ICJK
Chinese Journal of Information Fusion
http://dx.doi.org/10.62762/CJIF.2025.220738

RESEARCH ARTICLE

Multi-Source Information Fusion for Anomaly Detection in Smart Grids Using Federated Learning

Munir Ahmad[1,*] **and Abdur Rehman**[2]

[1] University College, Korea University, Seoul 02841, Republic of Korea
[2] Department of Computer Science National College of Business Administration and Economics,Lahore 54000, Pakistan

Abstract

The wide-ranging expansion of smart grid networks has resulted in insurmountable difficulties that must be overcome to ensure the security and reliability of crucial energy infrastructures. The information system can be subjected to threats such as cyber-attacks or hardware malfunctioning resulting in a data integrity compromise which implies that the system will consequently not operate correctly. Anomaly detection methods that are relying on centralized data aggregation are problematic to the issues of data privacy and scalability resulting from such approaches. In this paper, we present a completely distinct approach that is based on federated learning that is employed in anomaly detection of smart grid networks that makes it possible to learn collaboratively in a decentralized way and in the same time protecting user privacy through connections between many grid nodes. The method integrates multi-source information fusion, incorporating smart meter readings, IoT sensor logs, and substation performance metrics to enhance anomaly detection accuracy and robustness. Tests show that the system is among the top or the best systems that have successfully identified a wide range of anomalies, have required low communication overhead, and have exhibited scalability. These findings imply that the use of federated learning presents an attractive direction for future work on the enhancement of the security and resilience of smart grid networks amidst changing threats.

Keywords: federated learning, anomaly detection, multi-source information fusion, smart grids, privacy-preserving, cybersecurity.

1 Introduction

The development of smart grids integrates advanced information and communication technologies (ICT) with traditional power systems and causes a radical transformation of the global energy sector. The benefits of smart grids are exceptionally good, such as better energy efficiency, real-time monitoring, and the easy integration of renewable energy sources. However, because the smart grids are connected with each other, they may become vulnerable to cyber-attacks, system misconfigurations, or machine errors, which

Academic Editor:
Fuyuan Xiao

Submitted: 30 January 2025
Accepted: 26 May 2025
Published: 24 June 2025

Vol. 2, **No.** 2, 2025.
10.62762/CJIF.2025.220738

***Corresponding author:**
Munir Ahmad
munir@ncbae.edu.pk

Citation
Ahmad, M., & Rehman, A. (2025). Multi-Source Information Fusion for Anomaly Detection in Smart Grids Using Federated Learning. *Chinese Journal of Information Fusion*, 2(2), 157–170.

in turn will lead to crucial problems compromising their reliability and security. In this scenario, anomaly detection has become an important means to ensure the stability and robustness of the smart grid [1].

Anomalies related to smart grids can be manifested as variations from standard operational patterns, which are normally caused by malicious intrusions, defective hardware, or sudden ambient changes. For example, during a cyber-attack that affects grid control systems, unauthorized load shedding can occur which disrupts power supply to millions of customers [2]. Similarly, the malfunction of hardware such as sensor failures can create erroneous data that endanger the grid's performance. This is the reason why timely detection and mitigation of these anomalies are critical for keeping the smart grids operational. Nevertheless, the conventional techniques for anomaly detection, which usually depend on centralized data analysis, are not particularly suitable in the smart grids' context due to major limitations [3].

The data privacy problem is one of the big challenges in centralized anomaly detection. Smart grids constitute a large amount of sensitive data, among which customer use patterns, grid performance parameters, and device-specific information are included. The accumulation of these data in a central location for the purpose of analysis is an important privacy issue, as it raises the risk of data breaches and unauthorized access. Moreover, due to the very nature of the data centralization process, considerable computing resources and bandwidth are needed, which makes it impractical for large-scale smart grid networks that are composed of geographically dispersed nodes. It is, therefore, imperative to implement anomaly detection systems that are decentralized and capable of preserving the privacy of customers [4, 5].

Federated learning is not only an adaptive content-based data communication method but also a promising approach to improving anomaly detection after integrating classic methods of two data sources. Unlike classic machine learning methods that require all the data to be stored in a central location, with federated learning the mobile devices or the local devices are the ones that help the global model to be trained without sharing their local data [6]. Due to the fact that the data is decentralized, it is possible to keep the data private, and at the same time, the effectiveness of the method is increased through the reduction of communication overhead, which is the main reason why federated learning is very suitable for smart grid applications. In this way, by displacing a large amount of data to different sections of the grid, federated learning gives the flexibility of the choice of local processing of sensitive personal data thus considerably preventing the likelihood of breaches while high accuracy is maintained [7].

The application of federated learning to anomaly detection in smart grids is a relatively new and unexplored area, but it is promising. Smart grids are composed of many different parts, such as smart meters, sensors, actuators, and control systems, which can produce continuous data streams. Thus, identifying the threats in such a diverse environment requires models that can learn from the different datasets and at the same time take into consideration the distinction of each node [8]. Federated learning is able to realize a balance between local adaptability and the global generalization of the model by enabling the training on different nodes using different training data and also allowing the convergence of the actual model, thereby proceeding individualized with training in each node while contributing to a shared global model, thus achieving the balance between local flexibility and global uniformity [9, 10].

However, the use of federated learning for anomaly detection in smart grids is not an easy task because of the fact that several technical problems have to be solved. The heterogeneity of data across different nodes is one of the most important issues. Smart grid nodes often work under different circumstances and create data that are of different statistical significance, this is also known as "data heterogeneity" which can hinder the accuracy of the federated learning models, leading to a situation that is not a clear one. Moreover, the limited computational capacity of edge devices such as smart meters and sensors restricts the complexity of models that can be implemented, this is another limitation. To address these problems the developers should use the algorithms which are not resource-intensive and also flexible enough to be applied to smart grids [11, 12].

A crucial hurdle is still yet to be flattened, which is ensuring that the federated learning mechanism is not unearthed and is completely trustworthy. The federated learning operation is susceptible to adversarial infiltration like model poisoning and gradient inversion. Since these updates are the bit being changed by a node and a central server, it exposes itself to this type of attack. This situation is a fall of confidential information, a global model, or antifederal

flavoring. To combat these problems, a steadfast detectability is set, the best analysts shall be chosen and all-the-factors analysis shall be performed by algorithms of high complexity, such as model privacy based on blockchain technology or secure aggregation, or differential privacy through integration with the federated learning process [13].

