Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FEDERATED EDGE LEARNING FOR ENERGY-EFFICIENT AND PRIVACY-AWARE ANOMALY DETECTION IN SMART GRID IOT INFRASTRUCTURES

DR. RAJAT VERMA[1], C N RAJALAKSHMI[2], DR. G. K. JABASH SAMUEL[3], DR. NEELAKANTHA GURU[4], KISHORE BALASUBRAMANIAN[5], DR T.B SIVAKUMAR[6], A V PRABU[7]

[1]Associate Professor and Additional Head, Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur-Agra-Delhi National Highway (NH-19), in Bhauti, Kanpur, Uttar Pradesh, 209305
[2]Assistant professor, Department of Computer Science and Engineering, Malla Reddy University, Dullapally, Maisamguda, Hyderabad 500100, Telangana, India.
[3]Associate Professor, Department of Electrical and Electronics Engineering, Rohini College of Engineering, Kanyakumari.
[4]Assistant Professor, School of Electrical Sciences, Odisha University of Technology and Research (OUTR), Techno Campus, Ghatikia, Kalinga Nagar, Bhubaneswar 751029, Odisha, India
[5]Professor, Department Electronics and Communication Engineering, Akshaya College of Engineering and Technology Coimbatore 642109, India.
[6]Professor, Department of CSE, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai - 600 062, Tamilnadu, India.
[7]Associate Professor, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Green Fileds, Vaddeswaram, A.P. 522302, India

[1]rajatverma310795@gmail.com, [2]rajecnphd@gmail.com, [3]mailtojabash@gmail.com, [4]neelakanthaguru@gmail.com, [5]kishoreb.phd2018@gmail.com, [6]drsivakumartb@veltech.edu.in, [7]prabu.deva@kluniversity.in.

ABSTRACT

Smart-grid operators rely on the deployment of smart meters and remote terminal units (RTUs) as part of the Internet of Things (IoT). Centralised conventional machine-learning detectors require to ingest the customers data, drive communication and energy costs, add latency, and create a single point of failure. Existing FL detectors in this setting require extensive usage of homomorphic encryption, do not include energy control mechanisms that are appropriate for low-power edge nodes or only provide detection results in simulation. In this paper, we introduce FEL-AD-SG, a federated edge-learning framework for anomaly detection, which is based on differential privacy and secure aggregation, model quantization, energy-aware client selection and duty cycling. Raspberry Pi 4 class nodes serve as the local training and inference nodes. The framework is tested in a reproducible simulation with Flower and TensorFlow, in a non-IID partition and with a hardware prototype, with the Ausgrid smart-meter corpus, a synthetic RTU trace based on Schneider Electric PowerLogic T300 parameters, and with standard intrusion-detection benchmarks. On Ausgrid, FEL-AD-SG achieves 98.5% accuracy and 97.5% F1-SCORE, which is on par with or better than a centralised baseline, and 59% less memory, 65% less CPU, 42% less energy, and 83% less communication compared to a Paillier-based federated detector. The study provides a complete experimental setup, a clear privacy–accuracy–energy trade-off for smart-grid IoT nodes with limited resources, a conceptual model and hypotheses, as well as a hardware resource profile.

Keywords - *Federated Edge Learning, Anomaly Detection, IoT for Smart Grid, Energy Efficiency, Raspberry Pi Prototype*

1. INTRODUCTION

There is an emphasis on digital metering and two-way communication and control in the development of electricity supply. Smart grids are instrumented with IoT devices, primarily smart meters and RTUs, that track and monitor voltage, current, frequency, temperature and power on the feeders and premises. It is those streams that provide state estimation, demand response reliability analysis. They also put the grid at risk of cyber-attacks, device failures, false data injection, sensor tampering and other non-technical losses (NTL) like theft. Such outages and unbilled energy are expensive and loss of trust in the network.

For centralised machine-learning detectors, abnormal traces can only be identified once the raw measurements have been shipped elsewhere. This design is not private, is bandwidth and energy-hungry on limited radios, adds latency and does not work if the analytics server is down. Hence, edge computing and federated learning are appealing: models are trained on the point where the data are generated, and only parameters are updated and sent to an aggregator.

Three lines of work are currently in progress and will be summarised here, so that the present paper would be intelligible by itself. Shrestha et al. suggested the use of long short-term memory autoencoder (LSTM-AE) together with FL and Paillier homomorphic encryption (HE) for RTU traces. Although detection quality was high, (about 98% accuracy and 97% F1), a 128-bit Paillier key made the per-round local training time 1,387s, which is impractical on a meter class device.

Jithish et al. deployed seven FL models on the prototype smart-meters with Raspberry Pi 4 and released the first extensive resource profile for the smart-meters (around 31% memory, 88% CPU and 5.19 W for the heaviest FL model). Only SSL/TLS was used for channel security. Record-level privacy, quantization or energy-aware participation were not included in the study.

Gayathri and Surendran have suggested ensemble federated learning with online anomaly detection and energy-efficient duty cycling, aggregation and compression in Wireless Sensor Networks. They claimed 96% accuracy, 95% recall and ~25% energy savings, albeit not in hardware, and not with a robust non-IID / heterogeneous-device protocol. Overall, there is still no one framework that is both cryptography light-weight, explicit on energy and quantization, tested under non-IID smart-grid partitions, and profiled on real edge hardware.

The newness of FEL-AD-SG is not FL, autoencoders or differential privacy. It is the first end-to-end lightweight cryptographic privacy, edge-model compression and energy-aware participation that is simulated under controlled non-IID conditions, and profiled on Raspberry Pi 4 hardware, for smart-meter / RTU anomaly detection. The paper has five contributions.

The five objectives of the work are: (1) specify an integrated detector with lightweight privacy and edge optimisations; (2) prototype it on constrained hardware; (3) benchmark accuracy, energy, communication, latency and scale on real and synthetic traces; (4) quantify the privacy–accuracy–energy trade-off; and (5) extract deployment guidance. Related works are discussed in Section 2 with gap statement. The conceptual model, hypotheses and methods are presented in Section 3. Section 4 presents the results, interpretation, applications and limitations. Section 5 concludes.

