MSTS Methods in Science and Technology Studies

futuristech PT. Teknologi Futuristik Indonesia

Date of publication April 24, 2026, date of current version April 24, 2026.
*Digital Object Identifier* 10.64539/msts.v2i1.2026.462

Article

# Energy-Efficient Federated Learning with Temporal Convolutional Networks for Intrusion Detection

**Godfrey Perfectson Oise[1,*], Felix Oshiorenoya Uloko[2], Kevin Chinedu Pius[1], Roli Lydia Oshasha[3], Eric Edeigue Osemwegie[4], Immunhierokene Clinton Obrorindo[3]**

[1] Department of Computing, Wellspring University, Edo State, Nigeria; e-mail: godfrey.oise@wellspringuniversity.edu.ng (G. P. Oise), kevin.pius@wellspringuiversity.edu.ng (K. C. Pius).
[2] Department Computer Science, Veritas University, Abuja, Nigeria; e-mail: ulokof@veritas.edu.ng (F. O. Uloko).
[3] Department of computer science and information technology, Petroleum Training Institute, Effurun Delta State, Nigeria; e-mail: arenyeka_rl@pti.edu.ng (R. L. Oshasha), obrorindo_ci@pti.edu.ng (I. C. Obrorindo).
[4] Department of General studies, Edo State College of Health Sciences & Technology, Benin City 300104, Edo, Nigeria; e-mail: ericosemwegie@gmail.com (E. E. Osemwegie).
* Correspondence

The author(s) received no financial support for the research, authorship, and/or publication of this article.

**Abstract:** The rapid proliferation of Internet of Things (IoT) devices has significantly increased the attack surface of modern network infrastructures, necessitating intelligent and scalable intrusion detection systems. Federated Learning (FL) has emerged as a promising paradigm for distributed model training without centralized data sharing; however, challenges such as energy efficiency, data heterogeneity, and privacy preservation remain inadequately addressed. Existing studies often emphasize optimization objectives theoretically without validating them under realistic constraints. This paper proposes an energy-aware federated learning framework integrating Temporal Convolutional Networks (TCNs) for intrusion detection using distributed network traffic data. The framework incorporates differential privacy for secure model updates and a conceptual energy-aware client participation strategy. Experiments are conducted on the UNSW-NB15 dataset under a controlled setting with fixed client participation and communication parameters. The results demonstrate that the proposed model achieves improved classification accuracy and stable convergence behavior across communication rounds while operating under a fixed energy budget. However, energy consumption remains constant due to controlled experimental conditions, indicating that the study evaluates performance under energy constraints rather than dynamic energy optimization. The findings highlight the effectiveness of TCN-based federated models for intrusion detection in resource-constrained environments. Future work will focus on dynamic energy modeling, heterogeneous client environments, and comprehensive multi-objective evaluation.

**Keywords:** Federated Learning; Intrusion Detection System; Temporal Convolutional Network; Energy-Efficient Computing; Differential Privacy; IoT Security; Distributed Machine Learning.



## 1. Introduction

The rapid proliferation of Internet of Things (IoT) technologies and the evolution of cloud computing have significantly transformed modern network infrastructures. In particular, the adoption of multi-cloud environments, where services and workloads are distributed across multiple cloud providers, has enhanced system scalability, flexibility, and resilience [1]. However, this paradigm simultaneously introduces substantial security challenges due to heterogeneous infrastructures, distributed traffic flows, and cross-domain communication channels, which collectively expand the cybersecurity threat surface [2]. As a result, ensuring robust and scalable intrusion detection in such environments has become a critical concern.

Traditional intrusion detection systems (IDS), originally designed for centralized network architectures, are increasingly inadequate in multi-cloud settings [3]. These systems rely on aggregating network traffic data at a central location, which raises significant concerns related to scalability, privacy preservation, and communication

overhead. Furthermore, centralized approaches introduce single points of failure and are often incompatible with data sovereignty regulations and organizational privacy policies, particularly in distributed cloud environments [4], [5]. These limitations highlight the need for decentralized and privacy-preserving intrusion detection mechanisms capable of operating efficiently across multiple domains.

