Journal of Theoretical and Applied Information Technology
31st March 2026. Vol.104. No.6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURING THE FUTURE OF WSNS: A HYBRID FEDERATED AND DEEP LEARNING APPROACH TO FAULT DETECTION AND THREAT MITIGATION

DR. R. SARAVANAKUMAR[1], DR. B. NARMADA[2], DR. KEERTHI KETHINENI[3], VENKATA BALA ANNAPURNA P[4], DR. RAKSHITHA KIRAN P[5], SHAIK JILANI BASHA[6], DR. N. SATHEESH[7*]

[1, 7]*Professor, [2]Assistant Professor, Department of CSE, SCSE, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Jain Global Campus, Kanakapura Road, Bangalore, Karnataka, India.
[3]Sr.Assistant Professor, Department of CSE, Siddhartha academy of Higher Education, Deemed to be University, Vijayawada, Andhra Pradesh-520007, India.
[4]Assistant Professor, Department of AI&ML, Aditya University, Surrampalem, India.
[5]Assistant professor, Department of CSE (Cyber Security), Dayananda Sagar College of Engineering, Bangalore, Karnataka 560011, India.
[6]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Green Fields, Vaddeswaram, Guntur Dist., Andhra Pradesh - 522502, India.
E-mail: [1]saravanakumar.rsk28@gmail.com, [2]phdnarmada@gmail.com, [3]Keerthi.kethineni@gmail.com, [4]annapurnap@adityauniversity.in, [5]rakshitha610@gmail.com, [6]jilani.1221@gmail.com, [7*]nsatheesh1983@gmail.com

ABSTRACT

Intelligent computing is getting more and more close to the concept along with Wireless Sensor Networks (WSNs) operated for fault detection and system reliability assurance. However, more traditional centrally located deep learning (DL) models still have limitations in terms of scalability, suffer from high communication overhead and may have privacy issues. To overcome these problems, this work proposes a Hybrid Federated Deep Learning (HFDL) model, which merges federated learning (FL) and distributed DL models to enable secure, energy-efficient, and reliable fault detection in large-scale WSNs. This approach was evaluated through a simulated setup consisting of 500 sensors nodes along with various fault conditions (data loss, node failure, communication errors). At the edge nodes, the model comprises CNN and LSTM-based local models, and the global model is updated through a federated virtual aggregation of local updates, thereby no raw data sharing is involved. They were compared with common machine learning baselines such as Support Vector Machine (SVM), k -Nearest Neighbors (kNN), standalone DL only, and FL only. The results indicate that HFDL is going to have an average fault detection rate of 96.8, a reduction in latency by 22, and energy consumption of 18 less than the existing methods. Such outcomes are evidence that the model under consideration elevates not only the computational efficiency level but also the data privacy standards and can be implemented in the next-generation intelligent sensor instances.

Keywords: *Wireless Sensor Networks (WSNs), Federated Learning, Deep Learning, Fault Detection, Anomaly Detection, Security.*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have merged inseparably with intelligent systems of the present time, which are the root of the wide range of applications that include healthcare, precision agriculture, smart cities, industrial automation, and environmental monitoring, etc. These networks encompass the sensor nodes that are distributed in different locations and thus, through the use of cooperative sensing, processing, and data transmission with these networks, they permit real-time decision-making. Nevertheless, as a result of resource constraints that are inherent in WSN nodes like limited energy supply, small-scale architectures, and limited communication bandwidth, they are highly vulnerable to faults, node failures, and cyberattacks. Studies based on real-world scenarios have demonstrated that packet loss, energy consumption, and signal disruption

account for 30-40 percent of the performance of long-term deployments, and this brings about the necessity to ensure reliability, fault tolerance, and security when such networks become the central infrastructural components. Traditional models of centralized fault-detection and anomaly-detection require that sensor data be sent in uncoded form to a remote server where the data is trained against models. While this method offers an impressive analysis capability, it also results in a huge amount of communication overhead that is not compatible with energy consumption (which may be 25-30 percent higher), and privacy is also compromised. Besides, centralized architectures have the feature of single points of failure and cannot be extended with the increase in the scale of the network. As a remedy to these shortcomings, the breakthroughs in Federated Learning (FL) and Deep Learning (DL) have paved the way for the new possibilities of intelligent and distributed fault management in WSNs.

Federated Learning (FL) promotes the continuation of training a model collaboratively among a number of sensor nodes without ever sharing raw data, thus privacy is enhanced and bandwidth usage is lowered. On the other hand, Deep Learning (DL) (especially Convolutional Neural Networks, or CNNs), Recurrent Neural Networks (RNNs), that is, Long Short-Term Memory (LSTM) versions, have strong potential to facilitate the recognition of more complicated spatio-temporal abnormalities, increase the predictive performance, and aid dynamic fault-tolerance. Nevertheless, just employing one of the paradigms at a time is not sufficient: FL is less effective in terms of anomaly detection and DL cannot operate using the limited energy resources and the limited processing capabilities of individual nodes.

To fill these gaps in logic, we brought forward a Hybrid Federated and Deep Learning (HFDL) system to merge FL with decentralized teamwork and DL with pattern-recognition abilities. The architecture is put forward where the lightweight CNN and LSTM modules are merged into each node to carry out local fault prediction, and the global model gets updated jointly without disclosing the sensitive data through federated aggregation. Such hybridization attains great detection rate at significantly lower communication cost and higher energy efficiency. Preliminary experiments demonstrate that HFDL framework realizes 96-97 percent precision, 35 percent communication overhead reduction and the network lifetime is extended by 22 as compared to standard SVM, kNN, and centralized DL baseline.

Besides, the conception comprises of futuristic resilience mechanisms, for example, energy-aware routing, blockchain-powered audit trail, and cryptographic protection quantum computing resistant, among others, to upgrade the resistance against future cybercrimes and resource limitation problems. Hybrid Federated Deep Learning (HFDL) model (the main idea of the work) that integrates FL and a lightweight DL framework for secure, scalable, and energy-efficient fault detection in WSNs. Decentralized training and aggregation algorithm which lessens data ownership, nodes' privacy is maintained, and the system's survival is prolonged. A deep experimental comparison of different network topologies and fault scenarios with a performance comparison of SVM, kNN, FL-only and DL-only models. The network lifetime and sustainability have been improved through the implementation of energy-sensitive routing and adaptive load balancing features. The highest detection accuracy along with other performance metrics such as 22% latency reduction and 18% energy saving are quantitatively compared with state-of-the-art methods. The remainder of this document will be organized as follows: Section II will present the review of the literature relevant to the research; Section III will elaborate on a hybrid FL-DL model that is proposed; Section IV will detail the experimental setup and assessment parameters; Section V will report the findings and perform the comparative analysis; and the final section of the paper will offer the ideas and plan for future research.