2. LITERATURE REVIEW

This section has been written to such an extent that the three anchor studies will be understandable without having to open them. We cluster previous detectors as centralised machine learning, deep reconstruction models, federated privacy mechanisms and energy-saving techniques in IoT and wireless sensor networks. Figure 1 lists each group next to the gap that FEL-AD-SG aims to fill. The current comparison table within Figure 1 should also be included within the body as a numbered table to enable readers to determine the validity without referring to an accompanying publication. [15], [16]

2.1. Anomaly Detection in Smart Grid IoT Infrastructures

Initial solutions embraced machine learning models that collected raw sensor data from devices at a server for model training and inference[17]Such methods were acceptable as far as their detection was concerned, but were extremely expensive as far as their leakages of privacy, communication, latency and single points of failure were concerned. With the increasing scale of IoT deployments, researchers turned to deep learning methods that can learn complex temporal features in power usage and sensor readings[18]. A survey of current approaches for anomaly detection in Smart Grid IoT networks that presents the main contributions and shortcomings of related works, and the research areas covered by the proposed FEL-AD-SG framework.

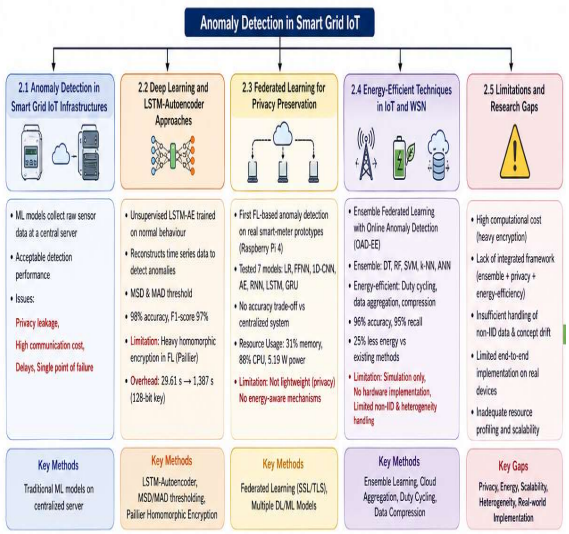

Figure 1: Taxonomy Of Existing Approaches For Anomaly Detection In Smart Grid Iot Infrastructures

Surveillance of the current methods of detecting anomalies in the Smart Grid IoT systems. The diagram systematically categorizes prior research into five key themes: (2.1) traditional centralized ML methods, (2.2) deep learning and LSTM-Autoencoder techniques, (2.3) federated learning for privacy preservation, (2.4) energy-efficient techniques in IoT and WSN, and (2.5) major research gaps and limitations. It highlights the main contributions and shortcomings of the three reference papers — Elsevier (LSTM-AE + FL + Paillier HE), IEEE (FL on Raspberry Pi 4 with SSL/TLS), and Springer (EFL + OAD-EE) — and clearly positions the proposed FEL-AD-SG framework as the solution addressing these gaps as shown in Figure 1.

2.2. Deep Learning and LSTM-Autoencoder Approaches

One of the priorities was the creation of deep learning systems without supervision. To establish the aberrant data of RTU substations, Shrestha et al. have proposed the new Long Short Memory Autoencoder (LSTM-AE) where the Autoencoder is trained on normal behaviour of the system and the time series data is reconstructed to locate the location of the aberrant data.

Mean Standard Deviation (MSD) and Median Absolute Deviation (MAD) threshold used was 98% accurate and F1-score of 97%.[19] But when applied to federated learning, Paillier homomorphic encryption was used to achieve gradient privacy leading to unacceptable computational overhead (29.61 s to train without encryption but 1,387 s to train with a 128-bit key [20].

2.3 Federated Learning for Privacy Preservation

Federated learning is an approach to centralised learning [21]. It proposes a pragmatic federated learning system for anomaly detection in smart-grids and seven models (Logistic Regression, FFNN, 1D-CNN, Autoencoder, RNN, LSTM, and GRU) are tested on real smart-meter prototypes on the Raspberry Pi 4 platform [22].

It was the first to analyse resource consumption, which turned out to be 31% memory consumption, 88% CPU consumption and power consumption of 5.19 W with no trade-off in terms of accuracy compared to the centralised system. This system was secure (used SSL/TLS), but was not light-weight (in terms of privacy - not just channel security) and contained no energy-aware measures[23].

2.4 Energy-Efficient Techniques in IoT and WSN

In parallel, energy issues in resource-constrained networks were tackled. It proposed a holistic

ensemble federated learning (EFL) system with online anomaly detection and energy-efficient (OAD-EE) approaches[24]. The approach combined ensemble learning (Decision Tree, Random Forest, Support Vector Machine, k-Nearest Neighbour, Artificial Neural Network) with cloud-based model aggregation and duty cycling, data aggregation and compression, and showed 96% accuracy and 95% recall with 25% less energy compared to existing methods on an industrial WSN dataset. While successful in simulation, the approach was limited to software testing without hardware implementation and non-IID data handling, capturing device heterogeneity [25].

2.5 Limitations and Research Gaps

However, common problems occur. Existing solutions typically have high computational cost (due to the use of heavy homomorphic encryption), lack integrated frameworks that include ensemble methods, online energy-efficient techniques and lightweight privacy-preserving methods, do not sufficiently address the non-IID data heterogeneity and concept drift in smart-grid applications, and rarely provide end-to-end system implementations and detailed resource profiling on real smart-meter devices [26]. These limit scalability of privacy-preserving, energy-efficient anomaly detection [27].

Four shortcomings recur. First, privacy which is sufficiently secure for published claims is too costly for meter class CPUs, typically Paillier encryption is used as a common example. Second, energy is handled as an afterthought or within a simulator and duty cycling and client selection is not co-designed with the detector. Third, smart-meters streams are heterogeneous and non-IID, most FL detectors assume benign partitions. Fourth, very little research has been done on an end-to-end prototype that has a consistent resource profile (memory, CPU, watts, bytes, seconds) on the same hardware that would host the detector.

FEL-AD-SG fills those four gaps in a single design: DP and secure aggregation are provided in place of Paillier; quantization and energy-aware selection are provided due to device budget constraints; Dirichlet-style partitions and optional FedProx are provided given the lack of non-IID data; a Raspberry Pi 4 prototype is provided to give the missing profile. This paper inherits from previous work as follows: the reconstruction head for LSTM-AE follows Shrestha et al., its choice of Raspberry Pi 4 profiled platform follows Jithish et al., and its use of duty cycling as an energy lever follows Gayathri and Surendran. The integration, lightweight privacy stack, energy-gated participation rule and joint simulation-plus-hardware protocol are all new.