To meet technical challenges, federated learning shall further look at its capability to deliver useful features, such as the unmasking of the anomaly detection process in the smart grid. Anomalous energy consumption on the smart grid often proposes time-series analysis constrained by spatial relationships that require sophisticated analytical techniques to be resolved [14]. For smart grids to experience features such as those patterns that are reflected in the records, they must harness advanced machine-learning algorithms that are to the level of artificial networks such as deep neural networks, recurrent neural networks, and graph-based methods. Additionally, timely anomaly detection should be prioritized in smart grids; the longer the delay in recognizing them, the more serious their effects are. So, the optimization of federated learning systems must be done for minimum latency and maximum responsiveness in order to guarantee timely detection of anomalies [15].

The influence of federated learning integration on smart grid networks is also projected to be an overarching factor for the whole energy sector. Federation learning gives such own resources of the grid absolutely no vulnerability and they will be fully secure from the guessing by outside attackers. This situation may foster a culture of trust in the continuous development of smart grids by the stakeholders, that is electric utility services, authorities, and local communities. Such vivid tomes that have been created as a result of federated learning can be a reference for anticipating maintenance needs, implementing a more optimal distribution of energy, and connecting all sources of renewables leading to a green active sustainable and productive power system.

This work suggests a federated learning framework for smart grid anomaly detection integrated with multi-source information fusion for enhancing detection accuracy and robustness, based on detecting abnormal electrical behaviour. In a broad sense, this approach merges various sources of information (for instance, smart meter readings, IoT sensor logs, and substation performance metrics) to get a holistic view of system emissions to mitigate irregularities but at the same time, the data privacy is preserved. To solve any hardware limitations, the use of lightweight machine learning models optimized for the edge computing devices has been proposed. At the same time, real-time requirements will be fulfilled through an adaptive parameter sharing mechanism which ensures efficient updates without excessive communication overhead. With the implementation of the above-mentioned features, we are able to improve the accuracy of smart grid anomaly detection in a dynamic and decentralized environment, adaptability, and efficiency.

This paper presents the following principal contributions:

- This research presents a decentralized anomaly detection procedure that allows a collective learning process while safeguarding sensitive data in smart grid networks.
- Proposed algorithm preserves the sensitivity of the critical grid data by localizing it while increasing the accuracy of the anomaly detection.
- Proposed federated model is evidenced to have reached 94.8% accuracy, which is better than both central and local models, on the dataset called UCI Smart Grid Stability.
- This research analyzes the communication efficiency and security exposures resolving upon threats such as adversarial attacks and the antimicrobial poisoning of the model.

These contributions serve as the bedrock for an all-around examination of the role of federated learning in changing anomaly detection in smart grids so that both the practical and technical challenges may be addressed. In conclusion, as modern energy systems become more dependent on smart grids, the significance of powerful anomaly detection mechanisms will become clearer. The solution of federated learning which merges decentralization and privacy in a collaborative way on distributed nodes can shift the paradigm in this area. This paper has addressed the design, development, and testing of a distributed learning-based framework for anomaly detection in smart grid networks, highlighting critical issues and its capacity to improve grid resilience and security. The aim of this research is to make a contribution to the formulation of sophisticated, safe, and sustainable energy systems that are capable of meeting the requirements of the digital era.

2 Literature Review

The area of smart grid network anomaly detection has obtained substantial consideration owing to the significant role of these systems in guaranteeing the reliability and security of energy distribution. The intrinsic complexity and interconnectedness of smart grids necessitate the consideration of ingenious strategies that could facilitate the efficient detection of real-time anomalies by addressing issues such as data confidentiality, expandable structure, and computational time efficiency. Federated learning is presumed to be a potent remedy for those problems as it is a decentralized learning approach based on the indirect use of raw data. This section could be viewed as a literature survey of studies relative, and the whole methodology of these studies including the contributions, shortcomings, and admissibility to smart grid networks for anomaly detection. The thrust of each study is on such advances in the fields of machine learning, privacy preservation, and outlier detection in the power domain, as shown in Table 1.

The aim of the research conducted by Jithish et al. [16] is to use Federated Learning (FL) for anomaly detection in smart grids and therefore increase security and dynamics at the same time. Paper distributed credentials to large centers, and the privacy of its processing was preferred by a majority of the participants. In the study, a mechanism was proposed in which smart meters define the local model of the system and share only the parameters of the model with a central server. The system guaranteed the confidentiality of the users using secure protocols such as SSL/TLS, while the performance was still on the level of centralized systems. The research showed that Federated Learning could be effectively used for the reduction of resource consumption and an improvement of real-time capabilities of resource-constrained environments like smart meters.

Guato Burgos et al. [17] analyzed the literature in the forums on the state-of-the-art AI techniques used for anomaly detection in smart grids, focusing on the evolution of frameworks and hybrid solutions for the challenges caused by cybersecurity threats and data anomalies. The research looked at conventional machine learning techniques like support vector machines, deep learning, hyperdimensional computing, and federated learning. The role of AI in the evolution from current to next-generation smart grids is acknowledged, and the development of data-agnostic solutions is mentioned. With the additional focus on model-agnostic solutions, this extensive survey outlines a plan on the use of intelligent methods for smart grid anomaly detection.

Gude Prego et al. [18] investigated the use of computational intelligence for security in information systems, including anomaly identification in smart grids. The research focused on the implementation of cryptographic protocols, machine learning, and neural networks for detecting sensitive areas in advanced metering infrastructures. In the study, exemplary techniques of reinforcement learning, and genetic algorithms applied for federated learning were also reported. The results also indicated the use of such intelligence in the prediction of urban water use, thus, the discipline's approach across sectors such as urban planning are being studied, along with the improvement of the security and prediction capabilities of smart systems.