Recent advances in deep learning have significantly improved intrusion detection performance by enabling automatic feature extraction and modeling of complex spatial–temporal patterns in network traffic data [6]. Architectures such as convolutional neural networks, recurrent neural networks, and hybrid models have demonstrated strong classification capabilities on benchmark cybersecurity datasets. Despite these advancements, most deep learning-based intrusion detection models assume centralized data availability, requiring the aggregation of raw traffic data into a single training location [7]. This assumption limits their applicability in multi-cloud environments, where data sharing is restricted due to privacy, regulatory, and operational constraints.

Federated Learning (FL) has emerged as a promising paradigm to address these challenges by enabling decentralized model training without requiring raw data sharing [8]. In this approach, client nodes train models locally on their respective datasets and share only model updates with a central aggregator, thereby preserving data privacy while enabling collaborative learning. This paradigm aligns naturally with multi-cloud architectures, where data remains confined within individual domains [9]. However, despite its advantages, FL introduces several practical challenges that remain insufficiently addressed in existing research.

These challenges include communication overhead, computational energy consumption, statistical heterogeneity arising from non-identically distributed (non-IID) data, and privacy risks associated with model updates [10], [11]. In real-world multi-cloud deployments, iterative synchronization among geographically distributed clients incurs non-negligible communication and energy costs [12]. Additionally, non-IID data distributions across clients can lead to gradient divergence, slowing convergence and degrading global model performance. The integration of differential privacy mechanisms, while enhancing security, introduces additional noise into the training process, which may further affect convergence stability and model accuracy.

Existing studies often address these challenges in isolation and frequently emphasize optimization objectives theoretically without providing comprehensive empirical validation [13]. For example, frameworks such as FL-TEAR incorporate energy-aware strategies for routing in Fog–Cloud–IoT environments, demonstrating improvements in trust evaluation, energy efficiency, and communication performance [14]. Similarly, federated reinforcement learning-based approaches have been proposed to jointly optimize security, efficiency, and privacy, achieving high detection accuracy and reduced latency under controlled experimental conditions [15]. However, these approaches often assume dynamic optimization behavior without adequately validating system-level trade-offs under realistic constraints, leading to a gap between theoretical formulations and practical applicability.

Another limitation in current research is the limited exploration of advanced temporal models within federated intrusion detection systems. Temporal Convolutional Networks (TCNs) have demonstrated strong capability in modeling sequential data due to their ability to capture long-range dependencies through dilated convolutions and residual connections. These characteristics make TCNs particularly suitable for analyzing network traffic sequences. However, their integration within federated learning frameworks for intrusion detection remains underexplored, particularly in the context of resource-constrained and privacy-sensitive environments.

To address these limitations, this paper proposes an energy-aware federated learning framework that integrates a TCN-based architecture for intrusion detection in distributed multi-cloud environments. The framework incorporates differential privacy to ensure secure model updates and considers energy efficiency as a design constraint. Unlike prior studies that assume dynamic optimization of multiple objectives, this work evaluates model performance under a controlled experimental setting in which client participation, communication frequency, and computational workload are fixed. Consequently, energy consumption remains constant across communication rounds, and the study focuses on analyzing classification performance under constrained resource conditions rather than demonstrating explicit optimization trade-offs.

The contributions of this paper are reflected in the design and evaluation of a federated intrusion detection framework that leverages Temporal Convolutional Networks for improved sequential pattern learning, integrates differential privacy for enhanced security, and operates within a controlled energy-aware setting. The study further provides a comprehensive evaluation using standard classification metrics to assess model performance under distributed training conditions.

The remainder of this paper is organized as follows: Section 2 reviews related work. Section 3 presents the proposed methodology. Section 4 and 5 discusses the experimental results and analysis. Section 6 concludes the paper and outlines future research directions.

## 2. Literature Review

The rapid expansion of cloud computing has significantly transformed modern information systems, enabling scalable and distributed service delivery across geographically dispersed infrastructures [16]. In particular, multi-cloud architectures, where services are deployed across

multiple cloud providers, have gained prominence due to their flexibility, redundancy, and performance advantages. However, this distributed paradigm introduces complex cybersecurity challenges [17]. The heterogeneity of platforms, dynamic resource provisioning, and cross-cloud communication channels expand the attack surface and complicate centralized monitoring. Traditional intrusion detection systems (IDS), which are primarily signature-based or rule-driven, were originally designed for static and centralized environments and often struggle to detect sophisticated or zero-day attacks in distributed cloud ecosystems [18], [19].