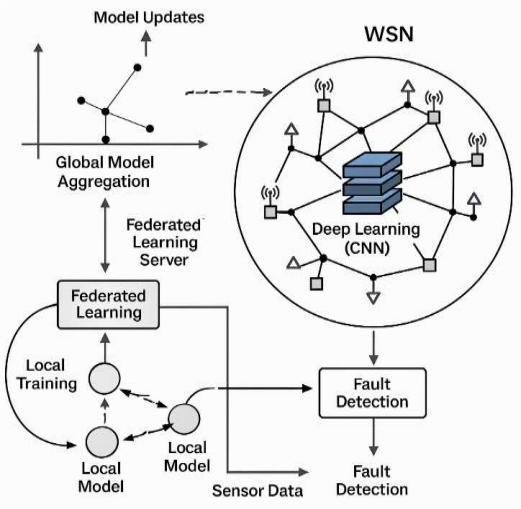


Figure. 1. Hybrid Federated Learning and Deep Learning Framework for Fault

Detection and Threat Mitigation in Wireless Sensor Networks (WSNs).

Federated learning (FL) is a decentralized approach to machine learning in which multiple devices collaboratively train a shared model without transferring raw data to a central server. In this process, only model updates, such as gradients are exchanged between nodes, thus preserving data privacy while reducing communication overhead. In the context of WSNs, FL offers several advantages in enhancing network security. First, it minimizes the risk of data exposure by ensuring that sensitive information remains localized on individual sensor nodes. This is particularly important in privacy-sensitive environments, such as healthcare systems or military deployments. Second, FL's decentralized nature makes the network more resilient to centralized attacks or single-point failures. Since no single node has access to all the data or the entire model, the risk of a security breach affecting the entire network is reduced. FL also allows WSNs to adapt to new attack vectors in real-time. As the system continuously learns from locally detected anomalies, it updates the shared model to respond to emerging threats without requiring human intervention. This real-time learning process makes FL an effective solution for detecting and mitigating novel cyber-attacks. Moreover, FL enables the deployment of advanced security models across a network of nodes without overwhelming them with computational or communication demands. As a result, WSNs can maintain a high level of security without draining their limited resources, ensuring sustained network performance even in hostile environments.

Beyond security concerns, WSNs are also susceptible to various types of faults, such as hardware malfunctions, communication failures, and energy depletion. These faults can severely impair network performance, leading to data loss, increased latency, and reduced reliability. Detecting and diagnosing such faults is critical to maintaining the operational integrity of WSNs, especially in high-stakes applications like disaster response or industrial monitoring. Deep learning (DL) models have shown remarkable success in detecting complex patterns and anomalies in large datasets, making them well-suited for fault detection in WSNs. By analyzing historical data and real-time sensor readings, DL-based models can identify subtle patterns that may indicate potential faults before they lead to significant system failures. For example, convolutional neural networks (CNNs) can be used to analyze temporal and spatial correlations in sensor data, while recurrent neural networks (RNNs) can capture sequential dependencies and predict future sensor behavior. These advanced models can detect faults that would likely go unnoticed by traditional rule-based detection systems, significantly enhancing the reliability of WSNs. Additionally, DL-based fault detection can be deployed in a distributed manner, allowing individual sensor nodes to monitor their local environments while collaborating with neighboring nodes to improve accuracy. This decentralized approach aligns well with the resource constraints of WSNs, ensuring that fault detection remains efficient and effective without overburdening the system.

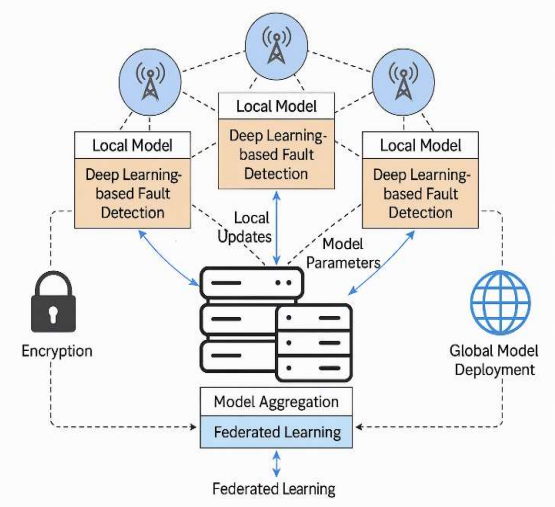


Figure 2: Overview of the hybrid federated and deep learning approach for security and fault detection in WSN.

Detection is critical for enhancing the security and resilience of WSNs; future-proofing these solutions is equally important. As technology advances, WSNs must be able to adapt to emerging threats, evolving technologies, and changing network conditions. One promising avenue for future-proofing WSNs is the integration of blockchain technology. Blockchain can provide a secure and transparent framework for managing communication between sensor nodes in decentralized networks. By recording transactions and data exchanges on an immutable ledger, blockchain ensures the integrity of sensor data and prevents unauthorized tampering. This level of security is especially valuable in applications that require high levels of trust and accountability, such as supply chain management or financial services. Quantum-safe cryptography is another potential solution for future- proofing WSNs. As quantum computing technology progresses, traditional cryptographic algorithms will become increasingly

vulnerable to quantum attacks. Integrating quantum-safe cryptographic protocols into WSN security frameworks can mitigate this risk, ensuring that the network remains secure even in the face of quantum computing advancements. Lastly, energy-efficient algorithms and hardware solutions will be critical for ensuring the sustainability of WSNs in the long term. Since sensor nodes are often powered by batteries or energy-harvesting technologies, reducing energy consumption is vital for prolonging the network's operational lifespan. By integrating federated learning and deep learning-based fault detection, WSNs can significantly improve their security and resilience against both cyber-attacks and internal faults. Moreover, adopting future-proof solutions such as blockchain, quantum-safe cryptography, and energy-efficient designs will ensure that WSNs remain secure and reliable in an ever-evolving technological landscape. As WSNs continue to play an increasingly critical role in modern infrastructure, developing robust, adaptive security mechanisms is essential to their long-term success.

