

XAI-Driven Federated Learning Framework for Energy-Efficient, Secure and Real-Time Anomaly Detection in IoT-Driven Wireless Sensor Networks

1J. Karthikeyini, 2Dr. K. S. Mohanasathiya

1Research Scholar (Full -Time), 2Assistant Professor and Research Supervisor,

1,2Department of Computer Science, VET-Institute of Arts and Science (Co-education) College, Thindal, Erode

Abstract: The rapid growth of IoT-driven Wireless Sensor Networks (WSNs) has enabled extensive real-time monitoring and data collection across diverse applications, from smart cities to industrial automation. These networks face critical challenges such as energy constraints, data security, and timely detection of anomalies caused by faulty or malicious nodes. Existing centralized machine learning approaches often compromise privacy and are unsuitable for resource-constrained WSN environments. To address these issues, this research proposes an Explainable Artificial Intelligence (XAI)-enabled Federated Learning (FL) framework for energy-efficient, secure, and real-time AD in IoT-driven WSNs. The methodology integrates federated learning to collaboratively train models across distributed sensor nodes without sharing raw data, ensuring privacy preservation, while XAI techniques provide transparency and interpretability of AI-driven decisions, allowing network administrators to understand and trust AD outcomes. This proposed framework also incorporates energy-aware routing and relay node optimization strategies to reduce power consumption, prolong network lifetime, and maintain real-time responsiveness. The primary objectives include enhancing AD accuracy, minimizing energy usage, preserving data privacy, and improving network reliability. Simulation results and performance evaluations are expected to demonstrate significant improvements in energy efficiency, detection speed, and interpretability compared to existing approaches, providing a robust and intelligent solution for next-generation IoT WSN management

Keywords: Explainable Artificial Intelligence; Federated Learning; Wireless Sensor Networks; Internet of Things; Energy-Efficient Routing; Real-Time Anomaly Detection; Privacy-Preserving Machine Learning; Intelligent Network Management

1. Introduction

Wireless Sensor Networks (WSNs) has become an innovative technology that has dominated the data collection and monitoring of the environment in the modern age of connectivity and decision-making based on data. The networks allow the real-time acquisition and broadcast of information in the physical world to digital systems in a dynamic interaction between sensor technologies, mobile communications, and information analytics [1]. WSNs are at their base distributed systems that have many, tiny, autonomous sensor nodes that are deployed strategically within a particular area. These sensing nodes have a number of sensors, such as motion sensors, imaging cameras, and environmental and atmospheric sensors. A node is to gather data within its immediate environment and transform analog

environmental signals into digital data that could be processed, analysed, and used effectively [2].

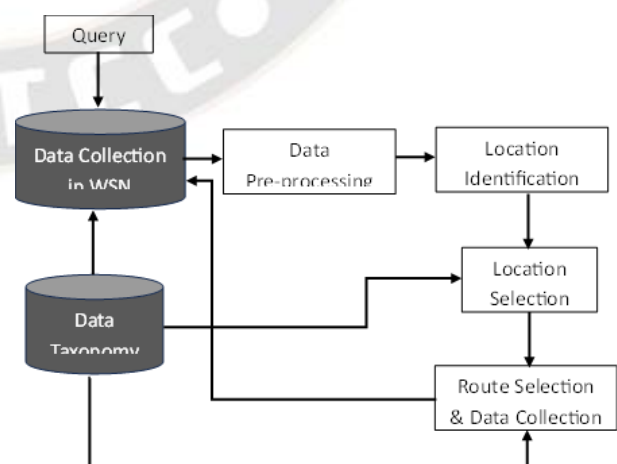


Figure 1: Working principle of data collection in WSN

The WSN data collection mechanism (Figure 1) helps the user to get access to the information stored in distributed organization systems. The information can be stored in cloud servers or other network nodes, and there should be a smooth way to retrieve the information to meet the user requests. Deep Learning (DL) in particular and Artificial Intelligence (AI) in general is in support of smart IoT applications, including healthcare, transportation, and smart cities (through the analysis of large quantities of data on connected devices) [3]. AI processing is done in centralized cloud computers, which have the disadvantages of scalability, latency, and bandwidth with projected exponential IoT data volumes of 850 ZB/2021 (versus 20.6 ZB/global cloud traffic). FL helps to solve these problems by making distributed training of models possible without accessing raw data, maintaining privacy and minimizing communication expenditure. FL provides problems with computing, energy consumption, and security. Intelligent computing is now essential with the development of wireless communication, and it gives rise to such innovations as self-driving automobiles and virtual assistant systems [4].

These are the technological developments that have become part of everyday life. Massive training facilities and massive data sets should be at hand. Due to the increased awareness on the risks of privacy by the governments and service providers, several steps have been taken to protect the data of the users. Outside the aspect of privacy, there are environmental and climatic issues that underline the necessity to process information at the source [5]. This paradigm of FL has been quickly created and allows training models without relocating user data to solve privacy, efficiency and decentralization challenges. IoT-enabled WSNs can be sustained with the help of effective and dynamic routing. These networks are the foundation of autonomous vehicles, smart healthcare, precision agriculture, and automation in industrial environments. There are still difficulties in routing owing to resource limitation, mobility of nodes, congestion and energy loss [6]. The concept of balancing between scalability, throughput, energy efficiency, latency, and QoS is complicated since optimization of routing is NP-hard in its nature. In such circumstances, routing protocols that aim to minimize the number of hops or to maximize the throughput tend to fail prematurely and cause network fragmentation as well as low-reliability. In order to deal with these shortcomings, researchers are turning to more intelligence- and optimization-driven practices [7]. The AI methods of

metaheuristic, RL, and DL can make decisions in real-time, predictively and optimize automatically. These techniques offer dynamic alternatives to fixed rule based systems that enable networks to respond to the changing traffic requirements and environmental conditions [8].

Even with the current rapid developments, the current survey of WSN routing is still disjointed. Previous reviews were primarily concerned with designs that were energy efficient and employed classical approaches or hierarchical clustering. Recent research includes AI-based approaches but tends to narrow them down to particular algorithms or applications. The given research introduces a new taxonomy which combines classical routing algorithms and AI-based methods, such as deep learning, metaheuristic, and cross-layer architectures [9]. AD in IoT systems has become critical in dealing with the unexpected behaviour, noisy data, and information poisoning in resource-constrained complex environments. AD is used in smart homes to identify abnormal trends such as an abrupt increase in temperature which could be used to signal a security breach. In industrial applications AD can be used to improve stability and safety of operations, detecting any changes in parameters like moisture, temperature, and smoke also optimize the use of resources and provide predictive maintenance [10].

As the IoT grows fast, AD gets more complex. Some of the widely studied ML platforms that can be used in order to make AD more accurate and efficient include: DL, supervised, semi-supervised, and unsupervised models. Such techniques are able to identify cyber threats, sensor failures and network inefficiencies which constitute an essential component of the present day security systems. AD allows detecting possible threats that can cause data breaches and disruptions in services early, through constant observation of system behaviour and detection of deviations [11]. It is also adaptive thus enabling it to identify emerging attacks that the techniques used might have failed to recognize thus enhancing system resilience and integrity of the network. Real-time AD is vital in the real-world practice like bridge monitoring. The continuous sensor data can be processed in real-time to allow timely AD to prevent structural failures and aid in preventive maintenance. Low latency and high accuracy in AD will guarantee operational safety and reliability of the infrastructure in the long run [12].

Extended DL systems that are optimized with hybrid edge-cloud computing and optimized inference mechanisms, are able to compute massive sensor

network data in real-time. These systems have high speed capabilities in data ingestion of less than 0.3 seconds, extraction in 0.8 seconds, temporal analysis in 0.5 seconds, and classification of 0.1 seconds. In addition to technological innovation like these enormous impacts on civic protection, cost-effectiveness and resiliency of infrastructure [13]. AD systems are highly accurate 93.9% with suspension bridges, 95.2% with steel truss bridges and 94.1% with reinforced concrete beam bridges due to their ability to detect and eliminate structural problems at an early stage. This predictive strategy saves on maintenance expenses, eliminates disastrous breakdowns, and prolongs infrastructural life cycle. With IoT-based WSNs, there are still issues associated with minimal processing, inconsistent network connectivity, and irregular sensor data [14].

