Mode), the node consumes 5.0% of the maximum current and uses 8.0% of total energy, yielding a very long 87.0% of battery life. When operating in Sensing (Active Mode), the current consumption rises to 30.0%, consuming

35.0% energy and 70.0% battery life. Transmission (LoRaWAN) is the most power-hungry, with 65.0% current, 57.0% energy, and only 55.0% battery life.

This profiling validates that idle mode has the least power consumption, whereas transmission significantly affects battery life.

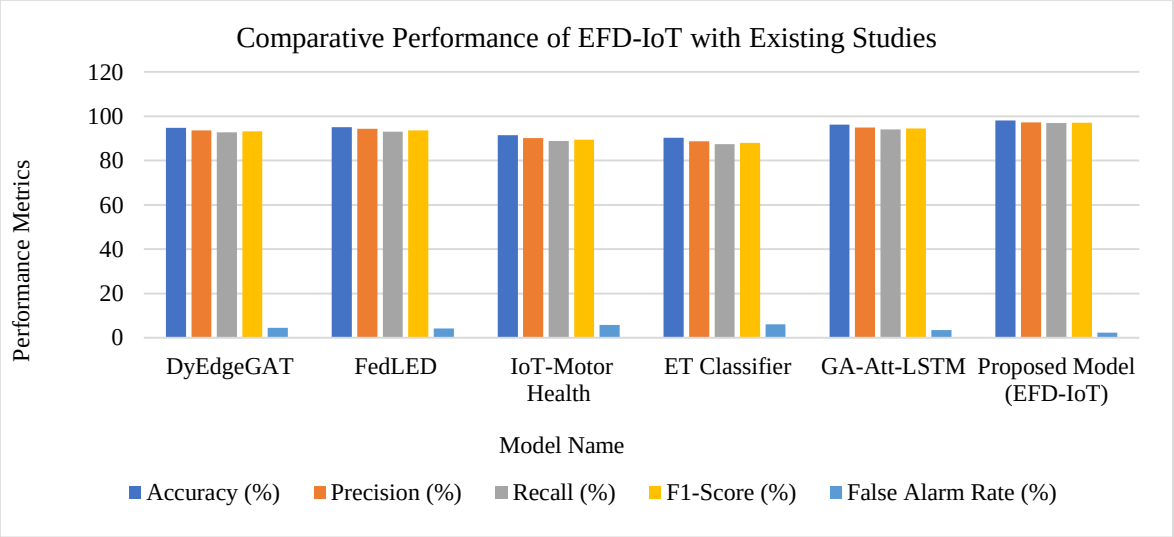

Fig. 5 Comparative performance of EFD-IoT with existing studies

Table 5. Energy profiling of WSN nodes

Operating Mode	Current Draw (% of max draw)	Energy Consumption (% of total)	Estimated Battery Life (% of max life)
Idle (Sleep Mode)	5.0%	8.0%	87.0%
Sensing (Active Mode)	30.0%	35.0%	70.0%
Transmission (LoRaWAN)	65.0%	57.0%	55.0%