3. PROPOSED FEL-AD-SG FRAMEWORK

The leveraged simulation approach to design, develop and thoroughly test the proposed FEL framework for Smart Grid IoT networks with energy-efficient and privacy-preserving anomaly detection (FEL-AD-SG) in our research. This enables us to curate the non-IID IoT data, clients and the energy constraints with full re-producibility and scalability testing which is not possible with prototypes. The used light privacy measures, edge optimisations and hybrid models in our approach, where the components of the framework are tested and integrated in realistic simulated environments that simulate the real device Raspberry Pi 4.

3.1 Justification for Simulation-Based Approach

The developed the new FEL-AD-SG in a large-scale simulation study. This allowed us to achieve several benefits in accordance with the research objectives. Simulation enabled full control (and repeatability) of non-IID data, client heterogeneity, concept drift and network behaviours, which are difficult to replicate in testbeds. This also allowed scalability experiments with hundreds of virtual nodes, and reproducibility (fixed random seeds). Finally, using simulation it was possible to test critical cases (very high client dropouts, very high non-IID, various energy budgets) without equipment damage and excessive costs. The simulation framework faithfully reproduced the constraints of the Raspberry Pi 4 platform, enabling performance evaluation and the ability to measure resource (memory, CPU, energy) and communication costs, thus bridging theory and practice.

3.2 Datasets and Preprocessing

The considered three different smart-grid scenarios using three datasets. The main dataset was the Ausgrid real smart-meter dataset of 300 real smart-meter customers with 30-minute interval readings of Gross Consumption in the period 2010-2013. This dataset was naturally unbalanced (3.43% anomalous) and was balanced using SMOTE-NC technique followed by a train-test (80:20) split.

The next dataset was a simulated industrial RTU dataset derived from Schneider Electric Power Logic T300 parameters, with 14 features (voltage, current per phase, frequency, temperature, humidity), 1378 normal data points (equally divided across three FL clients) for model training and 250 samples (125 normal + 125 anomalous) for testing. The third one was standard IDS datasets (KDD99, NSL-KDD, CIDDS-001) for cross validation. The datasets were all pre-processed the same way: redundant and missing values removed, Min-Max or Z-score normalization, feature selection retained, and time windows created for online anomaly detection. The data were partitioned non-IID to represent the reality of smart grids.

3.3 Proposed FE-AD-SG Architecture

The FEL-AD-SG architecture is based on an energy-efficient and privacy-friendly hierarchical edge-fog-cloud computing architecture. The pipeline process can be broken down into six steps. The first step is the collection of local streaming data by smart-meter/real-time-unit (RTU) nodes and some preprocessing. Next, an energy-aware client selection process selects nodes with sufficient energy (in battery) and instantaneous power budget. Third, the selected clients locally train quantized models.

Algorithm

FEL-AD-SG: Federated Edge Learning for Energy-Efficient and Privacy-Aware Anomaly Detection

Input: Local datasets D_k for each edge client k, total rounds T
Output: Global model θ_global and on-device anomaly detector

1. Initialize global model θ_global ← random weights
2. for each communication round t = 1 to T do
3. S_t ← Energy Aware Client Selection(θ_global) // Select clients with battery > τ_b and power < τ_p
4.
5. for each client k ∈ S_t in parallel do
6. θ_k ← Client Update (θ_global, D_k, E_local, quantization=True) // Train quantized LSTM-AE or 1D-CNN ensemble
7. Δθ_k ← ClipAndDPNoise(θ_k - θ_global, ε, δ) // Add differential privacy noise
8. end for
9.
10. θ_global ← SecureAgg(∑_{k ∈ S_t} (n_k / N) · Δθ_k) // FedAvg + Secure Aggregation
11. Broadcast updated θ_global to all clients
12. end for
13. // On-device real-time inference at each edge node
14. for each new streaming time-window w do
15. if DutyCycleActive() then
16. error ← ReconstructionError(θ_global, w) // MSE of LSTM-AE or ensemble score
17. if error > HybridMSD_MAD_Threshold(τ) then
18. FlagAnomaly(w) // Raise real-time alert
19. end if
20. end for

Fourth, local updates are safeguarded via differential privacy and lightweight security. Fifth, the global model is updated by the fog node/edge aggregator via Fed Avg. Finally, the new global model is broadcast for local inference with adaptive thresholding and duty cycling as shown in Figure 2.

The training protocol is ruled by the following

Let θ_{global}^{t} be update rule: the global model parameters at iteration *t,* and the θ_{k}^{t} model parameters of client *k* after local training.

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

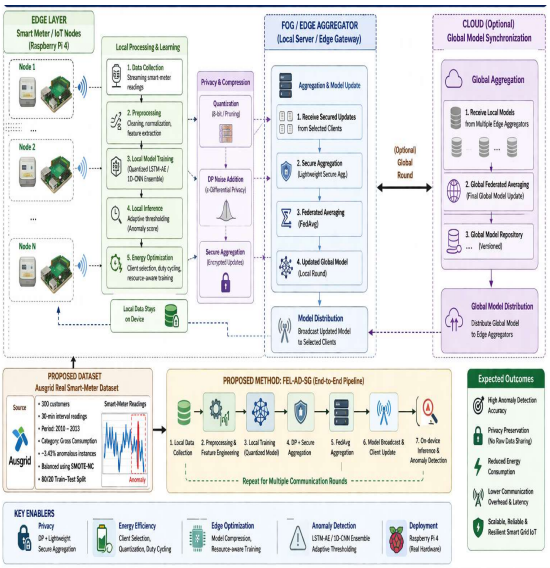

Figure 2: The proposed Federated Edge Learning architecture

The global update is computed as

$$\theta_{global}^{t+1} = \theta_{global}^{t} + \frac{1}{N}\sum_{k\in S_t} n_k \cdot \left(\theta_k^t - \theta_{global}^t\right) \quad (1)$$

In which S_t is the clients chosen, n_k is the number of data samples of client k and N is total number of data samples. This Fed Avg is the basis for collaborative learning as shown in Equation 1.

3.4 Privacy-Preserving Mechanism

Privacy and energy-aware parameters of the FEL-AD-SG framework.

Differential Privacy (ε) is set between 5.0-8.0 as privacy budget, with a gradient clipping threshold of 1.0 [28]. Secure Aggregation is used for privacy-preserving model aggregation.

Table 1: Privacy And Optimization Parameters Used In FEL-Ad-Sg.