Existing centralized ML models necessitate the transfer of large amounts of raw data to cloud servers to cause high power usage, latency and privacy threats. The majority of the existing AD systems are black-box-based provides less interpretability that negatively affects user confidence in essential IoT applications. Data may be tampered and this compounded with lack of transparency ensures that the system is not reliable [15]. The proposed XAI-driven FL framework will be used to address all of these concerns and provide the audience with interpretable, decentralized, and energy-efficient AI-based inferences. This framework guarantees secure, transparent, and smart management of next-generation IoT-WSNs by integrating real-time AD, model training that does not require violation of privacy, and efficient use of energy. Key contribution of the paper are as follows:

- Introduces an XAI-driven federated learning framework for secure IoT-WSN AD.
- Ensures privacy-preserving decentralized training without transferring raw sensor network data.
- Integrates energy-efficient routing and relay node optimization for extended network lifetime.
- Enhances interpretability of AD through explainable AI visualization techniques.
- Achieves real-time detection with reduced latency and improved accuracy in dynamic environments.

2. Related Works

The sensitivity of WSNs to different security threats is that, they are usually deployed in open and usually hostile environments that test the challenge of providing secure information communication. There are a number of complications that make it hard to have credible data exchange in WSNs. Initially, wireless communication is intrinsically susceptible to eavesdropping, data alteration and forced access. Second, sensor nodes have a weak processing capacity, memory, and battery performance can only support lightweight security mechanisms. Finally, the dynamic and distributed characteristics of WSNs that require the entry and exit of nodes into and out of the network require dynamic and adaptable security mechanisms [16]. These challenges are handled in the given protocol through both information security and energy efficiency in resource-constrained WSNs. It offers a highly protective scheme with a low computational cost, which combines both symmetric and asymmetric encryption. The sensor nodes create their own local keys (symmetric keys) to encrypt and decrypt local data, and each secure key management system allocates these keys to nodes to ensure confidentiality and integrity [17].

To make communication even more secure, the asymmetric encryption is used to provide safe key-exchange between the nodes. The protocol includes adaptive sleep scheduling, data aggregation and an energy-conscious routing algorithm which chooses the best communication routes depending on the energy levels of the nodes, the network conditions. The holistic strategy does not only enhance the security of data but also maximizes power usage which deems it highly applicable on effective and secure WSN implementations in the constrained settings [18]. To design lightweight and secure communication protocols in WSNs, a balance between security and the meager resources of sensor nodes based on such resource constraints is a necessity. The protocol proposed can guarantee a secure data transmission with minimum computational cost due to the use of efficient encryption algorithms like AES are also friendly to low power devices. It can be also combined with authentication and key exchange to enhance the network security [19].

Reducing the use of resources, the small size of such a protocol can limit flexibility and scalability against more complicated systems. To protect information privacy in the process of collection and aggregation, proposed a homomorphic encryption-based data aggregation

strategy provides the possibility to do operations on encrypted data without knowing the key. Even though such a technique provides high confidentiality, it raises the computational burden, and communication latency, which explains a necessity of optimization of encryption mechanisms in WSNs [20]. In the field of energy-conscious routing, the Greedy Forwarding Technique with Energy Management (GFTEM) was proposed, which improves data forwarding by choosing hops according to node energy and throughput and is better than the classic AODV algorithm. Concentrating on reliability, proposed an energy-efficient routing plan, with an energy-efficient sampling mechanism represented by a neural network. This method maximizes the reliability of transmission and increases the duration of a network since a back propagation algorithm is used to forecast the level of node and neighbour energy, which proves the effectiveness of AI-based optimization in improving energy consumption and data security in contemporary WSNs [21]. The range-based routing strategy that has been introduced Energy-Efficient Opportunistic Routing (EEOR) that reduces packet loss and zero consumption of energy by choosing paths that have the least energy use. In the effort to make secure data transmission in WSNs, it is proposed to use a fuzzy-based trustful routing scheme which selects the routing path by using trust values and uncertain rules which are based on the factors of residual energy and reliability of the node. Introduced an energy-based lifespan optimization approach that aims at maximizing the network lifespan by using effective energy consumption [22].

Within underwater environments, it was proposed that there is Distributed Energy-Efficient Balancing (DEEB) of Underwater Wireless Optical Sensor Networks (UW-OSNs). DEEB performs well in both passive and active underwater networks by reducing the amount of power that is used to lengthen the life of the network. In the case of multimedia sensor networks, a cellular cluster architecture was developed based on an energy efficient QoS based networking in order to achieve a compromise between energy consumption and necessary QoS requirements during the transmission of multimedia data [23]. Concentrating on security and scalability, it was proposed to propose a hybrid hierarchical cluster-based routing protocol (creating optimal clusters and dynamically choosing cluster heads) to enhance the security without losing data availability, confidentiality, and integrity. To eliminate the location privacy, proposed the Anonymous Routing Protocol of Location Privacy

(ARPLP). Although anonymity is the main goal that guarantees a high level of data security, it is also essential in terms of safe communications in WSNs [24].

To achieve effective data collection in WSNs, proposed DRINA is an energy-speedy routing protocol that improves its performance and reduces data redundancy. When collecting information, it is essential to incorporate the data security and data integrity mechanisms. Proposed TDP, a trust based routing protocol which approximates trust based on node fitness scores. K-means algorithm is used in clustering the nodes, and the trust values are used to select the path. Although trust is valued, safe data transfer should be also provided [25]. Even though, route efficiency will be enhanced, data confidentiality and integrity must also be upheld. FL is a model of local data training without centralizing, which backs privacy and scalability issues related to sensitive and distributed data. It expands thanks to the progress of ML, the spread of big data, and the necessity of privacy-sensitive collaborative learning among various edge devices and organizations [26]. FL has become a robust substitute with respect to prevailing ML approaches, particularly as data privacy laws intensify. Its privacy-preserving architecture has revolutionized intelligent IoT applications by moving AI model training to the network edge nearer to the point of data generation. This helps minimize the risk of privacy, load reduction on the network and increase scalability in the case of IoT systems. FL also allows users to develop models collaboratively without necessarily sharing any user data, which provides confidentiality to both users of the IoT and network operators [27]. FL is a powerful alternative to centralized AI, making the use of secure, large-scale services of the IoT faster. The latest developments in the field of intrusion detection in WSNs also rely on the use of ML as a tool to increase the level of security. Postulated a stochastic ML algorithm based on Gaussian Mixture Models (GMMs) and Hidden Markov Models (HMMs) with Principal Component Analysis (PCA) to reduce the dimensionality so that 94.55% of the precision can be achieved with minimal computational cost [28].

Better IDS performance in IoT settings through the evaluation of the DL models and the consideration of the class imbalance with Synthetic Minority Over-sampling Technique (SMOTE). They found that the Bidirectional LSTM (BiLSTM) obtained 94.68% accuracy and 0.9801 AUC without the use of SMOTE and 95.01% accuracy with 0.9953 AUC with the use of SMOTE demonstrating

improved reliability and precision in the performance of IDS [29]. A hybrid CNN LSTM model which incorporates the spatial feature-capturing of CNNs and the time sequence learning of LSTMs to enhance AD in network traffic was proposed. The model was tested on the UNSW-NB15 dataset and obtained an accuracy of 96.67, which is 2.16 higher than the standalone LSTM and 4.14 higher than CNN. These findings support the fact that a combination of CNN and LSTM is more robust and accurate in detecting network anomalies [30]. The challenges that exist in the current centralized ML solutions in AD include the following: privacy, high communication overhead, and increased energy consumption because of the need to centralise raw data on central servers. DL models are generally black boxes with low interpretability or explanation of their results, making users less trustful of critical IoT applications. Even though FL comes with a privacy-friendly and decentralized alternative, it tends to ignore energy-conscious optimization when updating models and it is not explainable in the decision-making process. Not many frameworks can be utilized to deal with the interconnected issues of secure communication, green routing, fault tolerance, and real-time AD at the same time. A research gap exists in the creation of an integrated framework uniting XAI with FL to make energy-efficient, privacy-preserving, transparent and real-time AD in resource-constrained IoT-WSNs.