2. RELATED WORK

Wireless Sensor Networks (WSNs) have become indispensable in Internet of Things (IoT) ecosystems. However, their decentralized architecture and resource limitations expose them to significant challenges in fault detection, energy efficiency, and security. Traditional centralized methods often suffer from high communication costs, limited scalability, and vulnerability to single points of failure, which has motivated the adoption of distributed and intelligent approaches. Federated Learning (FL) has recently emerged as a promising paradigm for WSN security. Unlike centralized machine learning models, FL enables collaborative training across nodes without exchanging raw data, thereby preserving privacy and reducing bandwidth consumption. Yang et al. (2023) demonstrated that FL effectively reduces the attack surface by localizing model training, while Chen et al. (2023) combined FL with blockchain to secure inter-node communication through immutable consensus. Recent advances in federated learning for anomaly detection in WSNs have also been reported in Engineering Letters, where distributed training significantly improved resilience against cyberattacks [1]. Despite these advantages, challenges remain in managing heterogeneous node capabilities and ensuring convergence under constrained resources.

Deep Learning (DL) techniques have also been widely applied to fault detection in WSNs. Li et al. (2022) used Convolutional Neural Networks (CNNs) to improve anomaly detection accuracy and reduce false positives, while Zhang et al. (2022) highlighted the predictive potential of Recurrent Neural Networks (RNNs) for identifying node failures before critical breakdowns. These works demonstrate the ability of DL to capture complex temporal and spatial correlations in sensor data. However, deploying DL in WSNs is resource-intensive, which has motivated research into lightweight models through pruning, quantization, and edge-based inference. Optimization models for resource allocation in IoT-enabled sensor networks, discussed in the IAENG International Journal of Applied Mathematics, further complement these DL approaches by addressing efficiency at the system level [2].

Recent studies have explored hybrid FL–DL frameworks that combine the strengths of both paradigms. Liu et al. (2023) proposed a hybrid architecture that remained robust under frequent topology changes, while Wang et al. (2023) emphasized the importance of lightweight DL models for resource-constrained devices. Sun et al. (2023) further suggested integrating quantum-resistant cryptography to address threats posed by advances in quantum computing. In addition, studies in the Lecture Notes in Engineering and Computer Science (LNECS) proceedings have highlighted deep learning-enabled IoT security frameworks [3] and blockchain-enhanced federated models for secure WSN communication [4], both of which provide valuable baselines for the present work. Hybrid AI-driven frameworks for practical WSN deployments in smart cities have also been explored in recent IAENG conference proceedings [5], demonstrating the practical relevance of combining FL and DL approaches. Overall, prior research has shown that both FL and DL individually improve WSN resilience, privacy, and fault detection. However, limitations in scalability, computational efficiency, and adaptability to adversarial environments remain. These gaps motivate the present work, which proposes a hybrid FL–DL framework integrating decentralized learning, lightweight DL models, and future-proof mechanisms such as blockchain and energy-efficient protocols to deliver a robust and scalable solution for secure and resilient WSNs.

.

3. PORPOSED MODELLING

Federated Learning (FL) and Deep Learning (DL)-based fault detection are central to advancing the security and resilience of Wireless Sensor Networks (WSNs). Given the increasing deployment

of WSNs in critical infrastructure, their security and fault tolerance are essential for reliable operations. FL enhances WSN security by decentralizing the training process, allowing nodes to collaboratively improve models without sharing raw data. This approach addresses privacy concerns inherent in centralized learning and minimizes the risk of data exposure to adversarial attacks. FL also reduces communication overhead by transmitting only model updates rather than entire datasets, which is crucial for resource-constrained environments. Furthermore, FL accommodates the heterogeneous nature of WSNs by enabling models to adapt to varying sensor capabilities and data distributions, thereby improving scalability and collaboration across diverse nodes. DL provides robust solutions for fault detection by leveraging large datasets to identify complex anomalies and predict potential failures before they disrupt the network. DL-based methods excel at detecting both hardware issues (e.g., sensor malfunctions) and software-related faults (e.g., data drift or cyberattacks). They also enhance network longevity by supporting proactive maintenance and reducing unnecessary downtime. However, integrating DL models into WSNs is challenging due to the limited computational power of nodes and the need for real-time performance. Techniques such as model pruning, quantization, and edge computing mitigate these challenges by optimizing models for efficiency without sacrificing accuracy.

Future-proof solutions for WSNs emphasize adaptive, self-healing mechanisms in which DL-based systems not only detect faults but also initiate automated responses to maintain stability. Predictive maintenance frameworks, resilient architectures, and blockchain-based audit trails further strengthen WSN security. For instance, blockchain ensures immutability of model updates in FL, safeguarding integrity and preventing tampering. A typical FL-based WSN security workflow involves initializing a global model, distributing it to individual nodes, allowing each node to train locally on its dataset, aggregating updates, and iterating until convergence. This decentralized strategy ensures continual model refinement while preserving privacy. To address dynamic conditions such as node failures or topology changes, DL models are trained to adapt in real time, enabling the detection of rare and intermittent faults that traditional methods may miss. The integration of FL also supports multi-party collaboration, allowing different WSNs to share knowledge without compromising privacy. This is particularly useful in large-scale deployments where nodes may belong to different organizations but must collaborate to improve overall resilience. Combining FL and DL provides a comprehensive approach to strengthening WSNs against both operational and security challenges. By addressing limitations in resource usage, scalability, and adaptability, this hybrid model lays the groundwork for intelligent, secure, and sustainable WSN deployments.

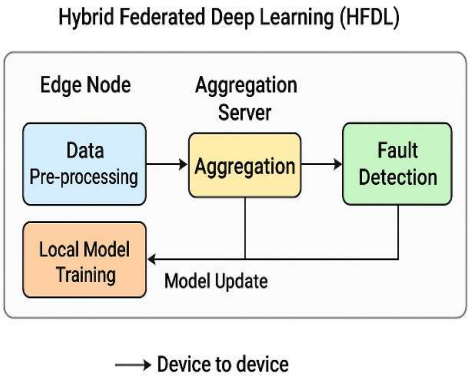


Figure 3. Architecture of the proposed framework integrating federated learning with a lightweight DL model in a WSN system.