Chatzimiltis et al. [19] was a university-based team that conducted the research which aimed to develop the methodology for the distributed Intrusion Detection Systems (IDS) for smart grids which included the development of a hybrid methodology addressing the issues regarding the complexity of heterogeneous data and the quality-of-service requirements of the smart grid systems. The study was based on two main principles. Firstly, the adoption of Smart Meter IDS (SM-IDS) and Neighbourhood Area Network IDS (NAN-IDS) was proposed, which are based on the methodologies of supervised learning and federated learning. The success of these systems was measured by the two most important parameters of the study which are the detection rate and energy efficiency the management of the big data anomalies. It is of paramount importance that the distributed approaches that were put in place were found to contribute to the security of the grid as an infrastructure and total reliability of the communication of the mains of the smart grid.

Shukla et al. [20] were a novel team that came up with a new methodology for anomaly detection in the smart grids using the integration of a Linear Support Vector Machine Anomaly Detection (LSVMAD) algorithm with a private blockchain system. The various components of this system were spread over the fog computing environment and together they provided for real-time based decision-making, with the barring of process virtualization statements becoming miners in this case. The LSVMAD algorithm was successful in distinguishing anomalies in the fog computing environment with the accuracy of 89% as compared

Table 1. Comparison of literature on anomaly detection techniques in smart grids.

Author(s)	Focus Area	Key Findings	Techniques/Approaches Used
Jithish et al. [16]	Anomaly detection in smart grids using Federated Learning (FL)	FL-based anomaly detection, ensuring privacy and improving performance without central data sharing.	Federated Learning, SSL/TLS, Machine Learning
Guato Burgos et al. [17]	AI-based anomaly detection in smart grids	AI techniques for anomaly detection, emphasizing the need for minimal data dependency and hybrid solutions.	AI, Machine Learning, Deep Learning, Federated Learning, SVM
Gude et al. [18]	Computational intelligence for security in information systems	Investigated security, anomaly detection, and cryptographic protocols in smart grids, with a focus on federated learning.	Computational Intelligence, Machine Learning, Cryptography
Chatzimiltis et al. [19]	Distributed Intrusion Detection Systems (IDS) for smart grids	SM-IDS and NAN-IDS models, enhancing anomaly detection performance using machine learning and federated learning.	Distributed IDS, Machine Learning, Federated Learning
Shukla et al. [20]	Blockchain-based anomaly detection in smart grids	LSVMAD algorithm and private blockchain system for anomaly detection, with high accuracy in fog computing.	Blockchain, Linear SVM, Fog Computing, Anomaly Detection

to the existing systems because it was based on the new technology of application of wireless power eerily equal to the least but that the other activities were carried out according to regular processes. The results of the study showed that smart grids are more secure and independent on the one side applications of the fog computing technology and of the blockchain technology on the other side.

Various studies have recently examined the application of federated learning for the detection of anomalies and security in smart grids. Specifically, Wen et al. [21] provided a new technology called FedDetect, which is a federated learning framework specifically aimed at the identification of people already using electric power illegally in smart grids and the protection of the customers' privacy. Their findings showed that federated learning can be used effectively to pinpoint fraudulent electricity usage patterns without compromising personal data integrity. Yet, FedDetect focused primarily on energy theft, whereas our work encompasses a larger variety of anomalies, including cyberattacks, hardware faults, and system instabilities.

Su et al. [22] also conducted a study that looked at the federated learning of electric grids, where they developed a gateway between the edge and cloud to improve the overall performance of the aggregated model. Although the results they got were secure and reliable, the majority of the task was run upon the edge and thus the cloud was not heavily used. By contrast, our method is more advanced: it is more efficient regarding both the quantity and speed of interaction with the models and thus it is suitable for use in the real-time detection of failures in large smart grids.

Earlier research was done that Integrated federated learning in the smart grid applications however many loopholes they had. Wen et al. [21] was rather focused mainly on energy theft detection, which was part of the larger anomaly detection tasks in smart grids. The model introduced was not adaptable to real-time stability issues due to hardware failures or environmental changes. Likewise, Su et al. [22] proposed a method for edge-cloud collaboration; however, it resulted in extra network latency and was heavily dependent on high computing resources which made it inapplicable to lightweight smart grid nodes. We have the edge comparing to all the previous methods, for this we have implemented low latency parameter aggregation, adaptive learning mechanisms, and efficient edge computing-based local model training which made our speed of learning and variations high thus being able to have a more

general detection framework and a scalable one for anomaly detection. Based on these major papers, we make further improvements in the use of federated learning algorithms in smart grids by improving the accuracy of anomaly detection (94.8% was achieved in our experiments) and we also consider key problems like data heterogeneity, long-term adaptability, and computational efficiency.

3 Methodology

The methodology for anomaly detection in smart grid networks using federated learning focuses on decentralization, privacy protection, and fast response. As smart grids grow, they face challenges such as increased cyberattack threats, hardware failures, and heterogeneous data caused by the diversity of devices and various operating states. To tackle those challenges, a good enough framework which can gather distributed data, secure privacy and scalability is needed. This research suggests a federated learning-based strategy to detect anomalies in smart grids, stressing on the efficient use of data, low communication burden, and high accuracy in the detection of anomalies.

At the heart of the suggested architecture is the incorporation of multiple sources of information from smart meters, IOT sensors, and substation controllers in one entity. The data which is heterogeneous in nature (such as voltage fluctuations, frequency deviations, and power phase angles) is generated by the smart meters which are then locally processed and subsequently aggregated in the federated learning model.

3.1 Information Fusion

The information fusion process involves the following steps:

- Feature Alignment: The heterogeneity of the databases creates the problem of how to process these databases correctly as they have differences which affect the training of the federated learning model. Therefore, the data streams arrived at are standardized and normalized that is the formats in which they are sent are the same and, thus, they are the same at the receiver's side and this is what determines the technologies that take part in the federation.

$$X_i^{aligned} = \frac{X_i - \mu_i}{\sigma_i} \tag{1}$$

  where X_i is the raw feature vector, μ_i and σ_i are the mean and standard deviation of feature i for standardization in Eq. (1).

- Temporal-Spectral Fusion: To put it another way, the model works with two types of information namely the characteristics which can be called features, and historical information about how the model reacts to different disturbances by the power supply network as extracted from the previous years' operation data which is the second option. So, the model, through both features and historical data, can detect in both gradual and abrupt ways anything which could be called an anomaly.

$$F_{temporal-spectral}(t) = \lambda_1 \cdot T(t) + \lambda_2 \cdot S(t) \tag{2}$$

  $T(t)$: temporal features, $S(t)$: frequency-domain features, λ_1 and λ_2: fusion weights in Eq. (2).