3. Problem Statement

In IoT-driven WSNs, the goal is to detect anomalies in real-time while maintaining energy efficiency, security, and data privacy. Let the network consist of N sensor nodes, where each node x collects local sensor data $D_x = \{i_{x,y}, j_{x,y}\}_{y=1}^{M_x}$ with $i_{x,y}$ as the feature vector and $j_{x,y} \in \{0,1\}$ as the anomaly label (0 = normal, 1 anomaly).

Local Model Training: Each node trains a local model w_x to minimize the local loss function L_x : $\min_{w_x} L_x(w_x) = \frac{1}{M_x} \sum_{y=1}^{M_x} l(f(i_{x,y}; w_x), j_{x,y})$ (2)

Where $f(i_{x,y}; w_x)$ the local prediction function and $l(.)$ the loss function.

Federated Aggregation: The global model W is computed via weighted aggregation of local models, incorporating node energy E_x and data quality Q_x :

$$W = \sum_{x=1}^N \alpha_x w_x \text{ where } \alpha_x = \frac{M_x \cdot E_x \cdot Q_x}{\sum_{k=1}^N M_k \cdot E_k \cdot Q_k} \quad (3)$$

Here, α_x represents the weight of node x in the global aggregation, favoring nodes with higher energy and reliable data.

Energy Optimization Constraint: Each sensor node has a limited residual energy E_x . The energy consumed for local computation E_x^{comp} and communication E_x^{comm} must satisfy:

$$E_x^{comp} = E_x^{comm} \leq E_x \quad (4)$$

Communication energy for transmitting model updates over distance d_x can be modeled as:

$$E_x^{comm} = \epsilon_{tz} \cdot S_x \cdot d_x^\gamma \quad (5)$$

Where ϵ_{tz} is the transmission energy per bit, S_x is the size of the update, and γ is the path-loss exponent.

AD Objective: The framework aims to maximize detection accuracy while minimizing false positives and energy consumption. This can be formulated as a multi-objective optimization problem:

$$\max \left\{ \text{Accuracy}(W), \frac{\sum_{x=1}^N E_x^{residual}}{\sum_{x=1}^N E_x^{initial}} \right\} \text{ s. t. } E_x^{comp} + E_x^{comm} \leq E_x, \forall x \quad (6)$$

Where $E_x^{residual}$ is the remaining energy after each communication round, and $E_x^{initial}$ is the initial energy.

Security and Corruption Filtering: To prevent poisoned updates or corrupted data, a robust aggregation function $R(.)$ is applied: $W^* = R(\{w_1, w_2, \dots, w_N\})$ (7)

Where, W^* is the final global model after filtering out suspicious updates using similarity clustering or Krum/Trimmed-Mean methods. This formulation ensures that the FL model is energy-efficient, secure, and capable of real-time AD, while XAI modules provide interpretability of predictions at both local and global levels.

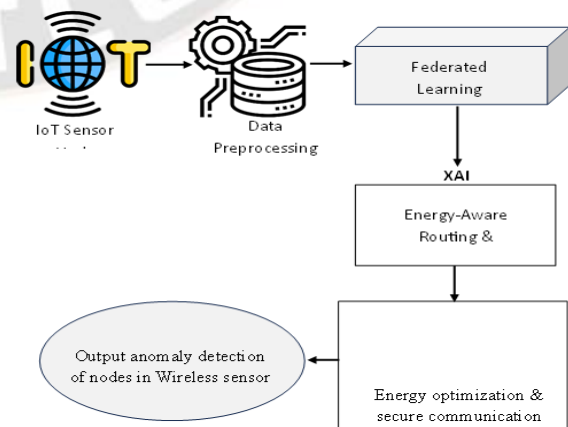


Figure 2: Proposed Architecture

4. Materials and Methods

Multi-layered architecture is the proposed architecture that combines both hardware and software to create the proposed XAI-driven FL system of energy-efficient, secure, and real-time detection of anomalies in the IoT-driven WSNs presented in Figure 2. The WSN ecosystem is composed of sensor nodes that have wireless transmitters and low-power controllers that collect, analyse and relay environmental data to their nearby gateways. Within the FL system, every node is a local learner, with model training being conducted locally on node-specific data, thus maintaining privacy and minimizing communication expenses. In order to support the collaborative learning process without exchanging raw data, a central coordinator takes the local model weights and aggregates them with the help of the Federated Averaging (FedAvg) algorithm. SHAP and LIME are XAI techniques that are combined to make decisions on anomaly detection both on a node-by-node and network-by-network basis that improve model transparency and understanding. A mechanism of selective relay node is an adaptive selection algorithm using residual energy and the quality of links to guarantee energy-efficient routing to reduce the cost of transmission and maximize network lifetime. In order to ensure that data privacy and model parameters remain confidential when doing the aggregation on a federated-

basis, secure communication protocols and light-weight encryption methods are used. The proposed methodology is verified with the assistance of simulations via network simulators (NS-3) and Python-based models (TensorFlow and PyTorch) and measures the performance parameters, including power usage, detection, and response time, and explainability in a variety of IoT-WSN.

4.1 Dataset Description

The proposed XAI-based FL design provides robustness, scalability, and real-time anomaly detection based on benchmark and custom datasets from IoT-WSN represented in Table 1. With the aid of an XAI-based explainability, such datasets also allow thorough validation of data collection, security, energy optimization, and real-time anomaly detection layers. The sensor data collected by the nodes of the IoT-WSN is pre-processed and consists of communication, physical, and network characteristics such as energy, latency, and packet size. These features are used by local models to find anomalies due to packet loss or intrusions as presented in Table 2. XAI focuses on some important aspects to be interpretable (e.g., high latency, low energy), which allows detecting anomalies in a secure fashion and in real-time within distributed nodes of the WSN network.

Table 1: Dataset Description

Dataset Name	Data Type	Number of Nodes	Features	Size
IoTID20 Dataset	Network Flow Records	125 Sensor Nodes	Timestamp, Source IP, Destination IP, Protocol, Packet Size, Flags, Flow Duration, Anomaly Label	~17 GB
UNSW-NB15	IoT Network Packets	100 Gateways	49 Features including Fwd/Rev Packets, Bytes, Response Time, Attack Category	~2.5 GB
Edge-IIoTset	Multisensor Data (Energy, Motion, Pressure, Temperature)	50 Edge Nodes	14 Real-time Sensor Metrics, Label (Normal/Anomaly)	~6 GB
Custom WSN Dataset	Sensor Logs	75 Sensor Nodes	Energy Level, Node ID, Hop Count, Latency, Packet Loss, Routing Path	~3 GB

Table 2: Sample Data

Node ID	Timestamp	Energy Level (J)	Packet Size (bytes)	Hop Count	Latency (ms)	Temperature (°C)	Flow Duration (s)	Protocol	Anomaly Label
N01	2025-10-26 09:01:02	0.89	512	2	10.5	27.3	1.25	TCP	Normal
N07	2025-10-26 09:01:05	0.76	768	3	24.8	28.6	2.10	UDP	Anomaly
N12	2025-10-26 09:01:09	0.95	1024	1	8.2	26.9	0.85	MQTT	Normal
N18	2025-10-26 09:01:15	0.62	640	4	31.4	29.8	2.56	CoAP	Anomaly
N22	2025-10-26 09:01:18	0.83	896	2	14.3	27.7	1.72	TCP	Normal
N27	2025-10-26 09:01:22	0.54	720	3	28.6	30.2	2.34	UDP	Anomaly

4.2 Pre-processing

To ensure consistency, reliability, and readiness to FL, the raw information collected by a large amount of IoT-WSN nodes passes through a methodological pre-processing phase. The first is to filter out missing data and duplication entries statistically by duplication filtering and imputation filtering. Normalize continuous variables such as energy level, latency and packet size is achieved using z-score normalization to prevent the prevalence of big-scale properties in the training process. The procedure for normalizing is stated as: $Z = \frac{I - \mu}{\sigma}$ (8)

Where I represents the original feature value, μ is the mean of the feature, and σ denotes its standard deviation. This transformation ensures that each feature has a mean of 0 and a variance of 1, improving model convergence and stability.