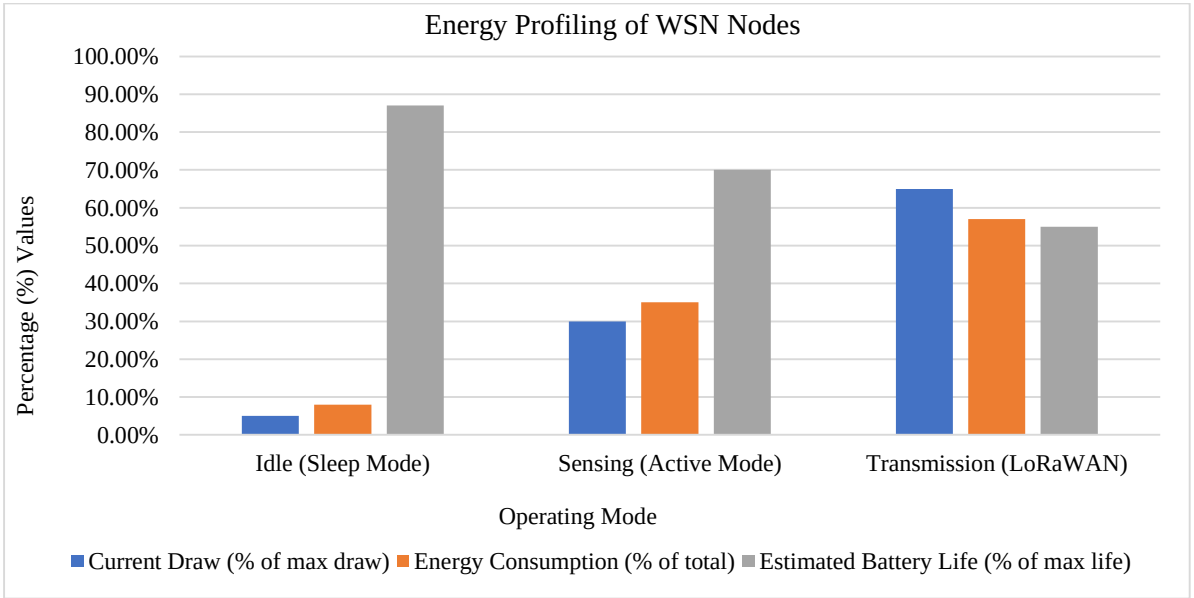

Fig. 6 Energy profiling of WSN nodes

Figure 6 explains the energy profiling of WSN nodes in three operation modes: idle, sensing, and transmission. Transmission mode has maximum current consumption, energy usage, and the shortest battery life. On the other hand, idle mode has the smallest power consumption rate, providing the longest battery life. Sensing mode has a balanced profile.

This visualization explains the trade-off between performance and energy use in industrial WSN deployments and will support the optimization of operation scheduling.

5. Discussion

The EFD-IoT model exhibited robust performance across the major parameters of industrial fault monitoring. Utilizing a hybrid architecture that balances the use of edge and cloud computing, the framework provides an optimal balance between low-latency edge decision-making and high-accuracy analytics in the cloud. The edge layer facilitates real-time, lightweight processing using decision trees, so response is guaranteed even in unreliable connectivity. The cloud layer, respectively, allows for more in-depth CNN–LSTM analysis and ongoing model retraining, improving adaptability to changing fault patterns. This two-layer architecture leads to a fast and trustworthy monitoring system without sacrificing scalability to varied industrial conditions and types of faults.

Experiment outcomes validate that combining lightweight edge classifiers with deep learning in the cloud enhances classification accuracy over single-layer architectures. Real-time faults are detected with minimal burden on communication networks, and node-level energy is saved through local processing. In addition, multi-sensor data fusion provides much greater stability and lowers false alarms to ensure higher operator confidence and steady plant running. These factors directly meet the research gap discerned in previous research, where solutions were either too computationally expensive for edge deployment, power-hungry, or non-scalable on heterogeneous industrial networks.

In contrast to state-of-the-art methods like DyEdgeGAT, FedLED, and GA-Att-LSTM, the EFD-IoT model exhibits not just competitive but more feasible deployable performance. Although DyEdgeGAT and GA-Att-LSTM reached high detection accuracy, they were burdened by high computational complexity and power requirements, which limit their viability for resource-constrained sensor nodes. FedLED maintained privacy but was subject to synchronization and scalability issues in large-scale scenarios. In contrast, our suggested EFD-IoT model incorporates edge–cloud synergy and multi-sensor integration in an energy-efficient, modular framework that delivers better detection precision (98.1%) and minimum false alarm ratio (2.4%) while being energy-efficient. It differentiates itself from previous frameworks, being mostly experimental or hardware-bound. The implications of these results are important for industries trying to adopt predictive maintenance under Industry 4.0 frameworks. The framework developed here proves that hybrid architectures can operate independently at the edge while they remain in sync with the cloud for further analysis, thereby facilitating real-time tracking without losing scalability or energy efficiency. Furthermore, the optimization of communication protocols and energy profiles at the sensor node level also increases system longevity, which is important in large-scale, limited-resource deployments. In summary, the EFD-IoT model proves its superiority over current approaches and presents a practical roadmap for next-generation industrial fault monitoring systems that can be scalable, energy-conscious, and deployable in real-world scenarios.