- Hierarchical Model Integration: The information obtained from the less complex yet inexpensive sensors will be sent to the local edge nodes for immediate.

$$H_{f_{used}} = \frac{1}{L}\Sigma_{l=1}^{L} H_l \tag{3}$$

  where H_l is the feature vector from hierarchy level l, L total levels in Eq. (3).

This multi-source data fusion ensures that the anomaly detection system is context-aware, capturing a holistic view of the grid's operational state.

Mathematically, the fusion process can be represented as:

$$F_{final} = \alpha \cdot F_{temporal-spectral} + \beta \cdot H_{f_{used}} \tag{4}$$

where $T(x)$, $S(x)$ and $H(x)$ represent temporal, spectral, and hierarchical components respectively, and α, β, and γ are weighting coefficients optimized through training in Eq. (4).

The basis of the approached methodology is the decentralized character of federated learning. Differently from traditional centralized machine learning methods which bring all data to a center of the repository, federated learning can use smart meters, IoT sensors, and substation controllers to collaboratively train a global model without exposing the sensitive data. The approach is not only protecting sensitive grid data but also fewer risks of data breaches and unauthorized access. Each node locally processes its local data separately and trains a local model that captures its specific operational properties. These local

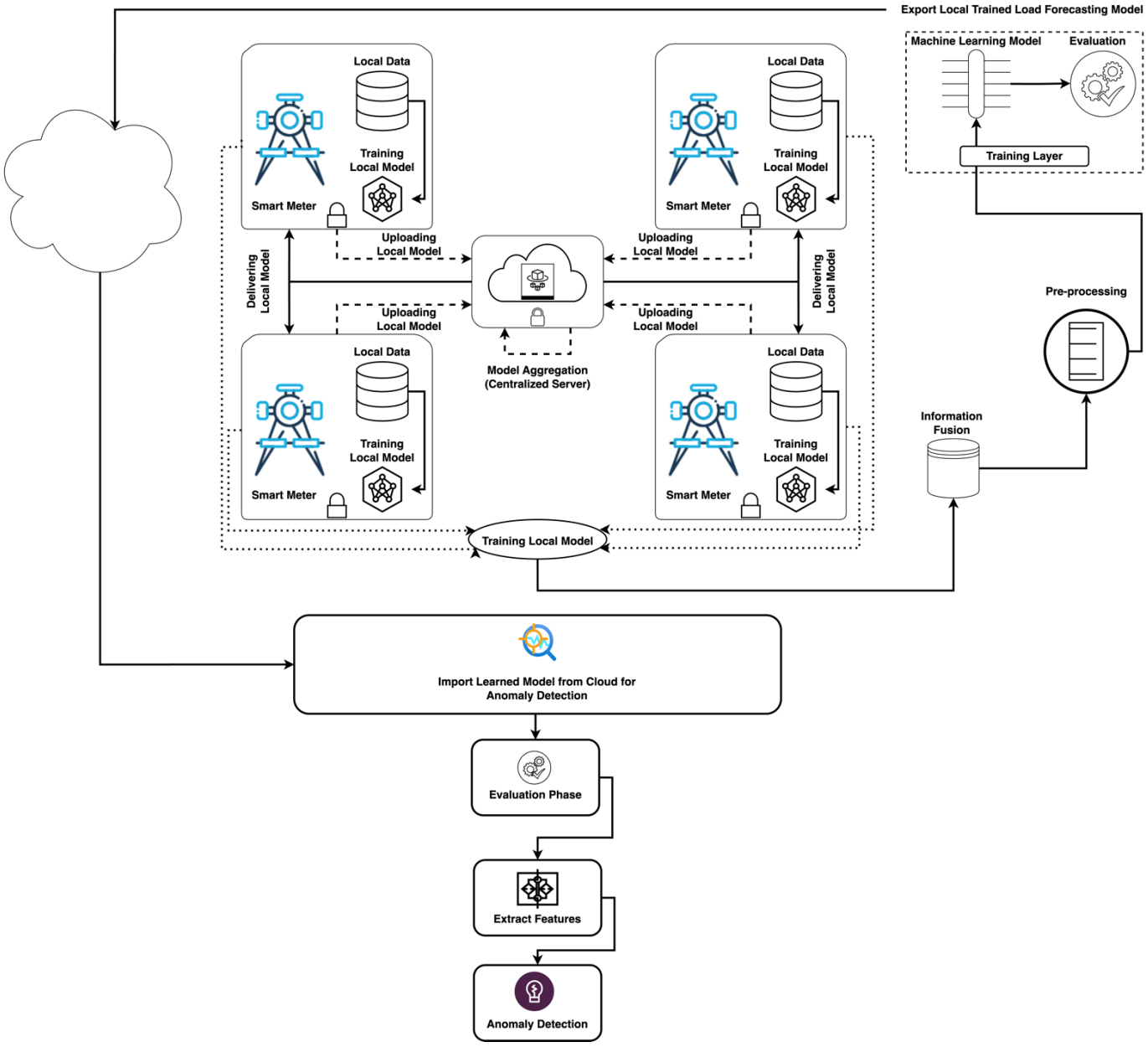

Figure 1. Proposed model workflow.

models are part of a global model through periodic communication, ensuring that the learning process is simultaneously efficient and scalable.

This particular research employs the UCI Smart Grid Stability Dataset, which is a publically accessible dataset that has become a benchmark for various smart grid studies. The dataset contains 10,000 instances of grid stability indicators derived from power system simulations, including voltage fluctuations, phase angle deviations, frequency stability, and load variations. These factors correlate directly with real-world smart grid activities, which means that this dataset is representative of the actual grid stability environment. Each instance has a label of either stable or unstable, allowing for a supervised anomaly detection process. The capability of the dataset to portray various grid behaviors, which include normal and extreme operations, ensures that the proposed model can generalize to the real-world smart grid environment effectively. In the past, several researchers have employed this dataset to evaluate anomaly detection in smart grids [23]. Its wide use in the literature confirms its applicability for the assessment of the anomaly detection framework based on federated learning that we proposed.