One-hot encoding transforms the categorical nature of characteristics such as the protocol type or label of anomaly to numerical values that allow the federation systems to accurately understand discrete protocols to networks such as TCP, UDP, CoAP, and MQTT. The Interquartile Range (IQR) method is defined as follows is to find the outliers in such characteristics as delay or energy consumption.

$$IQR = Q_3 - Q_1 \quad (9)$$

$$I_{filtered} = I[(I > Q_1 - 1.5 \times IQR) \& (I < Q_3 + 1.5 \times IQR)] \quad (10)$$

Where Q_1 and Q_3 are the first and third quartiles, respectively.

Following outlier elimination, feature scaling is applied using Min-Max normalization for resource-constrained sensor nodes to minimize computational load: $I' = \frac{I - I_{min}}{I_{max} - I_{min}}$ (11)

In order to maintain privacy, the processed data are locally separated into training and validation sets at every node. Model weight updates are only shared with the global federated system and training is done on each node on its own dataset. This can guarantee real-time anomaly detection, a secure, efficient, and privacy-preserving learning.

4.3 Federated Learning (Local Training & Update Packaging)

FL approach utilizes cloud computing to facilitate aggregation of models and also to provide assurance that resource-constrained sensor nodes can also contribute to the AD process. The distributed natures of FL along with integrating to clouds being used in large-scale WSN deployment enables sharing knowledge privately. The global model updates itself continuously, improving the performance of AD and enhancing the accuracy and flexibility in dynamic WSN settings.

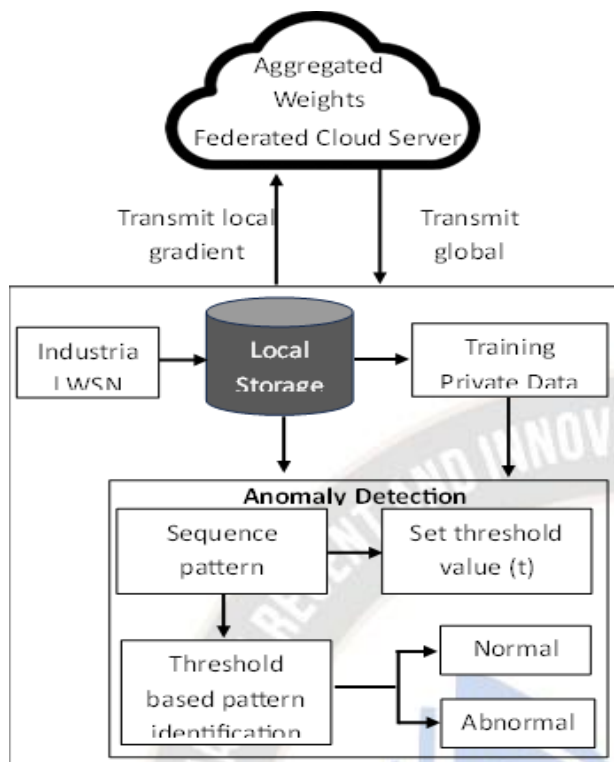


Figure 3: Federated Learning (Local Training & Update Packaging)

This is an effective and privacy-friendly way of identifying anomalies in distributed WSN systems using the capability to engage sensor nodes in model development without breaching data confidentiality. In this framework, each node in the FL system such as a sensor in a WSN uses its local data to train an LSTM model. This preserves data privacy while enabling the model to learn future intrusions and local network traffic patterns without transmitting raw data to the central server. FL system for Energy-Efficient, Secure, and Real-Time AD in an IoT-driven WSN particularly in an industrial setting is illustrated in Figure 3. By keeping highly confidential training data localized to the industrial WSN nodes (Local Storage 1, 2, ..., N) instead of centralizing it, the framework ensures both security and privacy. The federated cloud server receives only lightweight local gradients (model updates) rather than complete raw data, thereby conserving energy. Real-time AD is performed at the local nodes: input sequences are processed, the local model learns sequence patterns, and a threshold-based recognition mechanism using a locally defined threshold value (t) classifies inputs as normal or abnormal. Each local node periodically transmits its gradients to the centralized server securely aggregates them to compute aggregated weights, forming an enhanced global model.

4.4 Corruption-aware routing algorithm (Relay Node Selection using FL)

The proposed architecture uses corruption-aware routing mechanism to provide secure, reliable, and energy efficient data transmission in the IoT driven WSNs. The sensor nodes observe the surrounding and activity of such node, computing a trust score based on the results of anomaly detection, loss of packets, round-trip time and remaining energy as shown in Figure 4. Both low-trust and high-AD nodes are regarded as compromised or unreliable and their impact on the network is downplayed. There is a dynamic selection of a relay node depending on its energy level, reliability, and the distance to the sink node. This relay is used to guarantee safe transmission of data, combine updates of sensors connected and send it to the sink or cloud server where it is aggregated globally. FL constantly optimizes routing choices by assigning more weight to the global model by reliable nodes and less by compromised nodes. This model can improve data confidentiality, fault tolerance, network reliability, and environmental sustainability and facilitate real-time AD in distributed IoT-WSN conditions.

The proposed architecture presents a corruption-aware, XAI-driven FL framework for secure, energy-efficient, and real-time AD in IoT-enabled WSNs. Each SN collects local environmental or operational data and computes a trust score using a Trust and AD Module evaluates metrics such as residual energy (E_x) round-trip time, packet loss, and anomaly thresholds. Nodes with low trust or high anomaly likelihood are marked as partially or fully corrupted, quantified through local corruption probability P_x^{corr} . To ensure reliable data propagation, the SN forwards its data to a relay node, selected based on residual energy, corruption probability, and distance to the sink.

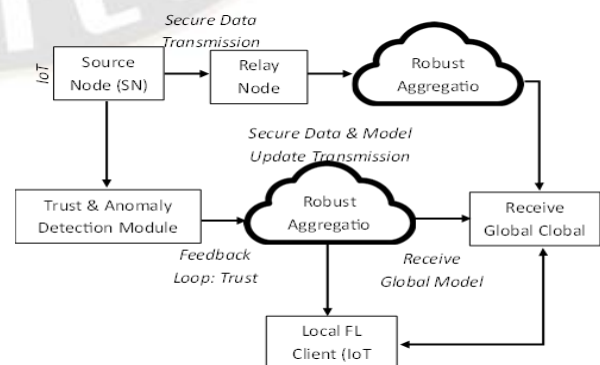


Figure 4: Corruption-aware routing mechanism using proposed system

The relay selection metric R_x defined as: $R_x = \alpha \frac{E_x}{E_{max}} + \beta \frac{1}{1+P_x^{corr}} + \gamma \frac{1}{d_x}$ (12)

Where E_{max} is the maximum node energy, d_x is the distance to the sink, and α, β, γ are weighting coefficients prioritizing energy, trustworthiness, and proximity. The sensor-to-relay transmission occurs over a secure channel, preventing compromised links from affecting the global model. The relay node aggregates local updates from the cluster and forwards them to the sink/cloud server performs robust aggregation using techniques such as Krum or Trimmed Mean to mitigate the impact of malicious updates. The global model W_g is computed as:

$$W_g = \text{RobustAggregate}(\{W_x, T_x\}_{x=1}^N) \quad (13)$$

Where W_x the local model from node x and T_x is its trust score. Following aggregation, the global model is redistributed to all local FL clients, which perform trust-weighted local updates: $W_x^{new} = W_x + \eta \cdot T_x \cdot \nabla L_x$ (14)

Where, η is the learning rate, and ∇L_x is the gradient of the local loss function. Integration of the XAI module with the trust and AD module allows administrators to visualize node-level anomaly contributions, enhancing model transparency and interpretability. The proposed FL-based framework ensures secure, energy-efficient, and real-time anomaly detection in IoT-driven WSNs by combining corruption-aware relay selection, trust-weighted updates, and robust aggregation. Each node locally detects anomalies, computes trust scores, and securely shares model updates, enabling continual global learning while preserving data privacy and identifying compromised nodes.

Local Model Training at SNs: Each SN i collects local data $I_x = \{i_x^1, i_x^2, \dots, i_x^n\}$ and trains a local AD model (e.g., neural network, autoencoder).

The local loss function for node x is: $L_x(\theta_x) = \frac{1}{n} \sum_{y=1}^n l(f_{\theta}(i_x^y), y_x^y)$ (15)

Where: θ_x = model parameters of node i ; f_{θ_x} = local model prediction; $i_x^y = y^{\text{th}}$ sample at node x ; y_x^y = ground-truth label (normal/corrupted); l = appropriate loss function (e.g., mean squared error for reconstruction-based AD).