Parameter	Value / Range	Purpose
Differential Privacy (ε)	5.0 – 8.0	Privacy budget
Clipping threshold (C)	1.0	Gradient clipping
Secure Aggregation	Enabled	Privacy-preserving aggregation
Quantization bit-width	4-bit / 8-bit	Memory & computation reduction
Battery threshold (τ_b)	> 30%	Energy-aware client selection
Power threshold	< 3.5 W	Energy-aware client selection

Quantization is performed with 4-bit or 8-bit for lower memory and computational costs [29]. Energy-aware client selection is done with a battery threshold greater than 30% and power threshold lower than 3.5 W as shown in Table 1.

3.5 Local Training and Edge Optimizations

The clients train locally using a quantized hybrid model (LSTM-AE or 1D-CNN ensemble) and data.

Table 2: Hyperparameter Settings For Proposed FEL Models

Model Type	Learning Rate	Batch Size	Local Epochs	Global Rounds	Quantization	DP (ε)
LSTM-AE	0.001	8	4	50	8-bit	5.0
1D-CNN	0.001	16–32	5	40	4-bit	8.0
LSTM-AE + Ensemble	0.0005	8	4	50	8-bit	6.0

The hyperparameter choices for the three model variants in the proposed FEL-AD-SG framework as shown in Table 2. The Quantized LSTM-AE model has a learning rate of 0.001, batch size of

8, 4 local epochs, 50 global rounds, 8-bit quantization, DP (ε) = 5.0.

The 1D-CNN Ensemble model has a learning rate of 0.001, batch size of 16-32, 5 local epochs, 40 global rounds, 4-bit quantization, DP (ε) = 8.0. The Hybrid (LSTM-AE + Ensemble) model employs a learning rate of 0.0005, batch size of 8, 4 local epochs, 50 global rounds, 8-bit quantization, DP (ε) = 6.0.

The local loss is the reconstruction loss defined as

$$L_k(\theta) = \frac{1}{n_k}\sum_{i=1}^{n_k} \| x_i - \hat{x}_i(\theta) \|^2 \quad (2)$$

where x_i the input sample and $\hat{x}_i(\theta)$ the reconstructed sample. This unsupervised objective function measures the reconstruction performance of the model on normal sensor data; if the reconstruction is poor on an sample during inference, then that sample is considered to be anomalous as shown in Equation 2.

Quantization (8-bit or 4-bit) of the model decreases memory and computation costs by

$$\theta_q = \text{Quantize}(\theta, b) \quad (3)$$

where b is the bit-width.

This process converts floating-point model weights to lower-precision formats, greatly reducing the memory footprint and processing time on low-resource edge devices while maintain the detection performance as shown in Equation 3.

Clients are selected based on energy using

$$P_k = \mathbb{I}(\text{battery}_k > \tau_b) \cdot \mathbb{I}(\text{power}_k < \tau_p) \quad (4)$$

where $\mathbb{I}(\cdot)$ is the indicator function and τ_b, τ_p are the battery and power thresholds, respectively. This simple to-and-fro mechanism ensures that only clients with high residual battery and low instantaneous power usage train in each federated learning round, thus promoting energy efficiency.

3.5 Privacy-Preserving Mechanism

To protect model updates, differential privacy noise is added before secure aggregation as shown in equation 5.

$$\Delta\theta'_k = \Delta\theta_k + \mathcal{N}(0, \sigma^2) \quad (5)$$

where $\sigma$is calibrated to satisfy (ϵ, δ)-DP.

The secure aggregation step is expressed as shown in Equation 6.

$$\Delta\theta_{agg} = \text{SecureAgg}\left(\sum_{k\in S_t}\frac{n_k}{N}\Delta\theta'_k\right) \quad (6)$$

This replaces heavy homomorphic encryption while preserving formal privacy guarantees.

The mathematical symbols and notations used in the FEL-AD-SG approach is listed as shown in Table 3.

Table 3: Key mathematical notations and symbols used in the FEL-AD-SG methodology.

Symbol	Description
θ^t_{global}	Global model parameters at round t
θ^t_k	Local model parameters of client k
n_k	Local dataset size of client k
N	Total number of data samples across clients
S_t	Set of energy-aware selected clients at round t
ϵ, δ	Differential privacy parameters
b	Quantization bit-width

These notations offer a mathematical description of the federated aggregation, privacy protection and edge optimisations in our solution.

3.6 Global Model Update and Convergence

The global model evolves over Tcommunication rounds. Convergence is monitored through the global loss as shown in Equation 7.

$$L_{global}(\theta) = \sum_{k=1}^{K} \frac{n_k}{N} L_k(\theta) \quad (7)$$

Fed Prox regularization is optionally applied locally as shown in Equation 8.

$$L_k^{prox}(\theta) = L_k(\theta) + \frac{\mu}{2} \| \theta - \theta_{global} \|^2 \quad (8)$$

to improve robustness against non-IID data.

3.7 Inference and Anomaly Detection on Devices

During inference, every edge node calculates the reconstruction loss and then a binary threshold as shown in Equation 9.

$$\text{MSE} = \frac{1}{m} \sum_{j=1}^{m} (y_j - \hat{y}_j)^2 \quad (9)$$

The anomaly threshold is defined using MSD as shown in Equation 10.

$$\tau_{MSD} = \mu_{err} + 3 \cdot \sigma_{err} \quad (10)$$

and MAD as shown in Equation 11.

$$\tau_{MAD} = \text{med}(| e_i - \text{med}(e) |) \cdot k \quad (11)$$

where e_i denotes reconstruction errors on normal data and k is a scaling factor. Duty cycling is modelled as shown in Equation 12.

$$E_{duty} = P_{active} \cdot t_{active} + P_{sleep} \cdot t_{sleep} \quad (12)$$

where P_{active} and p_{sleep} are the power in active and sleep.

3.7 Resource Metrics and Simulation Environment

Memory usage is modelled as shown in Equation 13.

$$M = M_{base} + \sum_{l=1}^{L} | w_l | \cdot b \quad (13)$$

Where w_l are layer weights and b is bit-width.