To overcome the limitations of conventional IDS, machine learning techniques were introduced to enhance anomaly detection capabilities. Classical models such as Support Vector Machines, Decision Trees, and Random Forests demonstrated improved detection performance by learning statistical patterns from network traffic features. Nevertheless, these approaches rely heavily on manual feature engineering and often fail to capture the high-dimensional and nonlinear characteristics of modern network traffic data [20]. The emergence of deep learning further advanced intrusion detection by enabling automatic hierarchical feature extraction. Convolutional Neural Networks (CNNs) effectively capture spatial relationships among traffic features, while recurrent architectures such as Long Short-Term Memory (LSTM) networks model temporal dependencies in sequential data [21]. Hybrid CNN–LSTM architectures have demonstrated strong performance on benchmark datasets by jointly learning spatial and temporal attack patterns. For example, a CNN-based intrusion detection framework evaluated on the UNSW-NB15 dataset achieved high classification accuracy while improving interpretability through visualization techniques such as Grad-CAM, highlighting the relevance of key traffic features in decision-making [22]. Despite their strong predictive performance, these deep learning approaches typically assume centralized data availability, which limits their applicability in multi-cloud environments where data sharing is constrained by privacy regulations and organizational policies.

Federated Learning (FL) has emerged as a promising paradigm for distributed training without direct data exchange. By allowing client nodes to compute local updates and share model parameters instead of raw data, FL preserves data locality while enabling collaborative model learning [23], [24]. Federated optimization algorithms, particularly Federated Averaging (FedAvg), have been widely adopted across domains including mobile computing, healthcare, IoT, and cybersecurity. In intrusion detection applications, federated CNN-based and anomaly detection models have demonstrated competitive performance compared to centralized approaches while reducing the exposure of sensitive network traffic data. However, most federated IDS frameworks primarily focus on improving detection accuracy, often treating system-level constraints such as communication overhead, energy consumption, and client heterogeneity as secondary considerations rather than integral components of the learning process.

A major challenge in federated learning is statistical heterogeneity resulting from non-identically distributed (non-IID) client datasets. In multi-cloud environments, different cloud providers host diverse applications and user populations, leading to skewed traffic distributions across nodes [25]. This heterogeneity can increase gradient divergence, slow convergence, and degrade global model performance. Various techniques, including proximal regularization, control variates, and adaptive aggregation strategies, have been proposed to mitigate these effects. While such methods improve convergence behavior, their integration into intrusion detection systems often lacks a clear connection to practical deployment constraints such as communication efficiency and energy usage.

Privacy preservation represents another important research direction in federated learning. Although FL reduces the need for raw data sharing, model updates remain vulnerable to attacks such as gradient inversion and membership inference. To enhance privacy, techniques such as Differential Privacy (DP) and cryptographic methods have been incorporated into federated pipelines. Differential Privacy introduces calibrated noise into model updates to provide formal privacy guarantees; however, this noise can increase training variance and affect model accuracy. Existing studies often examine privacy and accuracy in isolation, without fully considering how privacy mechanisms interact with system-level constraints such as communication overhead and computational resources.

Energy efficiency and communication cost are also critical concerns in federated learning, particularly in geographically distributed infrastructures. Periodic synchronization of model updates requires the transmission of high-dimensional parameters, leading to significant bandwidth usage and energy consumption [26]. To address these challenges, several approaches have been proposed, including communication compression, model quantization, adaptive synchronization, and client selection strategies [27]. While these methods demonstrate improvements in efficiency, they are often implemented as heuristic optimizations rather than being systematically evaluated within the broader learning framework. Moreover, explicit modeling and empirical validation of energy behavior in federated intrusion detection systems remain limited, particularly in multi-cloud environments where resource constraints directly influence scalability and deployment feasibility [28].