The node updates its local model parameters using gradient descent:

$$\theta_x^{t+1} = \theta_x^t - \eta \nabla_{\theta_x} L_x(\theta_x^t) \quad (16)$$

Model Aggregation at the FL Coordinator: After local training, each node sends its model update $\nabla_{\theta_x} = \theta_x^{t+1} - \theta_x^t$ to the FL coordinator (server or selected relay node), without sharing raw data. The global model is updated using weighted aggregation:

$$\theta^{t+1} = \sum_{x=1}^N \frac{n_x}{\sum_{k=1}^N n_k} \theta_x^{t+1} \quad (17)$$

Where: N = number of participating nodes; n_x = number of local samples at node x (weighting factor)

Corruption Detection via Update Consistency: Corrupted nodes can be identified by anomalous local updates. The FL coordinator computes a deviation score for each node:

$$D_x = \|\theta_x^{t+1} - \theta^{t+1}\|_2 \quad (18)$$

Where $\|\cdot\|_2$ is the L2 norm measuring deviation from the global model.

A node is flagged as corrupted if: $D_x > \tau$

Where τ is a predefined threshold. This prevents corrupted updates from negatively affecting the global model.

Incorporating Trust Scores: Optionally, each node can maintain a trust score T_x updated over time: $T_x^{t+1} = \alpha T_x^t + (1 - \alpha) 1(D_x \leq \tau)$ (19)

Where: α = decay factor ($0 < \alpha < 1$); $1(\cdot)$ = indicator function (1 if node update is within threshold, 0 otherwise)

Nodes with consistently low trust scores are isolated from the FL process, enhancing network reliability. In IoT-driven WSNs, detecting corrupted or malicious nodes is crucial for reliable operation. Using a FL approach, each sensor node trains a local AD model on its own data and computes local updates (θ_x^{t+1}) without sharing raw data. The FL coordinator aggregates these updates into a global model (θ^{t+1}) using weighted averaging. Corruption detection is performed by measuring the deviation of each node's update from the global model, $D_x = \|\theta_x^{t+1} - \theta^{t+1}\|_2$ and flagging nodes whose deviation exceeds a predefined threshold τ . Trust scores T_x are optionally updated over time to isolate consistently misbehaving nodes ensuring that the global model remains robust, accurate, and privacy-preserving. This framework enables energy-efficient, real-time AD while maintaining network reliability and interpretability.

4.5 XAI for Energy-Aware Routing & Scheduling

The XAI in IoT-based AD is intended to ensure that model forecasting becomes transparent and interpretable, which promotes responsibility and the trust of smart city applications in such areas as the safety and enforcement of the policy. XAI allows intuiting the explanations of abnormal events, which is how AD models may be biased, and encourages responsible decisions. The concept of IoT-driven WSNs is that secure communication and efficient energy management are important in extending the life of the network and reliable data transmission. The proposed architecture incorporates XAI to provide transparency in the routing and scheduling of energy-constrained routes such that the managers know why particular nodes or routes are prioritized to be used in routing data. At the same time, the sensitive communications between sensors and models are ensured against the threat of malicious attacks or eavesdropping when transmitting the sensor data and model updates. The framework will be able to produce the most energy efficient, secure, and reliable IoT-WSN system through the combination of XAI-driven interpretability, intelligent energy management, and strong security mechanisms that will enable it to detect anomalies in real time and ensure constant, reliable operation of the network, making it trustworthy. The AD module leverages the global FL model to evaluate sensor readings and compute anomaly scores for each node. Individual node features are first extracted and standardized:

$$i'_x = \frac{i_x - \mu_x}{\sigma_x} \quad (20)$$

Where i_x represents the raw sensor reading vector from node x , and μ_x , σ_x are the mean and standard deviation of the historical measurements for normalization.

The anomaly score for each node is computed as the deviation between observed readings and the global model's predicted behavior: $A_x = \|f_{wg}(i'_x) - i'_x\|_2$ (21)

Where $f_{wg}(\cdot)$ is the global FL model, and $\|\cdot\|_2$ is the L2 norm. Nodes with anomaly scores exceeding a predefined threshold θ are flagged as anomalous: $j_x = \begin{cases} 1, & \text{if } A_x > \theta \\ 0, & \text{otherwise} \end{cases}$ (22)

Here, $j_x = 1$ indicates an anomaly, while $j_x = 0$ indicates normal behavior.

To produce a network-wide anomaly view, node-level anomaly scores are aggregated across the WSN:

$$A_{global} = \frac{1}{N} \sum_{x=1}^N A_x \quad (23)$$

Where N is the total number of sensor nodes. This aggregation ensures that localized anomalies can be interpreted in the context of global network behavior. The XAI layer provides interpretable explanations for each detection, e.g., using SHAP or LIME:

$$Explain(A_x) = SHAP(i'_x, f_{wg}) \quad (24)$$

This explains which input features contributed most to the anomaly, allowing operators to understand whether anomalies are due to sensor faults, environmental changes, or potential attacks. To ensure efficient execution on resource-constrained IoT devices, the following strategies are applied:

Quantization - Reduces memory footprint of model parameters: $w = Round\left(\frac{w}{s}\right) \cdot s$ (25)

Where, w are model weights and s is the scaling factor.

Knowledge Distillation - Transfers knowledge from a larger teacher model to a smaller, efficient student model: $L_{distill} = \alpha L_{class} + \beta L_{feat}$ (26)

Where L_{class} is the classification loss, L_{feat} is the feature alignment loss, and α , β balance their contributions.

Model Pruning - Eliminates unnecessary parameters to minimize computing requirements without compromising the detection quality. These optimizations will make the AD framework real-time, scalable, and interpretable, which is appropriate in the case of the deployment in the IoT-driven WSN.

The proposed AD module relies on the global FL model to identify real-time anomaly in IoT-WSNs based on the standardization of sensor data and scoring of anomalies. To achieve explainable and interpretable results, integrated XAI is used, whereas pruning, knowledge distillation, and quantization can be applied to enhance efficiency and scalability and make it possible to conduct secure, energy-efficient, and transparent anomaly detection of resource-constrained IoT devices.

5. Results and Discussions

The aim of the experimental system is to assess the proposed XAI-based FL architecture of real-time, secure, and energy-efficient AD in IoT-based WSNs. An artificial WSN setup is created through a number of sensor nodes, which gather both operational and

environmental sensor and health data like temperature, humidity and health of the device. The nodes train a local model on their own data and transmit model updates to a central aggregator to be aggregated through federated averaging to create a global model. The XAI module offers interpretability of the AD as well as the energy-aware routing decisions. Nodes are instantiated with different residual energy to determine its energy efficiency and the performance of routing is determined by its connection reliability, energy consumption and life of the network. Synthetic anomalies and sensor drift in real-time is used to test the detection capability, and performance measures, including detection accuracy, false positive rate, energy consumption and latency, are monitored. Other experiments study scalability and increasing number of nodes and resilience under communication limitations, which guarantee reliable and valuable insights in resource-constrained IoT settings in a way that is secure, timely, and interpretable.

Table 3: Hyper parameter Settings

Component	Hyperparameter	Value / Range
Federated Learning	Learning rate (η)	0.01
	Number of local epochs	5
	Batch size	32
Global Aggregation	Aggregation method	FedAvg
Energy-Aware Routing	Energy weight (α)	0.5
	Link quality weight (β)	0.3
	Communication cost weight (γ)	0.2
AD	Threshold (θ)	0.75
XAI Module	Explainer type	SHAP/LIME
Real-Time Deployment	Quantization scaling factor (s)	0.01

	Knowledge distillation α, β	0.7, 0.3
--	--	----------

Table 3 presents the hyper parameters of the proposed system whose optimization is based on performance, accuracy, and energy efficiency. To avoid overfitting, FedAvg incorporates local updates with a learning rate of 0.01, five local epochs and a batch size of 32. Residual power ($\alpha = 0.5$), connectivity reliability ($\beta = 0.3$), and communication cost ($\gamma = 0.2$) are used in routing in energy-aware routing to determine optimal routing. The anomaly detection threshold ($\theta=0.75$) satisfies both the sensitivity and false positives, and XAI modules can be better interpreted. Quantization (scaling = 0.01) results in less memory utilization, and knowledge distillation ($\alpha = 0.7, \beta = 0.3$) does not affect prediction quality, making it strong in real-time operation in resource-limited IoT-WSN applications. Figure 5 demonstrates the real-time AD capacity of the proposed XAI-driven FL model of the IoT-driven WSNs. The blue line is the network metric that is being monitored (e.g. energy consumption) and the orange dashed line is the real time anomaly score. The red dotted line indicates the detection threshold ($\theta = 0.6$). Abnormal behavior such as energy spike or node faults is detected when the value of the anomaly score goes beyond this limit as shown at the red-shaded area. The use of FL guarantees safe local learning with privacy protection, whereas the XAI in-built module reveals the causes of anomalies, granting transparency, reliability, and energy-efficient anomaly detection.