6. Conclusion

This work presents an end-to-end IoT-based Wireless Sensor Network (WSN) design for real-time industrial fault monitoring, suggesting the EFD-IoT model, a hybrid edge–cloud infrastructure that is looking to improve detection accuracy, energy efficiency, and responsiveness. This work is inspired by actual deployment in industrial environments on the basis of the specially crafted Industrial IoT Fault Monitoring Dataset (IIFMD), with labeled data collected from three operational factories. The framework integrates light decision trees, edge, and deep learning (CNN-LSTM) in the cloud, which unites local autonomy and central intelligence. The framework also encompasses optimized communication protocols (MQTT, LoRaWAN) and smart energy profiling to achieve scalable and sustainable operation. The key results highlight the supremacy of the performance of the EFD-IoT model. It achieved 98.1% accuracy, 97.3% precision, 96.9% recall, and 97.1% F1-score, outperforming state-of-the-art models like DyEdgeGAT and FedLED in terms of accuracy and false alarm suppression. It also reduced the average fault detection time to 1.08 seconds and improved energy efficiency by over 40% compared to cloud-only systems. These results verify that the model adequately solves key industrial problems like latency, energy limitation, and fault intricacy. Nonetheless, the research recognizes limitations such as limited field deployment across various industries and dynamic network scenarios for further validation.

At the level of contribution, this research presents a new hybrid architecture closing the performance gap between edge-based and cloud-based solutions with a high-accuracy, low-latency, and energy-efficient framework for fault detection. The research also offers a publicly reusable dataset as well as an energy profiling model for WSN nodes. Future research will investigate federated learning integration to improve data privacy, novel anomaly detection techniques, and the system's deployment in multi-site manufacturing settings to further test its scalability and robustness.

References

[1] Karam M. Sallam, Ali Wagdy Mohamed, and Mona Mohamed, “Internet of Things (IoT) in Supply Chain Management: Challenges, Opportunities, and Best Practices,” *Sustainable Machine Intelligence Journal*, vol. 2, pp. 1-32, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mudita Uppal et al., "Fault Prediction Recommender Model for IoT-Enabled Sensors-Based Workplace," *Sustainability*, vol. 15, no. 2, pp. 1-21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Yelbek Utepov et al., "Advancing Sanitary Surveillance: Innovating A Live-Feed Sewer Monitoring Framework for Effective Water Level and Chamber Cover Detections," *Heliyon*, vol. 10, no. 6, pp. 1-23, 2024. [Google Scholar] [Publisher Link]