The current literature on federated intrusion detection remains fragmented across multiple research directions. Deep learning-based approaches primarily emphasize predictive accuracy, federated learning frameworks

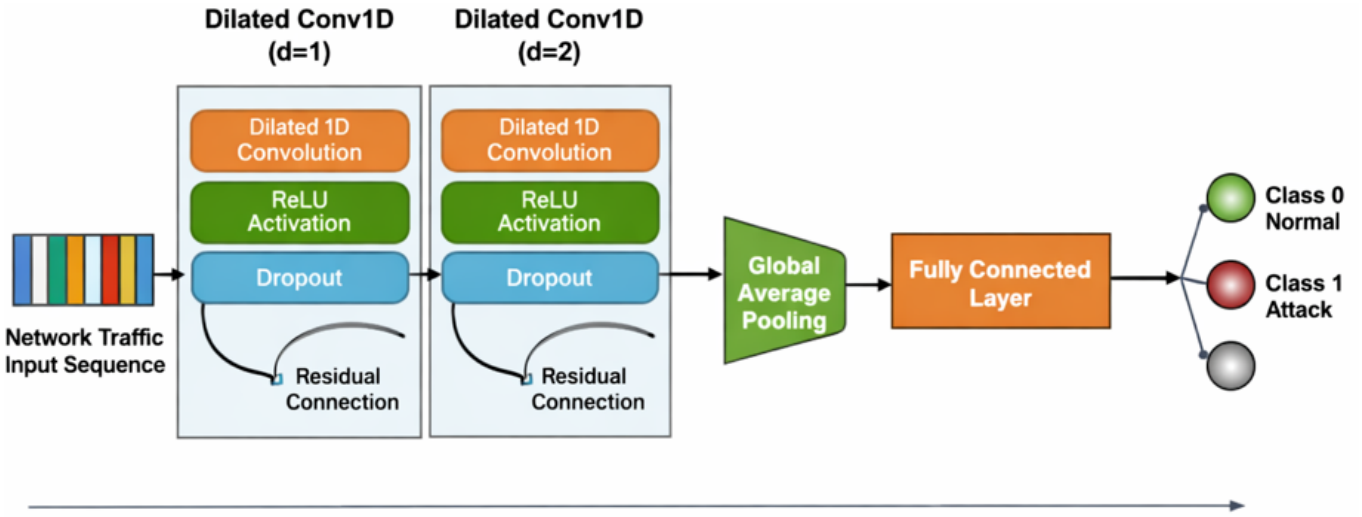


**Figure 1.** Temporal Convolutional Network (TCN) Architecture.

focus on privacy-preserving distributed training, and resource-aware techniques address communication and energy efficiency independently [29], [30]. As a result, many existing systems achieve strong performance in isolated aspects but lack a unified and realistic evaluation that reflects the combined impact of privacy, heterogeneity, and resource constraints.

Motivated by these limitations, this study proposes an energy-aware federated learning framework that integrates Temporal Convolutional Networks (TCNs) for intrusion detection [31]. Unlike prior works that emphasize theoretical optimization without sufficient experimental validation, this approach focuses on evaluating model performance under controlled and resource-constrained conditions. By explicitly acknowledging fixed energy settings and practical deployment constraints, the proposed framework aims to bridge the gap between theoretical design and empirical evaluation in federated intrusion detection systems.

## 3. Methodology

### 3.1. System Overview

The proposed framework adopts an energy-aware federated learning approach for privacy-preserving intrusion detection in multi-cloud environments. In this framework, network traffic data are distributed across multiple clients, where each client locally trains a Temporal Convolutional Network (TCN) model. Instead of sharing raw data, clients transmit model updates to a central server, where global aggregation is performed. This decentralized training paradigm preserves data privacy while enabling collaborative learning across distributed environments. Differential privacy mechanisms are incorporated during local training to enhance the security of shared updates. The overall training process is conducted iteratively across multiple communication rounds, allowing the global model to progressively improve its classification performance under controlled experimental conditions.