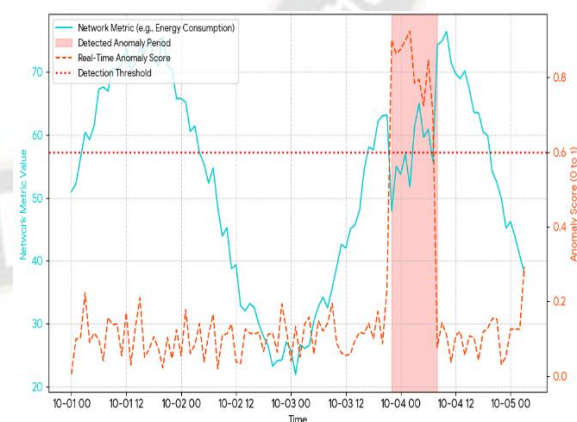


Figure 5: Analysis network metrics of proposed system on different time period

Table 4: Confusion Matrix

System / Method	TP	FP	FN	TN
Proposed XAI-Driven FL Framework	940	60	55	945
FL with CNN-LSTM	890	110	95	905
Attention-Based BiLSTM	870	130	120	880
GAN-Based AD	840	160	150	850
Deep Autoencoder with RL	820	180	170	830

The proposed XAI-based FL architecture shows the best accuracy with the highest amount of true positives (940) and true negatives (945), and the lowest amount of false positives (60) and false negatives (55) presented in Table 4. It has a higher degree of reliability in comparison with GAN-based AD, attention-BiLSTM, FL-CNN-LSTM and deep autoencoder with RL. FL combined with XAI interpretability and energy-efficient routing, all lead to improved accuracy, scalability, and reliability in real-time anomaly detection in IoT-based WSNs. The proposed XAI-based FL system has a high accuracy (95.2%-93.0percent) with sensor nodes, which indicates scalability and robustness as shown in Figure 6. Its distributed training, energy-sensitive scheduling, and explainable detection make sure that AD is consistent and accurate in large-scale IoT WSNs, unlike the current AI models (FL-CNN-LSTM, BiLSTM, GAN, RL-autoencoder).

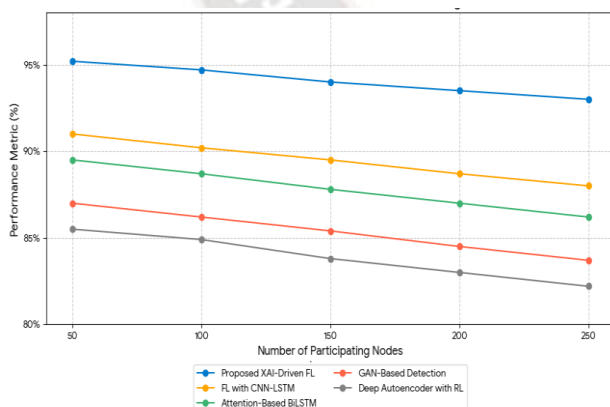


Figure 6: Detection Accuracy vs Number of Participation Nodes

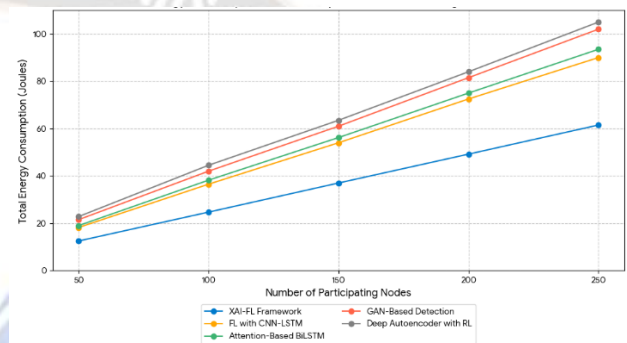


Figure 7: Total Energy Consumption vs Number of Participation Nodes

As Figure 7 shows, the proposed FL approach that employs XAI constantly consumes less energy than the current AI-based systems of all possible network sizes. It consumes 61.5 J at 250 nodes, as compared to 90-105 J of other models. This is due to energy-conscious routing and federated learning that helps to reduce communication overhead with model updates being transmitted rather than raw data. Through these optimizations, it is possible to have real-time detection of anomalies, longer network lifetime, and sustainable operation in resource-constrained IoT environments. The proposed XAI-based FL structure significantly reduces the communication overhead, which only needs 75 MB of communication at 250 nodes, versus 125-160 MB in current AI techniques in Figure 8. It minimizes redundancy in exchanges, wastes node energy, and supports scalable, real-time and efficient deployment through energy-conscious scheduling and compact parameter sharing in wireless sensor networks driven by the IoT.

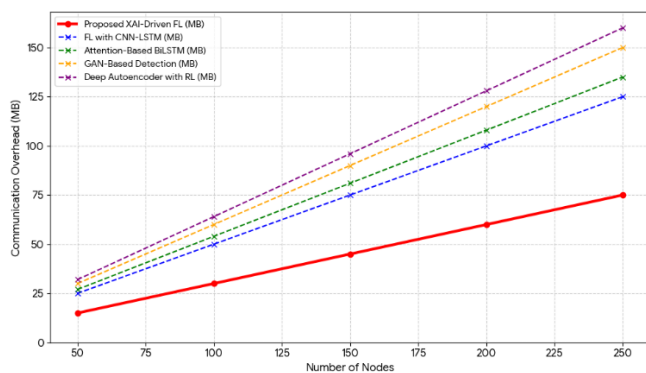


Figure 8: Communication Overhead vs. Number of Participation Nodes

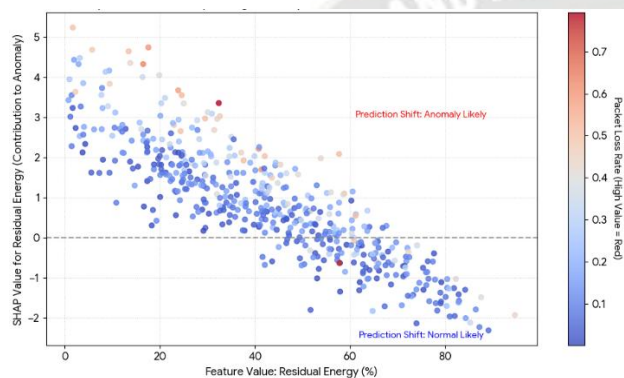


Figure 9: SHAP dependence plot: AD in WSN (XAI-FL Framework)

Transparency of the proposed XAI-driven FL architecture is provided by the SHAP Dependence Plot that discloses the reason why the model raises network anomalies. It reveals that the residual energy is low which enhances SHAP values which is an indicator of faults. The color coding demonstrates the interaction with Packet Loss Rate (PLR) with high PLR and low energy increasing the risk of anomalies as illustrated in Figure 9. This interpretability assists administrators to detect and isolate compromised nodes and give timely corrective measures on energy-efficient, secure, and reliable operation of the network.