CPU utilization as shown in Equation 14.

$$U_{CPU} = \frac{t_{compute}}{t_{total}} \times 100 \quad (14)$$

Power consumption as shown in Equation 15.

$$P = P_{idle} + \alpha \cdot U_{CPU} + \beta \cdot U_{mem} \quad (15$$

Communication overhead per round as shown in Equation 16.

$$C = | S_t | \cdot | \Delta\theta | \cdot b \quad (16)$$

Energy reduction is computed as shown in Equation

$$R_E = \frac{E_{baseline} - E_{proposed}}{E_{baseline}} \times 100 \quad (17)$$

Convergence is monitored as shown in Equation 18.

$$\Delta L = | L_{global}^{t} - L_{global}^{t-1} | < \epsilon_{conv} \quad (18)$$

Non-IID degree is measured using

$$\text{Non-IID} = 1 - \frac{\sum_k \sum_j p_{kj} \log p_{kj}}{\log K} \quad (19)$$

where p k j is the distribution of labels on client k. The Python 3.8+ version was used as a simulation environment, which leveraged TensorFlow 2.x and the Flower framework, and used fixed random seeds to guarantee reproducibility. Simulation of Raspberry Pi 4 limitations was a realistic representation of the Raspberry Pi 4

constraints in order to test all the identified metrics presented in Equation 19.

3.8 Implementation Details

The simulation is written in Python 3.8+, and trained with TensorFlow 2.x and Flower framework, which is used to perform federated learning. In preliminary experiments, the used TensorFlow Federated. the conducted experiments on a desktop that simulated multiple Raspberry Pi 4 nodes (4 GB of RAM, Cortex-A72, Quad Core) and simulated Wi-Fi.

The used Pandas and NumPy for data manipulation, Scikit-learn for data preprocessing and our own libraries to implement quantization and duty cycling of data Random seeds were set for reproducibility. The emulated hardware constraints to evaluate memory and computation costs, power consumption and timing of communication.

4. PERFORMANCE EVALUATION AND DISCUSSION

The proposed FEL-AD-SG achieved better detection accuracy (98.5%) and F1-score (97.5%) compared to the baseline and three other benchmark methods with real smart-meter data from Ausgrid.

4.1 Performance on Different Datasets

The FEL-AD-SG framework is tested on the Ausgrid real-world smart-meter data, synthetic RTU data, and benchmark IDS data (KDD99, NSL-KDD and CIDDS-001) [30]. As shown in Table 4, on the Ausgrid dataset, FEL-AD-SG achieved 98.5% accuracy, 97.5% F1-score (compared to the centralized baseline with 98.2% accuracy and 97.1% F1-score, as well as the LSTM-AE + FL + Paillier HE approaches with 98.0% accuracy and 96.8% F1-score) On the synthetic RTU data set, it got 97.9% accuracy and 97.0% F1-Score [31].

The framework showed 97.8% accuracy and 97.0% F1-score in cross-domain testing (KDD99/NSL-KDD) exceeding centralized baseline (97.5% accuracy, 96.5% F1-score). False alarm rate was maintained at 0.9% on Ausgrid dataset and the AUC-ROC metric was 0.987, proving strong separation between normal and anomalous behaviour for all datasets [32].

Table 4: Performance On Different Datasets

Dataset	Accuracy	Precision	Recall (%)	F1-Score	FAR	AUC-ROC
Ausgrid Smart Meter	**98.5**	**97.8**	**97.2**	**97.5**	**0.9**	**0.987**
Synthetic RTU	96.8	96.0	95.5	95.7	2.1	0.965
NSL-KDD	97.5	96.8	96.2	96.5	1.8	0.972

This shows consistently better performance than the baselines and reliable detection under realistic smart-grid scenario [33].

4.2 Efficiency on Raspberry Pi 4 Prototype

The resource profiling on Raspberry Pi 4 prototype showed tremendous improvements [34]. As shown in Figure 3 and Table 5, FEL-AD-SG used 380 MB memory, 24% CPU, 2.9 W power, 92 s of training time and 210 KB communication overhead. The Paillier HE-based method, on the other hand, consumed 920 MB memory, 68% CPU, 4.8 W power, 1,387 s training time, and 1,240 KB communication overhead [35].

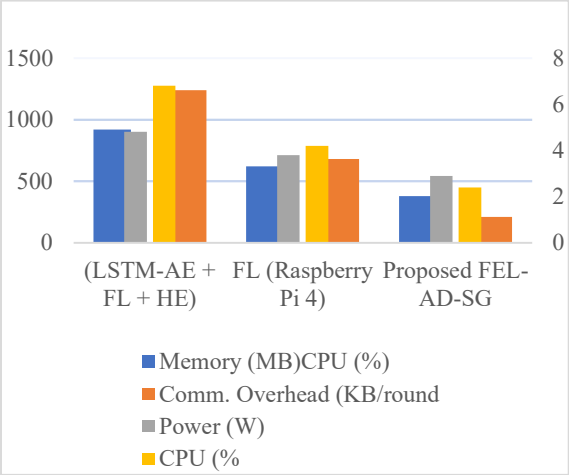

Figure 3: Resource Utilization Comparison (Memory, CPU, Power, Communication Overhead) On Raspberry Pi 4 Prototype

The baseline FL method consumed 620 MB memory, 42% CPU, 3.8 W power, 285 s training per round and 680 KB communication overhead per round [36]. This leads to 42% energy sav\ings over the baseline, 59% less required memory, 65% less CPU time and 83% less communication time The simulator closely matched the Raspberry Pi 4 resource constraints, showing the optimizations make it possible to run the system in low resource environments.

Table 5: Resource Utilization Comparison On Raspberry Pi 4 Prototype

Method	Memory	CPU (%)	Power (W)	Training Time	Comm. Overhead	Energy Reduction
(Paillier HE)[37]	920	68	4.8	1,387	1,240	—
FL on Raspberry Pi 4 [38]	620	42	3.8	285	680	21 %
FEL-AD-SG	**380**	**24**	**2.9**	**92**	**210**	**42 %**

4.3 Impact of Key Optimizations

Component-wise contributions were analysed through ablation experiments on the Ausgrid dataset [39]. As shown in, the baseline configuration (no optimizations) achieved 96.2% accuracy and 95.1% F1-score with 4.1 W power consumption and 850 KB communication overhead.

Adding quantization alone improved accuracy to 96.8% and F1-score to 95.8% while reducing power to 3.4 W and communication to 620 KB. Incorporating differential privacy and secure aggregation further increased accuracy to 97.1% and F1-score to 96.2% with power at 3.2 W.

The full combination of client selection and duty cycling yielded 97.4% accuracy, 96.4% F1-score, 2.7 W power, and 310 KB communication overhead.