### 3.2. Dataset Description and Pre-processing

The experimental evaluation utilizes the UNSW-NB15 dataset, which provides a comprehensive representation of modern network traffic and attack scenarios [29], [32]. The dataset was generated using the IXIA Perfect Storm tool within the Cyber Range Lab at the Australian Centre for Cyber Security and includes both real and synthetically generated attack traffic. It consists of nine attack categories, including Fuzzers, Analysis, Backdoors, Denial of Service, Exploits, Generic, Reconnaissance, Shellcode, and Worms, with a total of 49 extracted features derived using Argus and Bro-IDS tools [33]. For the purpose of this study, the dataset is transformed into a binary classification problem, where Class 0 represents normal traffic and Class 1 represents attack traffic. Preprocessing steps include the removal of missing or corrupted records, one-hot encoding of categorical features, normalization of numerical attributes to zero mean and unit variance, and random shuffling to reduce sampling bias. To simulate a federated learning environment, the dataset is partitioned into multiple client subsets, ensuring that raw data remain localized at each client.

### 3.3. Temporal Convolutional Network (TCN) Architecture

The core learning model in this study is based on a Temporal Convolutional Network (TCN), designed to effectively capture sequential dependencies in network traffic data. The TCN is particularly suitable for time-series analysis due to its ability to model long-range temporal patterns while maintaining computational efficiency. The model takes as input a traffic sequence of size L×F, where L denotes the sequence length and F represents the number of features. As illustrated in Figure 1, the architecture consists of stacked TCN blocks with increasing dilation factors. Each TCN block comprises a dilated one-dimensional convolutional (Conv1D) layer, followed by a Rectified Linear Unit (ReLU) activation and a dropout layer for regularization. A residual (skip) connection is applied

within each block to improve gradient flow and stabilize training. The extracted feature representations are then passed through a global average pooling layer to reduce dimensionality, followed by a fully connected layer. Finally, a Softmax activation function is applied to classify the input into normal and attack traffic. This design provides a balance between modeling capability and computational efficiency, making it suitable for intrusion detection in distributed and resource-constrained environments.

### 3.4. Federated Learning Process

The federated learning process involves iterative communication between clients and a central server. During each communication round, selected clients perform local training on their respective datasets for a fixed number of epochs using stochastic gradient descent. The resulting model updates are then transmitted to the central server, where they are aggregated using a weighted averaging strategy based on local dataset sizes. Differential privacy is enforced by applying gradient clipping and Gaussian noise injection to local updates before transmission, thereby limiting the risk of information leakage. Although an energy-aware client selection mechanism and weighted aggregation strategy are conceptually defined, they are not dynamically activated in this study due to the use of uniform client configurations and fixed participation settings.

### 3.5. Energy Model

Energy consumption within the framework is defined as a function of local computation, communication cost, and the number of participating clients. Local computation energy is proportional to the size of the dataset and model complexity, while communication energy depends on the size of transmitted model parameters. However, in this study, these factors are held constant across all communication rounds by fixing the number of participating clients, model size, and communication frequency. As a result, total energy consumption remains invariant throughout the training process and serves as a controlled experimental constraint rather than an actively optimized variable. This design allows the study to focus on evaluating classification performance under fixed resource conditions rather than demonstrating dynamic energy optimization.

### 3.6. Evaluation Metrics

The performance is evaluated using standard classification metrics:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

Both macro-average and weighted-average metrics are also computed to evaluate model performance across different class distributions.

## 4. Results

The proposed energy-efficient federated learning framework integrated with a Temporal Convolutional Network (TCN) was evaluated on the UNSW-NB15 dataset under controlled conditions. The results demonstrate strong intrusion detection performance while maintaining fixed energy consumption. Global model accuracy improved consistently across five federated rounds, increasing from 82.01% to 94.36%, indicating effective convergence through iterative aggregation of distributed client updates. Despite this improvement, total energy consumption remained constant at 14,480,156,790 units due to fixed client participation, communication frequency, and computational workload, confirming that performance gains were achieved without additional energy cost.