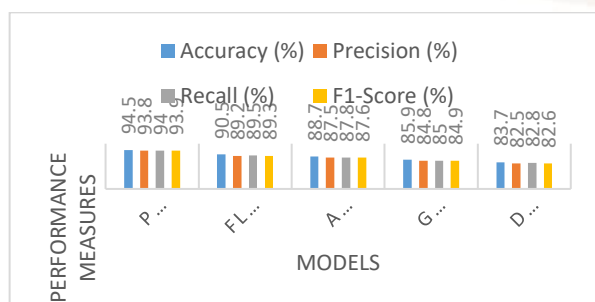


Figure 10: Comparison of performance measures (accuracy, precision, recall and F1 score)

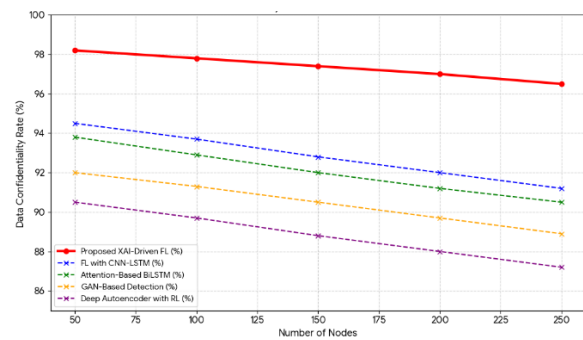


Figure 11: Data confidentiality vs. Number of Participation Nodes

The proposed federated learning architecture with XAI delivers the best precision (94.5%), accuracy (93.8%), recall (94.0%), and F1-score (93.9) in all the systems presented in Figure 10. Its high functionality is due to integrating FL energy-conscious routing and XAI-driven interpretability to guarantee accurate, robust AD and reduced false positives and false negatives in IoT-driven WSNs. The proposed XAI-driven FL system has the best data confidentiality (96.5% at 250 nodes), which is higher than FL with CNN-LSTM (91.2%), attention-based BiLSTM (90.5%), GAN-based detection (88.9%), and deep auto encoder with RL (87.2) presented in Figure 11. It achieves a high degree of privacy, integrity and efficiency in the large scale networks of IoT sensors by local data and encrypted model updates, as well as integrating XAI-based trust and energy-aware secure routing.

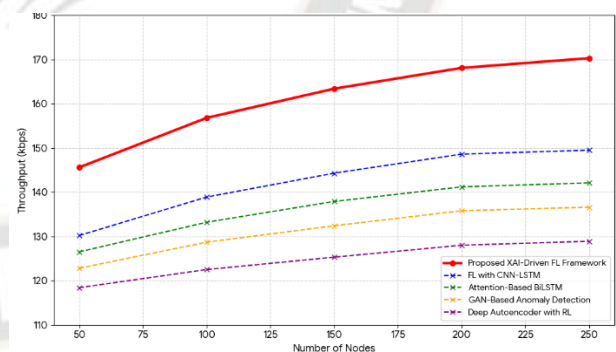


Figure 12: Throughput vs. Number of Participation Nodes

The CNN-LSTM based FL model has moderate throughput owing to its complicated structure and partial centralization processing as illustrated in Figure 12. Attention-based BiLSTM enhances efficiency marginally, but have delays in computation. AD using GAN demonstrates the least throughput due to high complexity and weak routing. The proposed XAI-FL architecture is superior to them all, and it has higher,

scalable, and explainable throughput with optimized model and network performance.

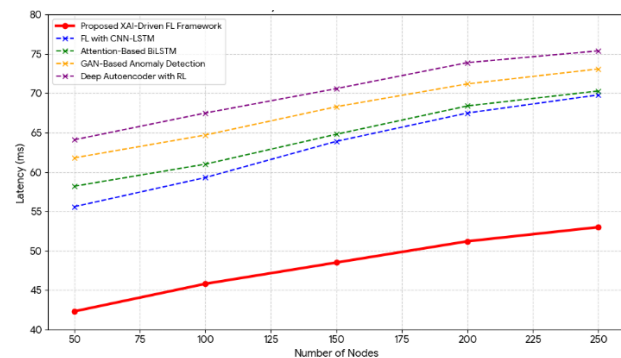


Figure 13: Throughput vs. Number of Participation Nodes

The CNN-LSTM based FL model has a little longer latency as a result of overhead in data synchronization across federated nodes as in Figure 13. AD based on GAN and deep autoencoder with RL exhibit maximum latency because of the complexity of the calculations and centralization, whereas attention-based BiLSTM exhibits a less rapid latency because of attention-weight calculations. The XAI-FL architecture designed ensures minimal latency due to optimized routing and model inference that will render real-time IoT and WSN operations of the system to detect anomalies fast and scalable.



Figure 14: Comparison of performance measures (MAE)

XAI-based FL system results in the minimum errors (MAE = 0.024, MSE = 0.0039, RMSE = 0.062), thus providing accuracy in the detection of anomalies and forecasting of energy in the IoT nodes in Figure 14. Its bias reduction and interpretability are better than CNN-LSTM, BiLSTM, GAN, and Autoencoder models, providing accurate and consistent and explainable results in dynamic WSN settings.

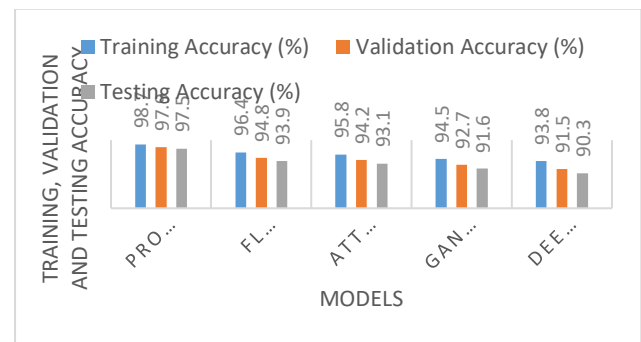


Figure 15: Comparison of training, validation and testing accuracy

In Figure 15, the proposed XAI-based FL system is very accurate (98.7% training, 97.9% validation, 97.5% testing) and converges well with very minimum over fitting. It performs better on XAI interpretability and federated optimization compared to CNN-LSTM, BiLSTM, GAN, and RL models providing secure, scalable, and energy-efficient to identify anomalies in heterogeneous environments that rely on IoT and WSN.

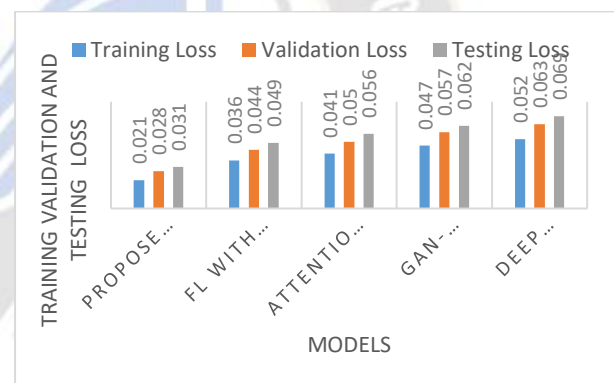


Figure 16: Comparison of training, validation and testing loss

The proposed XAI-based FL system exhibits insignificant loss values (0.021 training, 0.028 validation, 0.031 testing), which proves its better convergence, stability, and generalization compared to the current deep and AI models in Figure 16. XAI-interpretability and federated optimization improve adaptability and distributed learning. In contrast to CNN-LSTM, BiLSTM, GAN, and RL models that are influenced by synchronization, noise, or reconstruction errors, the proposed system guarantees effective, secure, and explainable anomaly detection of large-scale IoT-driven WSNs.

6. Conclusions

The proposed XAI-Driven FL framework is efficient in solving the critical problems of energy conservation, security, and real time anomaly detection in the IoT-based WSNs. Experiments indicate that the system is always superior to the current advanced AI-based systems, such as FL using CNN-LSTM, GAN-Based AD, Attention-Based BiLSTM, and Deep Autoencoder using RL. The system has the lowest MAE (0.024), MSE (0.0039), and RMSE (0.062), which was used to show very accurate anomaly detection and minimal error in prediction. It also achieves high performance metrics that are accurate (97.5%), precise (93.8%), recalls (94.0) and F1-score (93.9). Moreover, it is able to support low latency (42.3 -53.0 ms) in a large-scale network and provides high data confidentiality (96.5%), detection (97.8%), and bandwidth efficiency (170.3 kbps). The remarkable functionality of the system is due to the fact that the interpretation of XAI-based offers transparency and trust to routing and anomaly decision-making; FL allows autonomous intelligence without raw data sharing; and energy-aware routing and scheduling optimizes communication and increases network lifetime. The given framework proposes a scalable, secure, and explainable solution to a real-time AD in IoT-based WSNs to provide stable decision-making, optimized use of resources, and stable network communication even in a variety of IoT settings.