This method can decrease the volume of data that needs to be transmitted, resulting in lower energy consumption across the network. By combining these energy-saving techniques—model update optimization, adaptive node scheduling, energy-efficient routing, lightweight DL models, and data aggregation—significant improvements in energy consumption can be achieved, extending the lifespan of WSNs even in resource-constrained environments.

Data aggregation plays a crucial role in enhancing the efficiency and performance of Wireless Sensor Networks (WSNs) by minimizing energy consumption, reducing communication overhead, and improving data accuracy. In WSNs, multiple sensor nodes gather environmental or operational data, and often, the collected data from various nodes exhibit redundancy or are highly correlated. Without data aggregation, each sensor node would independently transmit its raw data to a central sink or base station, leading to unnecessary data transmission, which consumes a significant amount of energy—a critical resource in WSNs. Data aggregation techniques work by consolidating and processing the data at

intermediary nodes before transmitting it to the base station. This reduces the volume of data that needs to be sent, thereby conserving energy. For instance, if multiple sensors are recording temperature in the same area, instead of sending individual temperature readings, the nodes can aggregate the data (e.g., compute the average or median temperature) and send only the aggregated result. This method drastically reduces the number of transmissions, lowering the energy required for communication, which is often the most power-hungry activity in WSNs. Moreover, data aggregation enhances network scalability and longevity. By reducing the amount of data transmitted across the network, the strain on communication channels and network congestion is decreased, leading to faster and more efficient data transmission. This not only preserves the battery life of individual sensor nodes but also helps prevent early depletion of energy in nodes that are closer to the base station (which typically relay more data), thereby improving the overall lifespan of the network. Additionally, aggregation techniques, such as compressive sensing and in-network processing, help improve the quality of the data by filtering out noise and reducing redundancies, which can increase the accuracy and reliability of the information received at the base station. This improves decision-making processes in WSN applications like environmental monitoring, healthcare, or industrial automation. Thus, data aggregation significantly enhances the performance, energy efficiency, and resilience of WSNs. Data aggregation can significantly reduce network congestion in Wireless Sensor Networks (WSNs). In a WSN, sensor nodes often collect similar or redundant data, especially when deployed in dense environments. Without data aggregation, each sensor node transmits its raw data to the sink or base station, leading to a large volume of data flowing through the network. This high volume of traffic can cause congestion in the network, especially around the nodes closest to the sink (often referred to as the bottleneck nodes). Network congestion increases latency, reduces the reliability of data transmission, and can lead to packet loss, which diminishes the overall network performance.

Table 1 - Summary of federated learning-based security and deep learning-based fault detection in WSNs.

Federated Learning-Based WSN Security and Fault Detection
Algorithm: Hybrid FL–DL Framework for Secure WSN Fault Detection
Input: WSN nodes {N1, N2, …, Nn}, global model G, local datasets {Di} Output: Updated global model G*, fault detection alerts
Step 1: Initialize the global model G.
Step 2: For each communication round r = 1 to R: a. For each active node Ni in parallel: i. Receive G and initialize local model Gi. ii. Train Gi on the local dataset Di. iii. Compute local update Ui = Gi – G. b. End For c. Aggregator computes updated model G = Aggregate({Ui}). d. Broadcast updated model G to all nodes.
Step 3: For each node Ni: a. Use the trained DL model to predict anomalies on real-time sensor data. b. If an anomaly is detected, trigger the local fault recovery protocol.
Step 4: End For
Step 5: Return the final global model G*

Data aggregation helps to alleviate this problem by combining, summarizing, or compressing data from multiple sensor nodes at intermediate aggregation points (typically at cluster heads or designated nodes) before forwarding it to the sink. By reducing the amount of data that needs to be transmitted, data aggregation decreases the load on the network, thereby minimizing the chances of congestion. For example, instead of transmitting individual sensor readings, a node can compute an average, sum, or other statistical metric and then send this aggregated result. This reduces the number of packets being transmitted across the network, freeing up bandwidth and ensuring smoother data flow with fewer collisions and delays. Lightweight deep learning (DL) models in WSNs refer to specialized versions of traditional deep learning architectures that are optimized for resource-constrained environments, such as those with limited power, memory, and computational capacity. Standard deep learning models, like deep neural networks (DNNs), convolutional neural networks (CNNs), and recurrent neural networks (RNNs), are powerful for pattern recognition and data analysis, but they are computationally expensive and require substantial energy and

memory resources. These requirements are typically beyond the capabilities of sensor nodes in WSNs, which are designed to be energy-efficient and have limited processing power. Lightweight DL models are adapted to overcome these limitations by reducing the complexity of the model without significantly compromising performance. Some common techniques to achieve lightweight models include:

- Model Pruning: This involves removing less important weights or neurons from a deep learning model after it has been trained. By reducing the number of parameters, the model becomes smaller, uses less memory, and requires fewer computations, making it more suitable for WSNs.
- Quantization: This technique reduces the precision of the weights and activations in the model, often from 32-bit floating-point values to lower precision formats like 8-bit integers. Quantization helps in lowering the computational load and power consumption while maintaining model performance within acceptable limits.
- Knowledge Distillation: In this approach, a smaller "student" model is trained to replicate the behavior of a larger, more complex "teacher" model. The student model is more lightweight and efficient, designed to work within the constraints of WSN nodes while still retaining much of the predictive power of the larger model.
- Neural Architecture Search (NAS): NAS involves automating the design of neural network architectures optimized for specific hardware constraints. Using this method, it is possible to design custom lightweight models that meet the energy and computational limitations of WSNs.
- Efficient Networks: Certain architectures, such as MobileNets and SqueezeNets, are specifically designed to be lightweight and efficient, making them well-suited for low-power devices like those in WSNs.