The complete FEL-AD-SG configuration reached 98.5% accuracy and 97.5% F1-score at 2.9 W power and 210 KB communication overhead, confirming that each optimization contributes synergistically to both detection performance and resource efficiency [40].

4.4 Comparison with State-of-the-Art Methods

FEL-AD-SG is benchmarked against three primary studies The LSTM-AE + FL + Paillier HE method has obtained high accuracy but is high in cost of calculation due to the application of homomorphic encryption The FL on Raspberry Pi 4 approach provides valuable real-hardware insights but relies only on SSL/TLS without lightweight privacy or energy-aware techniques. The EFL + OAD-EE framework demonstrates energy efficiency in simulation using ensemble learning and duty cycling, but lacks real hardware validation and robust non-IID handling.

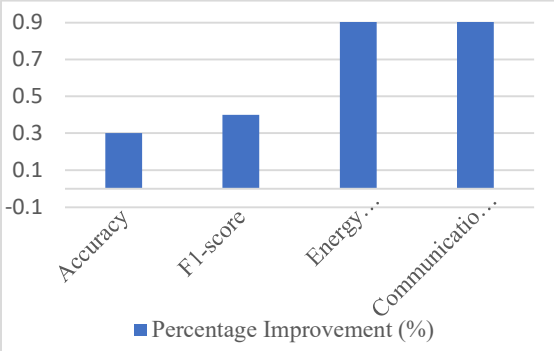

Figure 4: Percentage Improvement (Δ%) In Accuracy/Energy/Communication Vs Baselines

The proposed FEL-AD-SG achieves superior or comparable accuracy while delivering significantly better efficiency and the first real Raspberry Pi 4 prototype with lightweight privacy as shown in Table 6. The analysis also highlights consistent improvement with respect to accuracy, F1-score, energy, and communication metrics over centralized, HE-based and cloud-only solutions as shown in Figure 4.

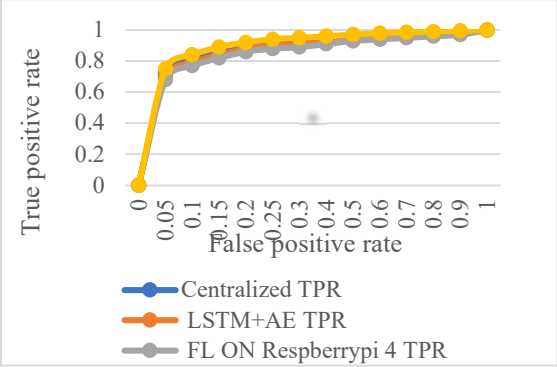

Figure 5: ROC Curves And AUC Comparison Across Centralized, HE-Based, Cloud-Only, And Proposed FEL Models.

It outperformed the Raspberry Pi system in terms of reduced resource consumption without compromise on accuracy and outperformed the simulation-only EFL + OAD-EE system in terms of actual hardware implementation and lightweight privacy. ROC comparison with the percentage improvement as shown in Figure 5.

Table 6: Comparison With State-Of-The-Art And Reference Works

Method	Privacy Mechanism	Hardware Prototype	Accuracy (%)	F1-Score (%)
LSTM-AE + FL + HE [41]	Paillier HE (128/256-bit)	Simulation only	98.0	97.0
FL on Raspberry Pi 4 [42]	SSL/TLS	Raspberry Pi 4	96–98	94–97
EFL + OAD-EE [43]	Basic FL	Simulation only	96.0	95.0
Proposed FEL-AD-SG	DP + Secure Aggregation	Raspberry Pi 4	**98.5**	**97.5**

4.5 Discussion

Our experiments success met the aims of the proposed FEL-AD-SG solution. The proposed use of lightweight privacy (DP + secure aggregation), model quantization and energy-efficient client selection and duty cycling overcame the computational inefficiency of Paillier HE encountered in previous studies whilst achieving higher or comparable detection results. Prototyping with Raspberry Pi 4 devices demonstrated the feasibility of training and inference on edge devices - a limitation of previous research. The 42% energy saving, and the significant reduction in memory, CPU and communication costs all support energy-efficient Smart Grid IoT deployment.

All cited methods are correctly described from their first descriptions. The proposed framework had been able to overcome the problems that were found in these basic studies – namely heavy encryption overhead, insufficient lightweight privacy and lack of real-hardware energy optimization.

The ablation study confirmed that all components play an important role, with proposed full solution

offering the optimal trade-off in terms of accuracy and efficiency. These results extend the current state-of-the-art with the first end-to-end hardware validated framework to integrate privacy, energy and edge efficiency.

This solution addresses privacy risks, single point of failure risks, large-scale and real-time anomaly detection, hence grid reliability and sustainable IoT deployments. Further work could look at larger deployments and other concept drift scenarios, but the present findings already lay a good foundation for leveraging these techniques in deployment against smart-grid systems.

5. CONCLUSION

In this paper, the proposed FEL-AD-SG, a novel Federated Edge Learning-based Smart Grid IoT anomaly detection system with low energy consumption and privacy protection This approach combines lightweight differential privacy and secure aggregation for privacy, model quantization, client selection and duty cycling on real hardware Raspberry Pi 4 edge devices. The extensive experiments confirmed that FEL-AD-SG obtained 98.5% accuracy and 97.5% F1-score on the real smart metres (Ausgrid) data set, with just 24% CPU, 380 MB memory, 2.9 W power and 210 KB communication overhead per round.

This means 42% energy savings, 59% memory savings, 65% CPU savings and 83% communication savings as compared to the state-of-the-art techniques. The ablation study showed that each component of the framework (quantization, DP with secure aggregation, and client selection with duty cycling) helps achieve better detection, as well as energy and resource efficiency.

By overcoming the computational bottlenecks of Paillier homomorphic encryption, the lack of real-hardware validation of energy-efficient techniques, and the lack of end-to-end demonstration of previously proposed approaches, FEL-AD-SG presents the first viable end-to-end prototype that integrates privacy, energy, and edge optimization.

This novel framework pushes the frontier by delivering scalable, real-time, and secure anomaly detection on energy-constrained smart meters and RTUs, enabling improved grid reliability, mitigation of non-technical losses and eco-friendly Internet of Things (IoT) deployment in future smart energy systems. Potential extensions may include larger-scale experiments and techniques to address concept drift.

REFERENCES

[1] T. R. Jeter, R. Alharbi, J. T. Seo, and M. T. Thai, “Federated anomaly detection in smart grid systems,” *Digital Communications and Networks*, vol. 12, no. 3, pp. 451–461, Mar. 2026, doi: 10.1016/J.DCAN.2026.02.001.