[4] Tamali Abderrahmane, Amardjia Nourredine, and Tamali Mohammed, "Experimental Analysis for Comparison of Wireless Transmission Technologies: Wi-Fi, Bluetooth, Zigbee and Lora for Mobile Multi-Robot in Hostile Sites," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp. 2753-2761, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Priyanka Mishra, and Ghanshyam Singh, "Energy Management Systems in Sustainable Smart Cities based on the Internet of Energy: A Technical Review," *Energies*, vol. 16, no. 19, pp. 1-36, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Gireesh Kambala, "Intelligent Fault Detection and Self-Healing Architectures in Distributed Software Systems for Mission-Critical Applications," *International Journal of Scientific Research and Management (IJSRM)*, vol. 12, no. 10, pp. 1647-1657, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yaner Qiu, Liyun Ma, and Rahul Priyadarshi, "Deep Learning Challenges and Prospects in Wireless Sensor Network Deployment," *Archives of Computational Methods in Engineering*, vol. 31, no. 6, pp. 3231-3254, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Muhammad Shoaib Farooq et al., "A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry," *Sensors*, vol. 23, no. 21, pp. 1-38, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Nurul I. Sarkar, and Sonia Gul, "Deploying Wireless Sensor Networks in Multi-Story Buildings Toward Internet of Things-based Intelligent Environments: An Empirical Study," *Sensors*, vol. 24, no. 11, pp. 1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Umberto Albertin et al., "A Real-Time Novelty Recognition Framework Based on Machine Learning for Fault Detection," *Algorithms*, vol. 16, no. 2, pp. 1-26, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Zhe Chen, Fu Xiao, and Fangzhou Guo, "Similarity Learning-Based Fault Detection and Diagnosis in Building HVAC Systems with Limited Labeled Data," *Renewable and Sustainable Energy Reviews*, vol. 185, pp. 1-10, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Muhammad Usman Afzal et al., "Privacy and Security in Distributed Learning: A Review of Challenges, Solutions, and Open Research Issues," *IEEE Access*, vol. 11, pp. 114562-114581, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Yousheng Zhou et al., "A Privacy-Preserving Logistic Regression-Based Diagnosis Scheme for Digital Healthcare," *Future Generation Computer Systems*, vol. 144, pp. 63-73, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Koren, "*System Model for Integration of Wearable Smart Device Data into a Central Health Information System*," Ph.D. dissertation, University of Zagreb, Faculty of Electrical Engineering and Computing, Department of Electrical Engineering Fundamentals and Measurements, 2023. [Google Scholar] [Publisher Link]

[15] Fadel Yessoufou, and Jinsong Zhu, "Classification and Regression-Based Convolutional Neural Network and Long Short-Term Memory Configuration for Bridge Damage Identification Using Long-Term Monitoring Vibration Data," *Structural Health Monitoring*, vol. 22, no. 6, pp. 4027-4054, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Qurban A. Memon, Mahmoud Al Ahmad, and Michael Pecht, "Quantum Computing: Navigating the Future of Computation, Challenges, and Technological Breakthroughs," *Quantum Reports*, vol. 6, no. 4, pp. 627-663, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] M. Karthikeyan, D. Manimegalai, and Karthikeyan RajaGopal, "Firefly Algorithm-Based WSN-IoT Security Enhancement with Machine Learning for Intrusion Detection," *Scientific Reports*, vol. 14, no. 1, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Saida Hafsa Rafique et al., "Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection, Current Research Trends," *Sensors*, vol. 24, no. 6, pp. 1-32, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mengjie Zhao, and Olga Fink, "DyEdgeGAT: Dynamic Edge via Graph Attention for Early Fault Detection in IIoT Systems," *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 22950-22965, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jie Shen "FedLED: Label-Free Equipment Fault Diagnosis with Vertical Federated Transfer Learning," *IEEE Transactions on Instrumentation and Measurement*, vol. 73, pp. 1-10, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Muhammad Yousuf et al., "IoT-based Health Monitoring and Fault Detection of Industrial AC Induction Motor for Efficient Predictive Maintenance," *Measurement and Control*, vol. 57, no. 8, pp. 1146-1160, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Pravindra Shekhar Shakunt, and Siba K. Udgata, "Machine Learning-Based Fault Detection Scheme for IoT-Enabled WSNs," *International Journal of Sensor Networks*, vol. 46, no. 2, pp. 61-72, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Edwin Omol et al., "Anomaly Detection in IoT Sensor Data using Machine Learning Techniques for Predictive Maintenance in Smart Grids," *International Journal of Science, Technology & Management*, vol. 5, no. 1, pp. 201-210, 2024. [Google Scholar]

[24] Jiuling Dong et al., "Real-Time Fault Detection for IIoT Facilities using GA-Att-LSTM Based on Edge-Cloud Collaboration," *Frontiers in Neurorobotics*, vol. 18, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Arash Heidari et al., "Assessment of Reliability and Availability of Wireless Sensor Networks in Industrial Applications by Considering Permanent Faults," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 27, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]