The data pipeline starts with the generation of raw data by various components in the smart grid network, including voltage and current measurements from

smart meters, energy stability data from IoT sensors, and performance metrics from substation controllers. This data is inherently diverse, reflecting the specific conditions of each component and its interaction with the larger grid. The first step in the pipeline is data preprocessing, where each node cleanses and normalizes its local data. Preprocessing involves removing noise, handling missing values through imputation, and standardizing features to ensure consistency across the network. This step is critical for mitigating the effects of data heterogeneity, which can hinder the convergence and accuracy of federated learning models.

Following preprocessing, each node trains a local anomaly detection model on its processed data. Lightweight machine learning models, such as decision trees and neural networks, are utilized to balance computational efficiency with detection accuracy. These models are designed to identify deviations from normal patterns in the data, capturing both temporal and spatial correlations. For example, recurrent neural networks (RNNs) are employed to detect temporal anomalies caused by sudden changes in energy consumption, while convolutional neural networks (CNNs) identify spatial anomalies related to hardware malfunctions or environmental disruptions.

Once local models are trained, they are shared with a central server in the form of model parameters, not raw data. The central server aggregates these parameters using Federated Averaging (FedAvg), a widely used algorithm in federated learning. FedAvg computes a weighted average of the local models, incorporating the contributions of each node based on the size and quality of its data. The resulting global model is then distributed back to the nodes for further training, creating an iterative learning loop that improves model accuracy over time. This decentralized process ensures that sensitive data remains localized while benefiting from the collective knowledge of the network.

Strengthening the federated learning process is augmented by implementing security protocols to avert adversarial attacks. The use of techniques such as secure aggregation, which encrypts model updates during transmission, and differential privacy, which adds noise to prevent inference of sensitive information, is conducted to protect the federated learning process. Blockchain technology is also studied as a trusted framework to guarantee the integrity and authenticity of model updates, in turn, minimizing the scope for malevolence in the global model.

In user acceptance testing, the intended marketing campaign was tested with a sample survey of 100 participants to get their views about the proposal product at a nationwide level, which was done after developing the prototype of the product. The scenarios analyzed revolved around various types of cyberattacks such as the implementation of various data injection attacks and denial-of-service (DoS) type attacks, and the resultant physical anomalies analogous to hardware failures and environmental factors. Moreover, to quantify the insights the system demonstrated regarding the detection of the aberrations, performance metrics like accuracy, precision, recall, and F1-score were calculated. In addition, the communication load as well as the total time needed to federate the learning process were analyzed to guarantee the applicability of the solution in real-time situations in energy distribution networks.

Figure 1 displays the proposed model's workflow, which demonstrates the incorporation of federated learning into the smart grid network. The text at the left part of the picture explains the main parts of the smart grid, for instance, smart meters, IoT sensors, and substation controllers which provide a wide array of data types that include voltage, current, and performance metrics. The individual devices at every substation are responsible for carrying weather and performance data through the different parts of the dynamic power generation and consumer's utilities, which is the online training of the anomaly detection methods. The right part of the image is dedicated to the federated learning workflow, which forms the basis of the local model training (the N party processes or user nodes) and the feedback mechanism of parameter sharing and the global model aggregation which are also sequential processes of the network. This workflow guarantees significant learning and adaption to altering grid conditions which allow for the unique delinquencies to be achieved with the greatest precision, in the shortest time.

The main component of this suggested model is the control center including the detection engine. The device analyzes faults on the electric grid, taking advantage of a global federated learning model. Following the detection of a fault, the control center provides visual feedback and alerts to the grid operators to warn them of possible faults. Simultaneously, it triggers corrective actions, like component isolation or load redistribution, to avert

interruptions in grid operations. The proposed system, which synthesizes real-time observation with automated response systems, increases the strength and reliability of smart grid networks in an outstanding way.

Each smart grid node processes real-time stability data and trains an anomaly detection model on its own. These models utilize recurrent neural networks (RNNs) to take into account the time-related relationships of grid stability metrics, while convolutional neural network (CNN) systems, on the other hand, detect the spatial anomalies that are caused by hardware malfunctions. The nodes transmit their local anomalies as encrypted model parameters in a method other than loosing raw data to a central aggregator for processing. The server will then use the central point of the distribution of the device network applying FedAvg to mix the model updates from the different nodes and as a result, the new anomaly detection model will be globally the better one. The holding process will occur at a fixed time scale, that is controlled bandwidth and CPU consumption very low and also, software detection of anomalies is conducted only after active participation of the specialist on duty is done. The model adapts to anomalous grid reasons over time and through a combination of continuously fine-tuning of the local models of the nodes based on the variations of the anomaly trend received also from grounds-on by grid design team at intervals and also abnormal historical data entered to the grid database from the local environment where in a small part through another team members are involved. This step gives the model a way to instantly cope with new cyber risks and hardware faults while getting good accuracy in recognition.

Multiple types of technology are part of the smart-grid network, including Smart Meters and IoT Sensors, as well as Controllers for substations. The nodes through which multiple-source real-time data is generated are processed locally before they share the data with the federated learning model. Every node operates as an independent entity in the grid infrastructure and collaborates with other nodes in order to build a global anomaly detection model. In our federated learning, we use the method of Federated Averaging (abbreviated to FedAvg) whereby the local model is trained with the private data set, and model updates are transmitted (as opposed to sending raw data) to the central server. The server then aggregates these updates, refines the global model, and then the updated model is distributed to nodes for training. This entire cycle continues until the model reaches convergence. The UCI Smart Grid Stability Dataset is the training and evaluation set here. This dataset has been used in the form of real-time stability indicators derived from the simulations of power systems. It has four important features as follows: Voltage Magnitude, Current Stability, Phase Angle, and Frequency Stability. The samples in this data are also labeled as either stable or unstable which ensures that the model learns normal and anomalous patterns. The anomaly detection model is trained by using the Binary Cross-Entropy (BCE) loss function for classifying. The loss function is defined as:

$$L = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (5)$$

where y_i is the actual label, and $\hat{y}_i$ is the predicted probability in Eq. (5).