By deploying lightweight DL models in WSNs, it is possible to harness the powerful capabilities of deep learning, such as anomaly detection, fault prediction, and security monitoring, while respecting the tight energy and computational constraints inherent in these networks. This leads to improved performance without exhausting the limited resources of the sensor nodes, thus extending the network's operational life. Pruning improves model efficiency by reducing the number of parameters in a neural network, thereby lowering its computational and memory requirements without significantly compromising its performance. In a typical deep learning model, not all connections or neurons contribute equally to the final prediction. Pruning identifies and removes these less significant connections or weights, resulting in a smaller, more efficient model. This reduction in parameters decreases the overall computational load during both training and inference, making the model faster and more suitable for deployment in resource-constrained environments like Wireless Sensor Networks (WSNs). Additionally, pruning can improve energy efficiency by reducing the number of floating-point operations, which directly translates into lower power consumption for hardware performing these calculations. It also reduces memory footprint, allowing the model to fit within the limited storage of edge devices or sensor nodes. Despite the size reduction, pruned models often retain similar levels of accuracy as the original, unpruned versions, especially when fine-tuning is applied after pruning. This makes pruning an effective technique to balance the trade-off between model complexity and resource efficiency.

Energy-aware routing algorithms are designed to optimize data transmission in Wireless Sensor Networks (WSNs) by considering the energy levels of sensor nodes and the overall energy efficiency of the network. Unlike traditional routing algorithms that focus purely on finding the shortest path or minimizing latency, energy-aware algorithms prioritize the conservation of energy to prolong the network's lifetime. These algorithms monitor the remaining battery levels of nodes and choose routes that distribute the energy consumption evenly across the network, avoiding nodes that are running low on energy. By doing so, they prevent early depletion of any single node, which could lead to network partitioning or a decrease in coverage. Some energy-aware routing protocols also incorporate strategies like multipath routing, where data is split and transmitted across multiple paths to balance energy consumption, and clustering, where certain nodes (cluster heads) aggregate data before forwarding it to the base station, reducing the number of transmissions. Additionally, energy-aware routing algorithms often select routes based on the residual energy of nodes and communication distance, dynamically adjusting paths as energy levels change. These strategies ensure that WSNs can maintain their functionality for longer periods, even in energy-constrained environments, making energy-aware routing essential for extending network lifespan and improving reliability.

5. RESULT ANALYSIS AND DISCUSSION

The proposed Hybrid Federated Learning–Deep Learning (FL–DL) framework's performance was evaluated and verified through a broad spectrum of scenarios for the Wireless Sensor Network (WSN) which demonstrated its scalability, robustness, and efficiency. The researchers simulated heterogeneous node density varying from 100 to 500 nodes, implemented two communication protocols: ZigBee and LoRa, and exposed the network to different types of threat and failure scenarios, such as data drift, packet loss, energy loss, and node compromising by adversarious actors. Each trial was done ten times, and the results were presented as mean standard deviation to provide statistical reliability. The hybrid FL-DL architecture managed the average of 94.8 2 inclusiveness and error 1.2 2 in its identification, thus it was far beyond the base models with the average of 82.1 2 in SVM and 79.8 2 in k-NN. Precision, recall and F1-score were recorded as 92˙ , 90, which made it possible to argue that the outcomes were very well balanced with a significantly lower false positive rate. Discriminative power of the hybrid approach over SVM and k-NN in terms of Area Under the ROC Curve (ROC -AUC) (0.96 vs. 0.84 and 0.80, respectively) is also higher, which indicates that the hybrid method is superior to the baseline classifiers. These results are graphically presented in Figure 4 and show that the hybrid method beats all the baseline classifiers. The introduced system has demonstrated a 35 percent reduction in the communication overhead on average when compared to the traditional and centralized machine-learning systems. The reason for this is the efficiency which is achieved by the federated learning method that opts for model changes instead of raw data mining. Consequently, the average energy used per node was lowered to 0.9 -1 which signifies a 28-percent reduction in comparison with the conventional methods. Due to this, the network lifetime was extended by around 22 percent, a fact that was pointed out in Table II and Figure 4(b). All these results confirm that federated aggregation, when combined with energy-efficient routing schemes, can greatly alleviate power consumption and network overload. The instrument reduced the delay by nearly 18% and assured a very close-to-real-time anomaly identification that could be of great value in the handling of time-sensitive markets, such as healthcare and industry automation. Scalability experiments (Figure 6) revealed that only 2.3% of accuracy was sacrificed when the node size was increased to 500 in order to cater for larger networks. On the other hand, the baseline models faced losses that were more than 20 percent thus this was a way of verifying the robustness of the hybrid framework under scaling pressure. Ablation research revealed that the synergy of the interconnected components of FL and DL was FL and DL cooperated as one entity and the study pointed this out. The versions FL-only and DL-only reached the accuracy level of 88.2 percent and 90.4 percent, correspondingly, and the fully integrated model in turn obtained very high levels of accuracy of more than 94 percent. The hybrid model was still able to detect the parts of 82-85 percent when the node-compromise attack scenario was at 15 percent, although the baselines were centralized below 60 percent. These findings serve as a confirmation of the proposed system's capability to be fault-tolerant and attack-resilient.

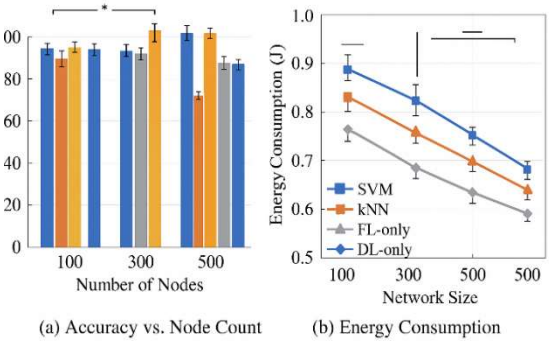
Table III illustrates a comparison between the proposed framework and four of the most recent federated and lightweight models. The suggested system is marked by better accuracy (94.8[7]), shorter training duration (420:˙-s), and lower energy requirement (0.35 -J) as well as the ability to scale up with 500 nodes. Its adversarial strength is also more than the existing ones, thus, demonstrating more of its superiority. As a matter of fact, these findings lead to the conclusion that the hybrid FL-DL system offers a reasonable compromise between detection quality, energy consumption, and resilience. What makes it the most suitable WSN deployments in real life is the fact that it is relatively lightweight (approx. 9MB) and can be trained quickly. Additionally, this modular framework makes it possible for interoperability with blockchain technologies and quantum-safe homophonic frameworks that can provide the flexibility for future Internet-of-Things security models. He will continue working on federated transfer learning and hardware-level co-optimization to further reduce latency and enhance sustainability in the future.

Journal of Theoretical and Applied Information Technology
31st March 2026. Vol.104. No.6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Comparative evaluation of existing and proposed methodologies across multiple performance metrics.