The model achieved an overall classification accuracy of approximately 94%, with strong evaluation metrics including precision (96.56%), recall (93.05%), F1-score (94.77%), specificity (95.96%), balanced accuracy (94.51%), and a Matthews Correlation Coefficient (MCC) of 0.8873. These results indicate a balanced trade-off between accurate attack detection and low false alarm rates. Confusion matrix analysis shows that the model correctly classified 7118 normal instances and 8421 attack instances, with 300 false positives and 628 false negatives. The low false-positive rate reflects effective minimization of unnecessary alerts, while the moderate false-negative rate suggests some missed attacks that may require further refinement.

The Receiver Operating Characteristic (ROC) curve further confirms strong model performance, with an Area Under the Curve (AUC) of 0.9825, indicating excellent separability between normal and malicious traffic. Overall, the results validate that the proposed federated TCN framework achieves high accuracy, stable convergence, and robust detection capability under fixed energy constraints, demonstrating its suitability for privacy-preserving intrusion detection in distributed environments.

Table 1 presents the global model accuracy and total energy consumption across five federated learning rounds. The global accuracy consistently improves from 82.01% in Round 1 to 94.36% in Round 5, demonstrating the effectiveness of iterative federated training. The total computation and communication energy remains constant at 14,480,156,790 units across all rounds, indicating that the energy-aware scheduling and weighted aggregation

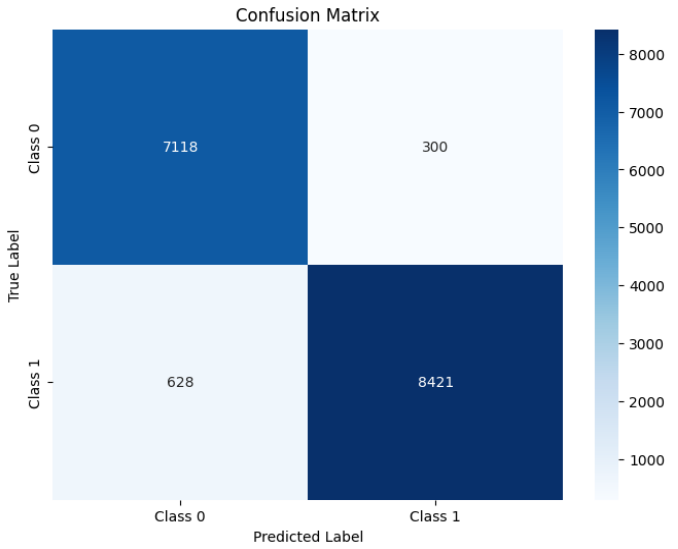


**Figure 2.** Confusion Matrix of the Federated TCN Model.

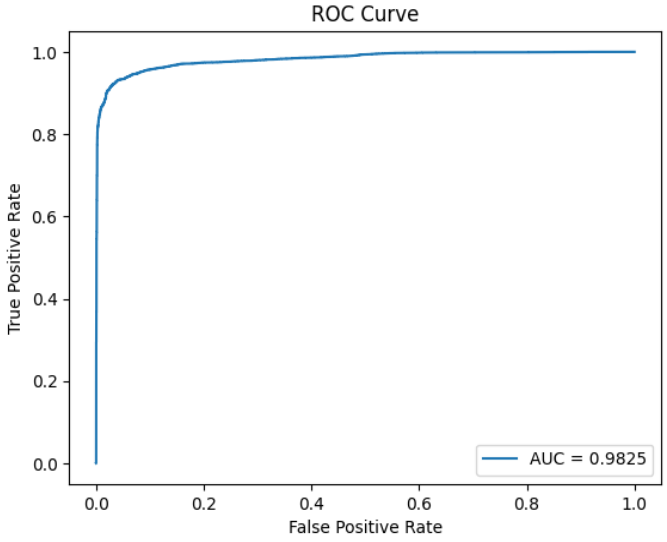


**Figure 3.** Receiver Operating Characteristic (ROC) Curve.

**Table 1.** Global Accuracy and Energy Across Federated Rounds.

| Round | Global Accuracy | Total Energy |
|---|---|---|
| 1 | 0.8201 | 14,480,156,790 |
| 2 | 0.8555 | 14,480,156,790 |
| 3 | 0.8990 | 14,480,156,790 |
| 4 | 0.9302 | 14,480,156,790 |
| 5 | 0.9436 | 14,480,156,790 |