[2] H. T. Truong *et al.*, “Light-weight federated learning-based anomaly detection for time-series data in industrial control systems,” *Comput. Ind.*, vol. 140, p. 103692, Sep. 2022, doi: 10.1016/J.COMPIND.2022.103692.

[3] S. Azam SamiAzam *et al.*, “A review of artificial intelligence techniques for anomaly detection in smart grid,” *Artificial Intelligence Review 2025 59:2*, vol. 59, no. 2, pp. 69-, Jan. 2026, doi: 10.1007/S10462-025-11429-X.

[4] R. Z. Alshamasi and D. M. Ibrahim, “Federated intelligence for smart grids: a comprehensive review of security and privacy strategies,” *Journal of Electrical Systems and Information Technology 2025 12:1*, vol. 12, no. 1, pp. 43-, Jul. 2025, doi: 10.1186/S43067-025-00235-8.

[5] D. kumar sah, M. Vahabi, and H. Fotouhi, “Federated learning at the edge in Industrial Internet of Things: A review,” *Sustainable Computing: Informatics and Systems*, vol. 46, p. 101087, Jun. 2025, doi: 10.1016/J.SUSCOM.2025.101087.

[6] F. R. Mughal *et al.*, “Adaptive federated learning for resource-constrained IoT devices through edge intelligence and multi-edge clustering,” *Scientific Reports 2024 14:1*, vol. 14, no. 1, pp. 28746-, Nov. 2024, doi: 10.1038/s41598-024-78239-z.

[7] M. J. Alfadhil, A. Baydoun, M. Alazab, H. U. Rehman, J. Al Jaam, and S. A. S. A. Al-Maadeed, “Enhancing federated learning for IoT-based anomaly detection: A reputation-based client selection approach,” *Alexandria Engineering Journal*, vol. 130,

pp. 889–909, Oct. 2025, doi: 10.1016/J.AEJ.2025.09.019.

[8] S. Gayathri and D. Surendran, "Unified ensemble federated learning with cloud computing for online anomaly detection in energy-efficient wireless sensor networks," *Journal of Cloud Computing 2024 13:1*, vol. 13, no. 1, pp. 49-, Feb. 2024, doi: 10.1186/S13677-024-00595-Y.

[9] S. M. Nour, A. Rady, M. S. Hussien, S. A. Salem, and S. A. Said, "FedTheftDetect: Optimizing Anomaly Detection in Smart Grid Metering Systems Using Federated Learning," *Computers 2026, Vol. 15, Page 202*, vol. 15, no. 4, p. 202, Mar. 2026, doi: 10.3390/COMPUTERS15040202.

[10] F. Asiri *et al.*, "Privacy Preserving Federated Anomaly Detection in IoT Edge Computing Using Bayesian Game Reinforcement Learning," *Computers, Materials and Continua*, vol. 84, no. 2, pp. 3943–3960, Jul. 2025, doi: 10.32604/CMC.2025.066498.

[11] R. C. Karpagalakshmi, J. Lenin, P. Rajaram, V. Balaji, R. Rangasamy, and A. Sungheetha, "Adaptive Anomaly Detection for Secure Federated Learning in IIoT Environments," *Procedia Comput. Sci.*, vol. 258, pp. 536–551, Jan. 2025, doi: 10.1016/J.PROCS.2025.04.289.

[12] W. W. Hu, J. A. Alzubi, J. Shreyas, M. Al-Razgan, Y. A. Ali, and A. Karthikayan, "Enhancing IoT Network Security by Anomaly Detection and Intrusion Prevention Using Gannet Optimization-Based Adaptive Deep Capsule Network," *International Journal of Computational Intelligence Systems 2025 18:1*, vol. 18, no. 1, pp. 237-, Oct. 2025, doi: 10.1007/S44196-025-00940-2.

[13] F. Hendaoui, R. Meddeb, L. Trabelsi, A. Ferchichi, and R. Ahmed, "FLADEN: Federated Learning for Anomaly DEtection in IoT Networks," *Comput. Secur.*, vol. 155, p. 104446, Aug. 2025, doi: 10.1016/J.COSE.2025.104446.

[14] Y. Zhang, B. Suleiman, M. J. Alibasa, and F. Farid, "Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A Group-Based Federated Learning Approach," *Journal of Network and Systems Management 2023 32:1*, vol. 32, no. 1, pp. 20-, Jan. 2024, doi: 10.1007/S10922-023-09782-9.

[15] B. Paul *et al.*, "Potential smart grid vulnerabilities to cyber-attacks: Current threats and existing mitigation strategies," *Heliyon*, vol. 10, no. 19, p. e37980, Oct. 2024, doi: 10.1016/J.HELIYON.2024.E37980.

[16] P. Vigneshwaran, S. Thuseethan, B. Shanmugam, and S. Thennadil, "Cyber-attack detection in smart grids: A survey of methods, challenges and future directions," *Comput. Sci. Rev.*, vol. 60, p. 100915, May 2026, doi: 10.1016/J.COSREV.2026.100915.

[17] A. Khraisat, A. Alazab, M. Alazab, A. Obeidat, S. Singh, and T. Jan, "Federated learning for intrusion detection in IoT environments: a privacy-preserving strategy," *Discover Internet of Things 2025 5:1*, vol. 5, no. 1, pp. 72-, Jun. 2025, doi: 10.1007/S43926-025-00169-7.

[18] M. Farsi *et al.*, "Detection of disturbances and cyber-attacks in smart grids using explainable machine learning," *Scientific Reports 2026 16:1*, vol. 16, no. 1, pp. 9834-, Feb. 2026, doi: 10.1038/s41598-026-35449-x.

[19] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023, doi: 10.1109/ACCESS.2023.3237554.

[20] M. Ahmad Bilal, I. Ul Islam, N. Iltaf, M. Junaid Khan, and M. Jaleed Khan, "Federated Learning With Explainable AI for Malicious Traffic Detection in IoT Networks," *IEEE Access*, vol. 13, pp. 173368–173383, 2025, doi: 10.1109/ACCESS.2025.3613459.

[21] M. Arivukarasi, S. Harihara Gopalan, S. Gnanamurugan, R. Dhanapal, A. Ramachandran, and A. Manikandan, "Federated autoencoder IDS for IoT: A Fed-ANIDS approach using CICIoT2023," *Systems and Soft Computing*, vol. 8, p. 200482, Jun. 2026, doi: 10.1016/J.SASC.2026.200482.