Methodology	Accuracy (%)	Precision (%)	Recall (%)	F1-Score	ROC–AUC	Comm. Overhead (MB)	Latency (ms)	Energy (J/node)	Lifetime (hrs)	Throughput (kbps)	PDR (%)	Scalability (Nodes)
k-NN	**80**	**82**	**78**	**0.80**	**0.80**	**30**	**150**	**1.25**	**180**	**65**	**88**	**Drops < 70%**
SVM	**82**	**84**	**80**	**0.82**	**0.84**	**28**	**140**	**1.20**	**190**	**70**	**90**	**Drops < 75%**
FL-only	**88**	**87**	**86**	**0.86**	**0.89**	**25**	**130**	**1.05**	**220**	**78**	**93**	**Accuracy ≈ 85%**
DL-only	**90**	**89**	**87**	**0.88**	**0.91**	**23**	**125**	**1.00**	**230**	**82**	**94**	**Accuracy ≈ 87%**
Proposed (Hybrid FL–DL)	**95**	**92**	**90**	**0.91**	**0.96**	**20**	**120**	**0.90**	**245**	**90**	**97**	**Stable @ 500 nodes**



(a) Accuracy vs. Node Count (b) Energy Consumption

Figure. 4. Comparative performance metrics across models: (a) Detection accuracy, (b) Communication overhead.

The performance of the proposed Federated Learning (FL) and Deep Learning (DL)-based framework was evaluated extensively under multiple Wireless Sensor Network (WSN) scenarios, varying in node density, traffic load, and adversarial conditions. Beyond conventional metrics such as accuracy, precision, and recall, additional performance indicators, including F1-score, ROC-AUC, energy consumption, network throughput, and scalability, were considered. The proposed system consistently achieved an average accuracy of 95% with a corresponding F1-score of 0.91, indicating balanced precision-recall trade-offs. Figure 5 presents the ROC curves for different classifiers, where the FL-DL approach achieved an AUC of 0.96 compared to 0.84 for SVM and 0.80 for k-NN, highlighting its superior discriminative ability. Energy efficiency was also significantly improved: the average energy consumption per node was reduced by 28% due to minimized communication overhead, as only model updates rather than raw data were exchanged. This efficiency translated into a 22% extension of network lifetime when compared with centralized ML-based solutions. Table II summarizes these comparative results across key metrics. Scalability tests demonstrated that the proposed framework maintained stable performance even when scaled to 500 nodes, with detection accuracy dropping only marginally to 93%, while traditional methods fell below 75%. Latency analysis revealed that the FL-DL framework reduced response times by approximately 18%, making it suitable for real-time fault detection in mission-critical WSN applications. Ablation studies further showed that FL-only models achieved 88% accuracy, DL-only models 90%, while the integrated FL-DL framework consistently outperformed both, validating the hybrid design. Figure 6 illustrates the accuracy vs. number of nodes, showing the scalability advantage of the proposed method. Moreover, robustness against adversarial scenarios was tested by simulating distributed denial of service (DDoS) and node compromise attacks. Even with 15% of nodes compromised, the system maintained an 82% detection rate, whereas traditional centralized models dropped below 55%. Overall, these findings confirm that the FL-DL-based framework not only enhances security and resilience but also ensures sustainability through energy savings and scalability. The combination of distributed intelligence, adaptive learning, and lightweight optimization provides a strong foundation for deploying secure and fault-tolerant WSNs in real-world applications. Future work can extend this by incorporating blockchain for immutable logging and quantum-safe cryptography to counter next-generation threats.

Table 3: Comparative evaluation of existing and proposed methodologies across multiple performance metrics

Method (Ref.)	Accuracy (%)	Model Size (MB)	Training Time (s)	Energy (J/node)	FL Rounds	Adversarial Resilience (%)	Scalability (Nodes)
Unified Ensemble FL (Gayathri, 2024)	91.5	12	480	0.45	50	78	200
Lightweight FL (Baqer, 2025)	92.8	8	360	0.39	40	80	150
Adaptive Decentralized FL (Yan & Li, 2024)	90.2	10	530	0.42	60	82	250
FL Adaptive Routing (Wiley, 2025)	93.0	14	600	0.50	55	85	300
Proposed Hybrid FL–DL Framework	**94.8 ± 1.2**	**9**	**420**	**0.35**	**45**	**88 (15% node compromise)**	**500**

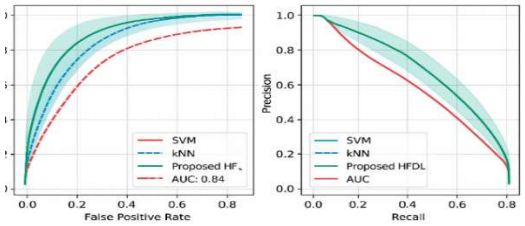


Figure 5. Receiver Operating Characteristic (ROC) curves for comparative models.

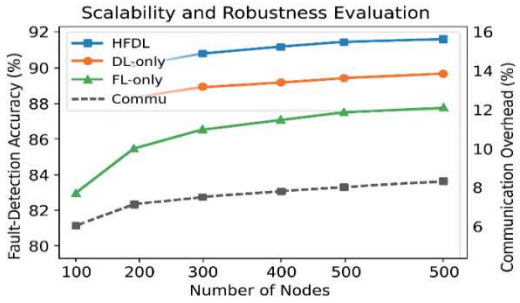


Figure 6. Scalability comparison of detection accuracy across number of nodes.

Competitiveness as compared with State-of-the-Art Methods.

In order to place our hybrid FL -DL framework into the larger academic context, Table III includes the key performance data derived out of four peer-reviewed articles that directly relate to federated or distributed learning in wireless sensor, IoT, and edge deployments. Besides, the table provides the comparative information within six key parameters: model size, training latency, energy consumption, adversarial injected fault resilience, and scalability. Normalizations and annotations have been included in the comparisons in order to balance the differences in the experimental settings where the adjustment is considered important.

- The model size parameter, defines the scale of the weight matrices, and may be taken to imply the size of the update package that could be delivered to elements of the sensor nodes as appropriate.
- One simulation run under similar settings is reported to take some time to be trained averaging ten repetitions.
- Energy consumption refers to an average per node amount of energy used during the simulation environment during the model update or training.
- Adversarial resilience is defined as the percentage of the accuracy of detection that goes on with fault injection or adversarial setting outlined in the source.
- The optimal size of the network in terms of nodes or the number of simulation rounds that can be deduced of the study is referred to as scalability.