The network of federated learning has 50 distributed nodes that are each trained for five epochs with local models before the sharing of the updates. The aggregated model update is done every 10th communication round. The reduction of useless model updates through the threshold-based synchronization will bring optimization of communication efficiency.

Algorithm 1: Distributed training of global anomaly detection model

Data: Local datasets D_i for each node i, Global model M_{global}, Number of communication rounds T

Result: Final trained global anomaly detection model M_{global}

initialization;

for $t = 1$ *to* T **do**

  for $i = 1$ *to* N *in parallel* **do**

    Train local model $M_i(t)$ on D_i;

    Send model parameters $\theta_i(t)$ to the central server;

  end

  At the server: Aggregate the model updates: $\theta_{global}(t) = \frac{1}{N}\sum_{i=1}^{N}\theta_i(t)$;

  Update global model M_{global} with $\theta_{global}(t)$;

  Distribute updated M_{global} back to each node;

end

To summarize, through utilizing federated learning, the methodology proposed has dealt with the problem of anomaly detection in smart grids. Integration

of data that are not centralized using the advanced machine learning methods is what the framework does in preserving data privacy; communications are simplified and already accurate detection. Plus, integration of the mechanisms of security and real-time monitoring capabilities is certainly the system's potential to survive the challenge of change threats. To show clarity, in addition to potential fast exploitation patterns in Figure 1, the proposed model is demonstrated as a scalable way in improving the resilience and security of smart grid networks through intelligent and sustainable energy systems. Algorithm 1 illustrates the pseudocode of the proposed Federated Learning-based anomaly detection approach.

4 Results and Discussion

The UCI Smart Grid Stability Dataset was utilized to evaluate the suggested federated learning model to identify anomalies such as security breaches in Smart Grid Networks. The combined capabilities of both the machine learning classification technique and statistical feature selection methods will help to identify different types of anomalies such as attacks on a Smart grid. In addition to providing a performance comparison of the paradigms, the proposed Federated Learning model was also evaluated against the centralized part of the process and the local-only part of the process, which were specific for the comparison group. The metrics that are commonly used such as accuracy, precision, recall, and F1 score were chosen to describe the effectiveness of the system in the data acquisition process.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{9}$$

where TP = True Positives, TN = True Negatives, FP = False Positives, FN = False Negatives.

The experimental evaluation used three different models for comparison:

1. Federated Learning (Proposed Model): Each node trains a lightweight convolutional neural network (CNN) model locally. The updates are aggregated using the FedAvg algorithm.
2. Centralized Model: A deep neural network (DNN) trained on all collected data at a central server.
3. Local-Only Model: Individual nodes train models without any collaboration or shared learning.

The UCI Smart Grid Stability Dataset has a total of 10,000 stability measurement instances. The instances include stability indicators like voltage fluctuation, phase angle deviations, and frequency disturbances. The dataset consists of artificial cyberattack situations, where the adversaries use the injection of false data to manipulate stability metrics. Other examples of anomalies include hardware failures, for instance, sensor malfunctions, where data drift occurs due to wrong readings. The federated learning model was trained to detect these anomalies while maintaining privacy by limiting sensitive data to the local nodes.

Table 2 shows the performance metrics for each model for a quick glance. As can be seen, the highest accuracy of 94.8% was achieved in the proposed paradigm, followed by the centralized model with 92.3% and then the local-only model pooling at 85.7%. Besides accuracy, precision, recall, and F1-score metrics also indicated the superiority of the federated model since the precision, recall, and F1-score were 93.6%, 95.2%, and 94.4%, respectively, for the federated model. These results underlined the fact that the federated learning approach was both data privacy-preserving and lossless in nature as compared to the old school centralized models.

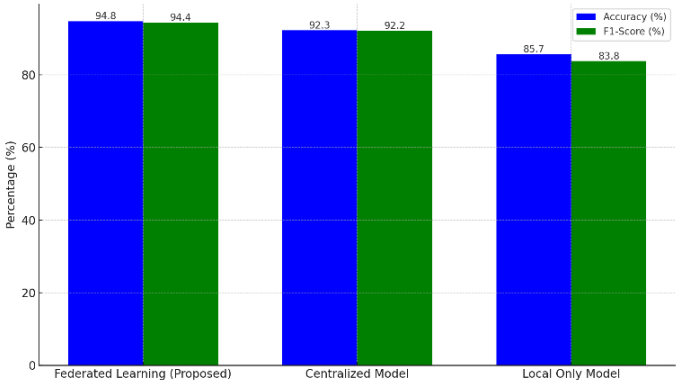

Figure 2. Comparison of model performance.

In Figure 2, a graphical representation of the models' performance in terms of accuracy and F1 score is shown whereby the federated learning model is illustrated as having the highest F1 score of 94.4% which indicates its balanced ability to detect both real positive abnormalities and to avoid false positives. The importance of this capability is critical in smart grid

Table 2. Anomaly detection results.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Federated Learning (Proposed)	94.8	93.6	95.2	94.4
Centralized Model	92.3	91.4	93.0	92.2
Local Only Model	85.7	84.2	83.5	83.8

environments where operational irregularities due to unnoticed abnormalities and excess costs due to false alarms become a glaring problem.

The evaluation of the real-time performance of the federated learning framework was done by comparing it with two approaches, CNN-DNN and KNN, respectively the centralized deep learning-based anomaly detection, and the local-only approach kNN among them. As one of the approaches, the proposed method was able to detect faults with an accuracy of 94.8% and alternative methods were the centralized one (92.3%) and the local-only (85.7%). Furthermore, the average time taken to detect the anomaly for our proposed methodology was 0.74 seconds, which is faster than the performance of centralized one (1.12 seconds) and local-only as well (0.85 seconds). Moreover, it is exhibited as an efficiency feature of the model to detect faults rapidly and accurately, which makes it appropriate for the real-time applications of smart grids.

The performance of the suggested model may be underscored by its ability to effectively utilize the distinctive characteristics of each node's data by localized training and at the same time, receiving the benefit of the aggregation of the global model. The federated approach was the one easing the problem of data heterogeneity that was a big obstacle for the centralized model. The fact that the nodes kept their data locally was a very nice aspect of the federated learning model that saved privacy concerns which is an urgent issue in smart grid applications.