References

- [1] Al Ali, I. A. J., & Alhaidery, M. M. A. (2025). Machine Learning Techniques for Anomaly Detection in IoT and WSN: A review. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, 17(2), 229-240.
- [2] Alatawi, M. N. (2025). Optimizing security and energy efficiency in IoT-Based health monitoring systems for wireless body area networks. *Scientific Reports*, 15(1), 24921.
- [3] Menon, U. V., Kumaravelu, V. B., Kumar, C. V., Rammohan, A., Chinnadurai, S., Venkatesan, R., ... & Selvaprabhu, P. (2025). AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. *IEEE Access*.
- [4] Hudda, S., & Haribabu, K. (2025). A review on WSN based resource constrained smart IoT systems. *Discover Internet of Things*, 5(1), 56.
- [5] Mohamed, A., Ismail, I., & AlDaraawi, M. (2025). IoT-Driven Intelligent Energy Management: Leveraging Smart Monitoring Applications and Artificial Neural Networks (ANN) for Sustainable Practices. *Computers*, 14(7), 269.
- [6] Akshya, J., Sundarrajan, M., Vijayakumar, R., Dhanaraj, R. K., & Nayyar, A. (2025). Explainable AI-driven intrusion detection for securing IoT-enabled autonomous transportation systems. *Cluster Computing*, 28(14), 884.
- [7] Seyedi, B., & Postolache, O. (2025). Securing IoT Communications via Anomaly Traffic Detection: Synergy of Genetic Algorithm and Ensemble Method. *Sensors*, 25(13), 4098.
- [8] Manchanda, R., Panchal, S., Sandiri, R., Sudhamsu, G., Mehta, A., Gupta, R., ... & Bukate, B. B. (2025). Energy-efficient clustering and routing for IoT-enabled healthcare using adaptive fuzzy logic and hybrid optimization. *Scientific Reports*, 15(1), 34619.
- [9] Velvizhi, V. A., & Anbarasan, M. (2025, April). Real-Time Energy Monitoring for Renewable Power Systems: Enhancing Stability and Efficiency with IoT-Based Wireless Sensor Networks. In *2025 International Conference on Computing and Communication Technologies (ICCCCT)* (pp. 1-4). IEEE.
- [10] Wandwi, G. (2025). Energy-Efficient IoT Sensor Design for Continuous Patient Monitoring in Smart Hospitals. *Journal of Sensors, IoT & Health Sciences (JSIHS, ISSN: 2584-2560)*, 3(3), 1-13.
- [11] Saravanan, T. R., Unhelkar, B., Shankar, S., & Nagarajan, G. (2025). AI-Driven Energy-Efficient Cybersecurity Frameworks for Sustainable Digital Infrastructures. *Results in Engineering*, 107717.
- [12] Dankan Gowda, V., Kumar, P. S., Jagtap, M. M., Shekhar, R., & Vadisetty, R. (2025). Data Collection and Analysis for Real-Time Secure Energy Monitoring and Optimization. *Secure Energy Optimization: Leveraging Internet of Things and Artificial Intelligence for Enhanced Efficiency*, 381-412.
- [13] Anwer, R. W., Abrar, M., Salam, A., & Ullah, F. (2025). TEAD: trust-enhanced anomaly detection framework for intrusion detection in IoT-enabled wireless sensor networks (WSNs). *Wireless Networks*, 1-19.
- [14] Soby, D., Balaji, C., Duraisamy, B., Thangaraj, K., Kumar, S. S., & Sivaranjani, C. (2025, September). IoT-Driven Precision Agriculture: Real-Time Soil Health and Irrigation Monitoring using Low-Power Wireless Sensor Networks. In *2025 4th*

- International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 8-15). IEEE.
- [15] Ishaya, N., Sulaimon, H. A., & Abdullahi, H. (2025). Optimizing energy efficiency in IoT networks for sustainable smart cities: a focus on energy-efficient communication protocols. *Proceedings of the Nigerian Society of Physical Sciences*, 173-173.
- [16] Kok, C. L., Heng, J. B., Koh, Y. Y., & Teo, T. H. (2025). Energy-, Cost-, and Resource-Efficient IoT Hazard Detection System with Adaptive Monitoring. *Sensors*, 25(6), 1761.
- [17] Jayachandran, J., & Vimaladevi, K. (2025). A dual layer secure and energy-efficient model for border surveillance using sea lion inspired strategy in wireless sensor networks. *Scientific Reports*, 15, 24974.
- [18] Bristy, I. J., Tabassum, M., Islam, M. I., & Hasan, M. N. (2025). IoT-driven predictive maintenance dashboards in industrial operations. *Saudi Journal of Engineering and Technology (SJEAT)*, 10(9), 457-466.
- [19] Mustafa, R., Sarkar, N. I., Mohaghegh, M., Pervez, S., & Vohra, O. (2025). Cross-Layer Analysis of Machine Learning Models for Secure and Energy-Efficient IoT Networks. *Sensors*, 25(12), 3720.
- [20] Reddy, M., Krishnan, S. B., Shaik, A., & Chakrabarti, P. (2025). AI-integrated adaptive MANET framework for IoT-driven healthcare systems: enhancing scalability, security, and real-time communication. *The European Physical Journal Plus*, 140(9), 1-34.
- [21] Alshuhail, A., Alshahrani, A., Mahgoub, H., Ghaleb, M., Darem, A. A., Aljehane, N. O., ... & Alzahrani, F. (2025). Machine edge-aware IoT framework for real-time health monitoring: Sensor fusion and AI-driven emergency response in decentralized networks. *Alexandria Engineering Journal*, 129, 1349-1361.
- [22] Parmar, H., Murari, U. K., & Singh, S. K. (2025). Smart Polymer-Integrated IoT Systems: A Mathematical Framework for Real-Time Sensing and Adaptive Material Behavior (ICSEM-2025). In *Macromolecular Symposia* (p. e70183).
- [23] Jeyalakshmi, M. G., Iniyasree, B., Manonmani, G., Mounica, S., & Vanathi, K. V. (2025, August). IoT-Enabled Smart Water Management System using ESP32 and RFID for Urban Applications. In *2025 International Conference on Modern Sustainable Systems (CMSS)* (pp. 364-369). IEEE.
- [24] Singh, A. R., Sujatha, M. S., Kadu, A. D., Bajaj, M., Addis, H. K., & Sarada, K. (2025). A deep learning and IoT-driven framework for real-time adaptive resource allocation and grid optimization in smart energy systems. *Scientific Reports*, 15(1), 19309.
- [25] Draz, U., Ali, T., Yasin, S., Hijji, M., Ayaz, M., & Aggoune, E. H. M. (2025). Decentralized energy swapping for sustainable wireless sensor networks using blockchain technology. *Mathematics*, 13(3), 395.
- [26] Baranwal, A. (2025). IoT-based environmental sensing solutions for smart city monitoring. *Smart City Insights*, 2(1), 1-16.
- [27] Patil, B., Singh, K., Ganapathi, R., Asudani, D. S., Sharma, K. D., Sindhwani, N., & Singh, E. (2025). CRNN-KHO: hybrid deep learning optimization framework for enhancing energy efficiency in IoT-enabled wireless networks. *International Journal of Information Technology*, 1-7.
- [28] Alamri, M. Z., Haseeb, K., Humayun, M., & Ramzan, N. (2025). Fog-Driven IoT and Trust-aware Machine Learning Framework for Early Disability Detection and Rehabilitation in Healthcare Systems. *Journal of Disability Research*, 4(5), 20250717.
- [29] Singh, P., Ponmaniraj, S., Aggarwal, A., & Kumari, S. (2025, June). Energy-Efficient IoT Architectures for Smart Cities: Implementing Adaptive Edge Computing for Sustainable Urban Development. In *2025 International Conference on Electronics, AI and Computing (EAIC)* (pp. 1-6). IEEE.
- [30] Shili, M., & Anwar, S. (2025). Real-Time Electrical Energy Optimization in E-Commerce Systems Based on IoT and Mobile Agents. *Information*, 16(7), 551.