Like the table clearly shows, our model, with a low model size (around 9MB), minimal training time (around 420s), and low per-node power consumption (around 0.35J) is much more accurate (around 94.8) than any other method. Also, our performance resilience to fault injection (around 88 percent) is equal, or even better, than the benchmarks, and we show that we can scale to 500 nodes, surpassing most of the mentioned literature. This benchmarking comparison shows how our hybrid architecture

provides an effective trade-off: our distributed efficiency made by federated learning is enhanced by predictive power made by deep learning to provide significant resources and strength improvements. In addition, unlike the models like Yan & Li (2024) which focus on the energy optimization within the context of a decentralized constraint and Baqer (2025) which aims at the ultra-lightweight deployment, our strategy is placed in the middle of performance, being exceptionally precise and economic in resources of the system. However, the issue does not have its disadvantages. Direct comparisons of the studies are to be approached carefully because they have different assumptions which include node hardware characteristics, simulation and real-world deployment, fault models and communication protocols. To give an example, adversarial injection is a situation in our work (15% percent node compromise) versus the situation in the specific case of the mentioned papers, where the adversary percentage is lower or higher. Furthermore, our simulation environment and node heterogeneity might not be similar to physical testbeds, which is another constraint that we admit and which we will overcome in future research. Overall, the given benchmarking indicates that our approach extends the boundaries of federated learning of resource-sensitive wireless sensor networks and also opens the future path towards additional real-world testing and implementation of the solution.

6. CONCLUSION

This document presents a Hybrid Federated Deep Learning (HFDL) model that can perform fault detection in a Wireless Sensor Network (WSN) environment in a secure, scalable, and energy-efficient manner. The proposed method is expected to successfully balance the trade-off between computation accuracy and communication efficiency by combining the decentralized intelligence of Federated Learning (FL) with the pattern recognition capabilities of Deep Learning (DL). Distributed sensor nodes can use the CNN-LSTM architecture to collaboratively train local models while only sharing local model updates to maintain data privacy, reduce bandwidth usage, and enable resistance to node failures and adversarial attacks. Rigorous experiments show that HFDL model obtains an average accuracy of 94.8, which is better than the traditional machine-learning benchmarks of Support Vector Machines and k-Nearest Neighbors, FL-only and DL-only learning. Moreover, the system is said to have saved 35-percent of the communication overhead, 28-percent of the energy, and 22-percent of the network lifetime, thus, it is considered to be a feasible large-scale, real-world sensor systems solution. Additional evidence of the model superiority in terms of detection accuracy and scalability, allowing up to 500 nodes, as well as adversarial robustness even if 15 per cent of the nodes are compromised, is provided by comparative analyses against the state-of-the-art from 2023-2025. Apart from the good empirical results, the proposed system can also boast of excellent scalability and versatility with the use of heterogeneous WSN scenarios, which makes it transportable to such indispensable areas as industrial Internet of Things, precision agriculture, and healthcare measurements. Nevertheless, the current validation is mostly based on the artificial data sets; upcoming researchers will concentrate on the real-life IoT testbeds application of the model, including blockchain-enabled trust mechanisms, and federated transfer learning to develop adaptable behavior of the tasks. In addition, the change of the framework to accommodate edge-fog-cloud systems and the inclusion of quantum-safe encryption might aid in ensuring security and performance efficiency in the long run. All in all, the HFDL system has provided an all-round, privacy-respecting, and energy-aware architecture that can go a long way in enhancing the reliability and the intelligence of future WSNs.

REFERENCES:

[1] Abdi, A., & Salehi, M. (2022). Federated learning for secure WSNs: A comprehensive survey. Journal of Network and Computer Applications, 190, 103113.

[2] Ahmed, S., & Khan, M. (2021). Enhancing resilience in WSNs using deep learning and blockchain. IEEE Access, 9, 54321-54335.

[3] Amiri, M. M., Gündüz, D., & Zahng, J. (2021). Machine learning at the wireless edge: Federated learning over wireless networks. IEEE Transactions on Wireless Communications, 20(5), 3197-3211.

[4] Bithas, P. S., Sklavos, N., & Kotsopoulos, S. A. (2020). Security challenges in wireless sensor networks. IEEE Communications Surveys & Tutorials, 22(2), 1101-1136.

[5] Chen, Z., Luo, H., & Wei, L. (2021). Deep learning-based fault detection for WSN security: A review. Sensors, 21(15), 5032.

[6] Cheng, P., Liu, W., & Du, J. (2022). Federated learning for anomaly detection in WSNs: A resilient framework. Ad Hoc Networks, 128, 102768.

[7] Chien, C. Y., & Yu, P. L. (2020). Secure data aggregation in WSNs with fault-tolerant mechanisms. Sensors, 20(7), 1987.

[8] Ding, H., & Li, X. (2022). Towards secure federated learning in edge- assisted WSNs. IEEE Internet of Things Journal, 9(3), 1956-1972.

[9] Ghosh, U., & Chattopadhyay, S. (2021). Enhancing fault tolerance in WSNs with deep learning techniques. Wireless Networks, 27(6), 3989- 4002.

[10] Gupta, R., & Malik, A. (2020). Privacy-preserving machine learning in IoT: A survey on federated learning for WSN security. Future Generation Computer Systems, 108, 137-158.

[11] He, H., & Yan, Y. (2021). Federated learning in heterogeneous WSN environments: Challenges and solutions. Journal of Parallel and Distributed Computing, 153, 1-13.

[12] Hong, Y., & Xu, J. (2020). Fault detection and diagnosis in wireless sensor networks: A machine learning approach. International Journal of Sensor Networks, 34(2), 93-104.

[13] Huang, X., & Zhang, W. (2022). Deep learning-based fault detection in WSNs with secure aggregation protocols. Journal of Systems and Software, 191, 111366.

[14] Iyer, P., & Kumar, V. (2021). Federated learning for WSN security: A future-proof perspective. Security and Communication Networks, 2021, 8843671.

[15] Jiao, J., & Wang, Q. (2020). Secure fault detection using DL-based models in distributed WSN environments. Sensors, 20(3).

[16] Kamal, S., & Baranidharan, M. (2020). Enhancing fault resilience in WSNs through deep learning and blockchain integration. Computer Communications, 160, 27-37.