**Table 2.** Classification Performance Report.

| Class | Precision | Recall | F1-Score | Support |
|---|---|---|---|---|
| 0 (Normal) | 0.92 | 0.96 | 0.94 | 7418 |
| 1 (Attack) | 0.97 | 0.93 | 0.95 | 9049 |
| **Accuracy** | | | **0.94** | 16467 |
| **Macro Avg** | 0.94 | 0.95 | 0.94 | 16467 |
| **Weighted Avg** | 0.94 | 0.94 | 0.94 | 16467 |

**Table 3.** Additional Evaluation Metrics.

| Metric | Value |
|---|---|
| Specificity | 0.9596 |
| Negative Predictive Value (NPV) | 0.9189 |
| Matthews Correlation Coefficient (MCC) | 0.8873 |
| Balanced Accuracy | 0.9451 |

mechanism efficiently manages client participation without increasing system energy expenditure. This table highlights the framework's ability to achieve high predictive performance while maintaining energy efficiency in a multi-client federated setting.

Table 2 summarizes the classification performance of the federated TCN model on the test dataset. The model achieves an overall accuracy of 94%, with high precision and recall for both classes, demonstrating effective detection of normal and attack traffic. Additional metrics in Table 3 indicate strong model reliability, including a specificity of 95.96%, a balanced accuracy of 94.51%, and a Matthews Correlation Coefficient (MCC) of 0.8873. These results confirm that the proposed framework maintains high predictive performance while preserving energy efficiency and privacy.

Figure 2 shows the performance of the energy-aware differentially private federated TCN model on the UNSW-NB15 test set. The confusion matrix shows 7118 true negatives, 300 false positives, 628 false negatives, and 8421 true positives. This indicates the model accurately identifies the majority of normal traffic and effectively detects malicious instances, with relatively few false alarms and moderate missed detections. Key performance metrics include accuracy ≈ 94.36%, precision ≈ 96.56%, recall ≈ 93.05%, and F1-score ≈ 94.77%, demonstrating strong discriminative capability and reliability in detecting attacks while maintaining a low false positive rate.

Figure 3 shows the ROC curve of the federated TCN model on the UNSW-NB15 dataset. The curve rises sharply toward the top-left corner, indicating high sensitivity even at low false-positive rates. With an AUC of 0.9825, the model demonstrates excellent separability between normal and attack classes, indicating near-optimal classification performance and robust detection under privacy-preserving federated learning.

## 5. Discussion

The experimental results demonstrate that the proposed energy-efficient federated learning framework with a Temporal Convolutional Network (TCN) achieves strong performance in intrusion detection under controlled and resource-constrained conditions [34]. The steady increase in global model accuracy across federated rounds confirms the effectiveness of decentralized training in learning meaningful patterns from distributed network traffic data. This indicates that the federated aggregation process successfully integrates knowledge from multiple clients despite the absence of raw data sharing.

A key observation from the results is the model's ability to maintain high classification performance while operating under a fixed energy budget. Unlike many existing studies that assume dynamic optimization of energy consumption, this work evaluates performance under constant energy conditions. The findings show that accuracy improvements are achieved without increasing computational or communication costs, suggesting that the proposed framework is suitable for deployment in environments where energy resources are limited or strictly regulated, such as IoT and multi-cloud systems.

The classification metrics further highlight the robustness of the model. High precision indicates a low false-positive rate, which is critical in intrusion detection systems to avoid unnecessary alerts and reduce administrative overhead. Similarly, the strong recall value demonstrates the model's capability to detect the majority of attack instances. However, the presence of some false negatives suggests that certain attack patterns may not be fully captured, possibly due to the effects of differential privacy noise or limitations in representing highly complex attack behaviors [35].

The confusion matrix analysis reinforces these observations by showing that the model effectively distinguishes between normal and malicious traffic, with relatively few misclassifications. The ROC curve and high AUC value further confirm the model's strong discriminative ability, indicating that it performs well across different classification thresholds. This robustness is particularly important in real-world scenarios where operating conditions and decision thresholds may vary [36].