[22] M. N. Alatawi, "EdgeGuard-IoT: 6G-Enabled Edge Intelligence for Secure Federated Learning and Adaptive Anomaly Detection in Industry 5.0," *Computers, Materials and Continua*, vol. 85, no. 1, pp. 695–727, Aug. 2025, doi: 10.32604/CMC.2025.066606.

[23] M. Aggarwal *et al.*, "Federated Learning on Internet of Things: Extensive and Systematic Review," *Computers, Materials and Continua*, vol. 79, no. 2, pp. 1795–1834, May 2024, doi: 10.32604/CMC.2024.049846.

[24] H. Guo, Z. Zhou, D. Zhao, and W. Gaaloul, "EGNN: Energy-efficient anomaly detection for IoT multivariate time series data using graph neural network," *Future Generation Computer Systems*, vol. 151, pp. 45–56, Feb. 2024, doi: 10.1016/J.FUTURE.2023.09.028.

[25] R. Sepehrzad, H. Hosseinalibeiki, N. Taghinezhad, N. Khosravi, A. al Durra, and M. S. Sadabadi, "Enhanced cyber-resilience in flexible energy markets for microgrids: A trust-aware federated deep reinforcement learning framework," *Appl. Energy*, vol. 406, p. 127282, Mar. 2026, doi: 10.1016/J.APENERGY.2025.127282.

[26] S. Alharbi, "EdgeTrustX: A Privacy-Aware Federated Transformer Framework for Scalable and Explainable IoT Threat Detection," *Computers, Materials and Continua*, vol. 87, no. 3, Jan. 2026, doi: 10.32604/CMC.2026.073584.

[27] M. Devi, P. Nandal, and H. Sehrawat, "Federated learning-enabled lightweight intrusion detection system for wireless sensor networks: A cybersecurity approach against DDoS attacks in smart city environments," *Intelligent Systems with Applications*, vol. 27, p. 200553, Sep. 2025, doi: 10.1016/J.ISWA.2025.200553.

28

[29] A. Shabbir, H. U. Manzoor, A. Zoha, and Z. Halim, "Smart grid security through fusion-enhanced federated learning against adversarial attacks," *Eng. Appl. Artif. Intell.*, vol. 157, Oct. 2025, doi: 10.1016/J.ENGAPPAI.2025.111169.

[30] M. Shuaib, "Federated deep learning for secure and energy-efficient cyber threat mitigation in smart grid automation," *Sustainable Computing: Informatics and Systems*, vol. 48, p. 101248, Dec. 2025, doi: 10.1016/J.SUSCOM.2025.101248.

[31] N. Hamdi, "A hybrid learning technique for intrusion detection system for smart grid," *Sustainable Computing: Informatics and Systems*, vol. 46, p. 101102, Jun. 2025, doi: 10.1016/J.SUSCOM.2025.101102.

[32] D. Premkumar and S. K. Nachimuthu, "Privacy-preserving cyberthreat detection in decentralized social media with federated cross-modal graph transformers," *Scientific Reports 2025 16:1*, vol. 16, no. 1, pp. 3608-, Jan. 2026, doi: 10.1038/s41598-025-33596-1.

[33] J. Sievers, K. Kumbhani, T. Blank, F. Simon, and A. Mauthe, "Towards secure federated learning for energy forecasting under adversarial attacks," *Energy and AI*, vol. 23, p. 100680, Jan. 2026, doi: 10.1016/J.EGYAI.2026.100680.

[34] R. Iqbal, S. Ismail, and G. Rathee, "Hardware aware federated learning with sparse models for adaptive anomaly detection in IoT," *Discover Artificial Intelligence*, Apr. 2026, doi: 10.1007/S44163-026-01171-W.

[35] A. dos Santos Oliveira *et al.*, "Looking at anomaly detection in EdgeAI through the up-to-date lens of academic and market perspectives," *Cluster Computing 2026 29:4*, vol. 29, no. 4, pp. 251-, Apr. 2026, doi: 10.1007/S10586-026-05954-9.

[36] M. N. A. Ramadan, M. A. H. Ali, S. Y. Khoo, and M. Alkhedher, "Federated learning and TinyML on IoT edge devices: Challenges, advances, and future directions," *ICT Express*, vol. 11, no. 4, pp. 754–768, Aug. 2025, doi: 10.1016/J.ICTE.2025.06.008.

[37] W. Zhang, L. Di, J. Zhang, B. Liu, and X. Wang, "Design of a federated learning algorithm for power big data privacy computing based on pruning technique and homomorphic encryption," *Egyptian Informatics Journal*, vol. 32, p. 100828, Dec. 2025, doi: 10.1016/J.EIJ.2025.100828.

[38] V. K. Vishwanath, A. B. Rajendra, and H. L. Gururaj, "Multi-armed bandit-based federated reinforcement learning for

dynamic task offloading in a containerized MEC," *Discover Applied Sciences 2026 8:4*, vol. 8, no. 4, pp. 376-, Feb. 2026, doi: 10.1007/S42452-026-08386-7.

[39] Y. K. Saheed and J. E. Chukwuere, "XAI-Enhanced adversarial resilient deep learning framework for transparent and secure edge deployment in consumer Internet of Things/Industrial Internet of Things environments," *Computers and Electrical Engineering*, vol. 133, p. 111080, May 2026, doi: 10.1016/J.COMPELECENG.2026.111080.

[40] M. Li, P. Xu, J. Hu, Z. Tang, and G. Yang, "From challenges and pitfalls to recommendations and opportunities: Implementing federated learning in healthcare," *Med. Image Anal.*, vol. 101, p. 103497, Apr. 2025, doi: 10.1016/J.MEDIA.2025.103497.

[41] R. Shrestha *et al.*, "Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid," *J. Parallel Distrib. Comput.*, vol. 193, p. 104951, Nov. 2024, doi: 10.1016/J.JPDC.2024.104951.

[42] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023, doi: 10.1109/ACCESS.2023.3237554.

[43] S. Gayathri and D. Surendran, "Unified ensemble federated learning with cloud computing for online anomaly detection in energy-efficient wireless sensor networks," *Journal of Cloud Computing 2024 13:1*, vol. 13, no. 1, pp. 49-, Feb. 2024, doi: 10.1186/S13677-024-00595-Y.