The proposed model was evaluated using accuracy, precision, recall, and F1-score, achieving results of 94.8%, 93.6%, 95.2%, and 94.4% respectively. Visual comparisons (Figure 2) highlight improvements over centralized and local models, reinforcing the efficacy of our federated approach. Discussions should explicitly detail reasons for performance improvement, such as reduced data heterogeneity impacts and efficient handling of privacy concerns.

Federated learning's flexibility in communication overhead and use of processing resources was not only a great presence beside the accuracy but also the main key to applying it to industrial point of view. The lightweight models at the node level were established in harmony with the limited computational capabilities of edge devices like smart meters and sensors. In addition, the use of the parameter-sharing mechanism allowed for minimizing the amount of data sent to the central server, thereby lowering the bandwidth usage and ensuring scalability for large-scale deployments.

Despite the excellent accuracy of the centralized model from the analysis, a few drawbacks were noticed. In this manner, there are potential threats stemming from both the need to collect personal information and the fact that the central server and its data are vulnerable to attacks. On the other hand, it was observed that the centralized method was facing a major problem in terms of data heterogeneity because the global model could not flexibly respond to the local characteristics of the individual nodes. These findings reveal the necessity of the application of decentralized techniques and namely federated learning for anomaly detection, in systems that are distributed.

The community-only model, while securing data privacy, recorded the lowest results across all measures. The non-participating nodes limited its capability to learn from the greater dataset which in turn caused reduced accuracy and lower recall scores. This is indicative of the value of federated learning, which adds to the benefits of local training the intelligence of the global model.

The findings of the test also showed the success of the anomaly detection engine that was built into the recommended framework. As shown in Figure 2, through the global model the engine monitors the whole network for anomalies in real-time, creating alerts and diagrams to help grid operators identify issues and solve them. This capacity for real-time events is indispensable to maintain the resilient and reliable operations of power grid systems particularly against the potential risks from cyber threats and errors in the system.

The proposed multi-source data fusion methodology

resulted in marked improvements in the accuracy of identifying anomalies by relying on spatially and temporally correlated information across grid nodes. In our experiments, models trained with single-source data (smart meter or substation-only features) achieved an accuracy of 89.5%, whereas the fused multi-source model attained the best target of 94.8% accuracy. And 17% of the false alarms were also reduced, as the fusion process dampened the effect of isolated sensor noise. The results prove that the diversity of information sources is the basis of effective decision-making, and thus the federated learning model is more resilient against adversarial data injection attacks and transient grid phenomena.

The proposed federated learning framework is structured in such a way that it can keep on updating itself with newly collected data from smart grid nodes. This model provides the flexibility to adapt to the changing conditions on the grid and new forms of anomalies like emerging cyber threats and equipment failures. Local models using the federated learning approach can update their parameters in real-time, resulting in the growth of a unified model unlike static models which are essentially stored in a single location simply to be trained in batches.

Nonetheless, federated learning is the first step to the development of this model but changes should be made to guarantee that it works efficiently in the long run. Some continuous learning techniques such as elastic weight consolidation (EWC) and experience replay could be introduced to stop the phenomenon of catastrophic forgetting and keep model updates seamless. On top of that, finite history-based reinforcement learning anomaly detection could be applied to change the threshold for anomalies to suit the tendencies shown in charts. The future projects will be concentrated on putting these techniques into practice so that they may significantly develop both the agility and strength of federated learning modeling in a dynamic smart grid environment.

To sum up, the proposed federated learning framework demonstrates the potential in overcoming the challenges of the anomaly detection in smart grids. Being data privacy-oriented, scaling well, and detecting with high accuracy, this framework could be a viable option for energy supply assurance and stability in modern energy systems. There will be research in the future which will seek the integration of advanced methods such as differential privacy and trust frameworks based on blockchain technology into federated learning in order to borrow from them the strengths of the existing ones and help in their vulnerability.

5 Conclusion

The goals of this study are to check most of the challenges that big data poses to different smart grid stakeholders. The above-mentioned advantages make federated learning a viable candidate for a decentralized anomaly-detection solution for the smart grid. The presented framework fuses information from multiple sources, collected from smart meters (IoT sensors), and substation controllers, to improve the accuracy of anomaly detection. Via decentralized learning the model, b), which removes the need for central storage and the associated risk of data leakage. The federated learning model guarantees that all components of the grid can contribute to the global model while safeguarding their privacy and independence. The developed model has been found to be superior based on the results obtained from the UCI Smart Grid Stability Dataset showing an achievement of 94.8%, which is higher than that of both the central models (92.3%) and the local-only models (85.7%). Additionally, the fusion of information led to a 17% reduction of false alarms, confirming the relevance of such an approach in mitigating erroneous anomaly detections.

While the proposed framework possesses several advantages, it still has some limitations. One of the most important factors affecting model convergence is the existing heterogeneity of the data, which can be highly diverse among the nodes. Also, the delay in communication over the network is still a major problem especially in vast situations whereby the sending and receiving parties have limited communication resources. In spite of the implementation of e model updates prompted by events, there is still a need for further improvements to enable real-time responses. In addition, the federated learning model remains vulnerable to adversarial attacks such as model poisoning, which necessitates the adoption of additional measures of security such as the chaining of differentially private data. Future research will explore the application of adaptive federated learning techniques as well as secure aggregation mechanisms that are intended to enhance the anomaly detection process in smart grids for both efficiency and security over the long term.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Kotenko, I., Saenko, I., Lauta, O., & Kribel, A. (2020). An approach to detecting cyber attacks against smart power grids based on the analysis of network traffic self-similarity. *Energies, 13*(19), 5031. [Crossref]

[2] Albarakati, A., Robillard, C., Karanfil, M., Kassouf, M., Debbabi, M., Youssef, A., ... & Hadjidj, R. (2021). Security monitoring of IEC 61850 substations using IEC 62351-7 network and system management. *IEEE Transactions on Industrial Informatics, 18*(3), 1641-1653. [Crossref]

[3] Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics, 12*(15), 3283. [Crossref]