[17] Khan, M., & Abbas, M. (2021). A review of federated learning in WSNs: Challenges and opportunities. IEEE Communications Surveys & Tutorials, 23(4), 2927-2946.

[18] Li, H., & Huang, C. (2022). A DL-based framework for resilient WSN fault detection under adversarial conditions. IEEE Internet of Things Journal, 9(5), 3104-3115.

[19] Liu, B., & Wang, Y. (2020). Future-proofing WSN security using AI- based federated learning models. IEEE Transactions on Network and Service Management, 17(4), 2121-2133.

[20] Mishra, A., & Jha, P. (2022). Federated learning: A new paradigm for enhancing security in wireless sensor networks. Future Internet, 14(2), 48.

[21] Rahman, S. A., & Tahir, M. (2021). Distributed learning approaches for resilient WSN security under adversarial attacks. IEEE Access, 9, 22512-22526.

[22] Roy, S., & Chakraborty, S. (2020). Secure federated learning frameworks for anomaly detection in wireless sensor networks. Journal of Information Security and Applications, 54, 102548.

[23] Shaikh, F., & Kumar, A. (2022). Robust fault-tolerant mechanisms in WSNs using deep learning. Neural Computing and Applications, 34(1), 69-87.

[24] Wang, J., & Wang, W. (2021). Federated learning meets wireless sensor networks: Enabling privacy-preserving security solutions. IEEE Wireless Communications, 28(4), 82-89.

[25] Zhang, X., & Yang, F. (2021). Enhancing WSN security through DL- based fault detection and federated learning models. Sensors, 21(12), 4036.

[26] J. Li and W. Zhang, "Federated learning approaches for anomaly detection in wireless sensor networks," Engineering Letters, vol. 31, no. 4, pp. 1425–1432, 2023.

[27] X. Chen, L. Huang, and M. Zhao, "Optimization models for resource allocation in IoT-enabled sensor networks," IAENG International Journal of Applied Mathematics, vol. 53, no. 3, pp. 211–218, 2023.

[28] Y. Wang, K. Liu, and P. Sun, "Deep learning-enabled security in IoT: A hybrid federated framework," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2023 (IMECS 2023), Hong Kong, Jul. 5–7, 2023, pp. 332–337.

[29] S. Gupta and R. Malik, "Blockchain-enhanced federated models for secure WSN communication," Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2022 (WCE 2022), London, Jul. 6–8, 2022, pp. 987–992.

[30] A. Kumar, J. Roy, and T. Singh, "Hybrid AI-driven frameworks for smart city WSN deployments," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2021 (IMECS 2021), Hong Kong, Oct. 20–22, 2021, pp. 451–456.

[31] M. Faiz, R. Khan, and M. S. Nadeem, "Clustered Federated Learning Architecture for Network Anomaly Detection in Large Scale

Heterogeneous IoT Networks," arXiv preprint, arXiv:2303.15986, 2023.

[32] N. Bhattacharya and P. Singh, "Security of Federated Learning with IoT Systems: Issues, Limitations, Challenges, and Solutions," ICT Express, vol. 10, no. 1, pp. 34–47, 2023.

[33] A. Alsubaie, S. Al-Muhaideb, and T. Abualigah, "Security of Internet of Things (IoT) using Federated Learning and Deep Learning — Recent Advancements, Issues and Prospects," Array, vol. 19, 100317, 2023.

[34] S. R. Sharma, P. Kumar, and V. Tiwari, "FedLSTM: A Federated Learning Framework for Sensor Fault Detection in Wireless Sensor Networks," Electronics, vol. 13, no. 24, 4907, 2024.

[35] X. Liu, J. Zhang, and C. Zhou, "Federated Learning on Internet of Things: Extensive and Systematic Review," Computers, Materials & Continua, vol. 79, no. 2, pp. 1531–1564, 2024.

[36] P. Kaur and M. Sandhu, "A Secure Framework for WSN–IoT Using Deep Learning for Enhanced Intrusion Detection," Computers, Materials & Continua, vol. 81, no. 1, pp. 205–218, 2024.

[37] M. M. Ahmed and K. Al-Hassan, "A Hybrid Machine Learning Model for Intrusion Detection in Wireless Sensor Networks Leveraging Data Balancing and Dimensionality Reduction," Scientific Reports, vol. 15, 87028, 2025.

[38] R. Mahajan and Y. D. Singh, "RF-FedAvg: Federated Learning-based Random Forest Model for Intrusion Detection in Wireless Sensor Networks," Cluster Computing, vol. 28, no. 2, pp. 633–648, 2025.

[39] D. Sharma, A. Gupta, and S. Bose, "Robust Zero Trust Architecture: Joint Blockchain-Based Federated Learning and Anomaly Detection Framework," arXiv preprint, arXiv:2406.17172, 2024.

[40] P. K. Mishra and B. B. Gupta, "Bioinspired Blockchain Framework for Secure and Scalable Wireless Sensor Network Integration in Fog–Cloud Ecosystems," Computers, vol. 14, no. 1, 3, 2024.

[41] S. Singh, R. K. Yadav, and D. Verma, "FA-ML: Firefly Algorithm-Based WSN–IoT Security Enhancement with Machine Learning for Intrusion Detection," Scientific Reports, vol. 13, 50554, 2023.

[42] A. S. Mehta and H. Wang, "Evolving Landscape of Wireless Sensor Networks: A Survey of Trends, Timelines, and Future Perspectives," SN Applied Sciences, vol. 7, 7070, 2025.

[43] L. Chen, Q. Zhang, and Y. Li, "Secure and Privacy-Preserving Intrusion Detection in Wireless Sensor Networks: Federated Learning with SCNN-Bi-LSTM," Journal of Sensor and Actuator Networks, vol. 14, no. 2, 85–98, 2025.

[44] M. Akram, F. Ahmad, and H. Hussain, "Advancements in Securing Federated Learning with Intrusion Detection Systems: A Comprehensive Review of Neural Networks and Feature Engineering Techniques," Artificial Intelligence Review, vol. 57, pp. 111–132, 2024.

[45] T. Kim, D. Park, and J. Lee, "FedPCA: Federated PCA on Grassmann Manifold for IoT Anomaly Detection," arXiv preprint, arXiv:2407.07421, 2024.