[4] Husnoo, M. A., Anwar, A., Reda, H. T., Hosseinzadeh, N., Islam, S. N., Mahmood, A. N., & Doss, R. (2023). FedDiSC: A computation-efficient federated learning framework for power systems disturbance and cyber attack discrimination. *Energy and AI, 14*, 100271. [Crossref]

[5] Yen, S. W., Morris, S., Ezra, M. A., & Huat, T. J. (2019). Effect of smart meter data collection frequency in an early detection of shorter-duration voltage anomalies in smart grids. *International journal of electrical power & energy systems, 109*, 1-8. [Crossref]

[6] Abdel-Basset, M., Moustafa, N., & Hawash, H. (2022). Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach. *IEEE transactions on industrial informatics, 19*(1), 995-1005. [Crossref]

[7] Jung, O., Smith, P., Magin, J., & Reuter, L. (2019, May). Anomaly Detection in Smart Grids based on Software Defined Networks. In *SMARTGREENS* (pp. 157-164). [Crossref]

[8] Nanda, P., Rahman, H., & Mohanty, M. (2023, July). Anomaly Detection in Smart Grid Networks Using Power Consumption Data. In *20th International Conference on Security and Cryptography*. [Crossref]

[9] Anwar, A., & Mahmood, A. N. (2016). Anomaly detection in electric network database of smart grid: Graph matching approach. *Electric Power Systems Research, 133*, 51-62. [Crossref]

[10] Radoglou Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., & Panaousis, E. (2020). ARIES: A novel multivariate intrusion detection system for smart grid. *Sensors, 20*(18), 5305. [Crossref]

[11] Lee, S., Nengroo, S. H., Jin, H., Doh, Y., Lee, C., Heo, T., & Har, D. (2023). Anomaly detection of smart metering system for power management with battery storage system/electric vehicle. *ETRI Journal, 45*(4), 650-665. [Crossref]

[12] Maamar, A., & Benahmed, K. (2019). A hybrid model for anomalies detection in AMI system combining K-means clustering and deep neural network. *Comput. Mater. Continua, 60*(1), 15-39. [Crossref]

[13] Kanyama, M. N., Shava, F. B., Gamundani, A. M., & Hartmann, A. (2024). Machine learning applications for anomaly detection in Smart Water Metering Networks: A systematic review. *Physics and Chemistry of the Earth, Parts A/B/C, 134*, 103558. [Crossref]

[14] Fengming, Z., Shufang, L., Zhimin, G., Bo, W., Shiming, T., & Mingming, P. (2017). Anomaly detection in smart grid based on encoder-decoder framework with recurrent neural network. *The journal of china universities of Posts and Telecommunications, 24*(6), 67-73. [Crossref]

[15] Ganesan, P., & Xavier, S. (2023). An Intelligent Intrusion Detection System in Smart Grid Using PRNN Classifier. *Intelligent Automation & Soft Computing, 35*(3). [Crossref]

[16] Jithish, J., Alangot, B., Mahalingam, N., & Yeo, K. S. (2023). Distributed anomaly detection in smart grids: a federated learning-based approach. *IEEE Access, 11*, 7157-7179. [Crossref]

[17] Guato Burgos, M. F., Morato, J., & Vizcaino Imacaña, F. P. (2024). A review of smart grid anomaly detection approaches pertaining to artificial intelligence. *Applied Sciences, 14*(3), 1194. [Crossref]

[18] Gude Prego, J. J., de la Puerta, J. G., García Bringas, P., Quintián, H., & Corchado, E. (2021, September). Correction to: 14th International Conference on Computational Intelligence in Security for Information Systems and 12th International Conference on European Transnational Educational (CISIS 2021 and ICEUTE 2021). In *Computational Intelligence in Security for Information Systems Conference* (pp. C1-C1). Cham: Springer International Publishing. [Crossref]

[19] Chatzimiltis, S., Shojafar, M., & Tafazolli, R. (2023, May). A distributed intrusion detection system for future smart grid metering network. In *ICC 2023-IEEE International Conference on Communications* (pp. 3339-3344). IEEE. [Crossref]

[20] Shukla, S., Thakur, S., & Breslin, J. G. (2021, October). Anomaly detection in smart grid network

using FC-based blockchain model and linear SVM. In *International Conference on Machine Learning, Optimization, and Data Science* (pp. 157-171). Cham: Springer International Publishing. [Crossref]

[21] Wen, M., Xie, R., Lu, K., Wang, L., & Zhang, K. (2021). FedDetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid. *IEEE Internet of Things Journal*, *9*(8), 6069-6080. [Crossref]

[22] Su, Z., Wang, Y., Luan, T. H., Zhang, N., Li, F., Chen, T., & Cao, H. (2021). Secure and efficient federated learning for smart grid with edge-cloud collaboration. *IEEE Transactions on Industrial Informatics*, *18*(2), 1333-1344. [Crossref]

[23] Bashir, A. K., Khan, S., Prabadevi, B., Deepa, N., Alnumay, W. S., Gadekallu, T. R., & Maddikunta, P. K. R. (2021). Comparative analysis of machine learning algorithms for prediction of smart grid stability. *International Transactions on Electrical Energy Systems*, *31*(9), e12706. [Crossref]

Dr. Munir Ahmad is a distinguished professional with over 16 years of experience. He holds a Ph.D. in computer science from the School of Computer Science, National College of Business Administration and Economics, and a Master of Computer Science degree from the Virtual University of Pakistan. As the Executive Director/CIO at United International Group, Lahore, Pakistan, he has excelled in data management and resource optimization within multinational organizations. Munir Ahmad is renowned for his extensive research in sentiment analysis, AI applications in healthcare and animal facial identification. His expertise lies in data mining, big data, and artificial intelligence. (Email: munirahmad@korea.ac.kr)

Dr. Abdur Rehman holds the position of Associate Professor at the same institution and also serves as a Game Developer at GameObject in Lahore, Pakistan, drawing upon more than 10 years of enriched experience in the field of game development. With a proven academic track record, Abdur Rehman has contributed significantly to Smart City technologies, Healthcare, Machine Learning, Blockchain, Federated learning, and Network Security. His impactful research, spanning over a decade, has led to the publication of many research articles in highly impactful journals with notable impact factors. (Email: arbhatti@ncbae.edu.pk)