The integration of differential privacy introduces an important trade-off between privacy and model performance. While privacy-preserving mechanisms enhance the security of model updates, they may also introduce noise that affects convergence and accuracy. Despite this, the model maintains high performance, suggesting that the chosen privacy configuration achieves a reasonable balance between security and utility [37].

Another important aspect of this study is the use of Temporal Convolutional Networks within a federated learning framework. The results indicate that TCNs are effective in capturing temporal dependencies in network traffic data, contributing to improved detection performance. Compared to traditional sequential models such as recurrent neural networks, TCNs offer advantages in parallelization and computational efficiency, making them well-suited for distributed and resource-constrained environments [38].

However, the study has certain limitations. The experimental setup assumes homogeneous client configurations and fixed participation, which may not fully reflect real-world federated learning environments characterized by client heterogeneity, intermittent availability, and varying resource capacities. Additionally, the energy model is static, meaning that the framework does not dynamically adapt to changing energy conditions or optimize energy consumption during training [39].

Future research should address these limitations by incorporating dynamic energy-aware client selection, adaptive communication strategies, and heterogeneous data distributions. Further investigation into optimizing the balance between privacy and performance is also necessary, particularly in scenarios involving stronger privacy guarantees. Extending the framework to multi-class intrusion detection and real-time deployment scenarios would also enhance its practical applicability [40].

The proposed framework effectively bridges the gap between theoretical design and practical implementation by demonstrating strong intrusion detection performance under realistic constraints. The integration of federated learning, differential privacy, and TCN-based modeling provides a promising direction for developing scalable, secure, and energy-efficient intrusion detection systems in modern distributed environments.

## 6. Conclusion

This paper proposed an energy-aware federated learning framework integrating a Temporal Convolutional Network (TCN) for privacy-preserving intrusion detection in distributed environments. The model was evaluated on the UNSW-NB15 dataset under controlled experimental conditions with fixed energy constraints. Results demonstrate consistent improvement in global model accuracy across federated rounds, achieving approximately 94.36% accuracy with strong precision, recall, and an AUC of 0.9825, indicating excellent classification performance. A key contribution of this study is the validation of model effectiveness under constant energy consumption, showing that high detection performance can be achieved without increasing computational or communication overhead. The integration of differential privacy further ensures secure model updates while maintaining performance stability. However, the framework assumes homogeneous clients and static energy conditions, which may limit real-world applicability. Future work will focus on dynamic energy optimization, heterogeneous client environments, and adaptive federated strategies to enhance scalability and robustness in practical deployments.

## 7. Declarations

### 7.1. Author Contributions

**Godfrey Perfectson Oise:** Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – Original Draft; **Felix Oshiorenoya Uloko:** Formal analysis, Investigation, Data Curation, Writing – Review & Editing; **Kevin Chinedu Pius:** Software, Validation, Data Curation, Visualization; **Roli Lydia Oshasha:** Investigation, Resources, Writing – Review & Editing; **Eric Edeigue Osemwegie:** Resources, Supervision, Project administration; **Immunhierokene Clinton Obrorindo:** Supervision, Writing – Review & Editing, Project administration.

### 7.2. Institutional Review Board Statement

Not applicable.

### 7.3. Informed Consent Statement

Not applicable.

### 7.4. Data Availability Statement

The dataset used in this study (UNSW-NB15) is publicly available at: https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15.

### 7.5. Acknowledgment

Not applicable.

### 7.6. Conflicts of Interest

The authors declare no conflicts of interest.

## 8. References

[1] V. K. Pandey, D. Sahu, S. Prakash, R. S. Rathore, P. Dixit, and I. Hunko, "A lightweight framework to secure IoT devices with limited resources in cloud environments," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025. https://doi.org/10.1038/S41598-025-09885-0.

[2] F. Cavallin and R. Mayer, "Anomaly Detection from Distributed Data Sources via Federated Learning," *Lecture Notes in Networks and Systems*, vol. 450, pp. 317–328, 2022. https://doi.org/10.1007/978-3-030-99587-4_27.

[3] H. G. A. Umar *et al.*, "Energy-efficient deep learning-based intrusion detection system for edge computing: a novel DNN-KDQ model," *Journal of Cloud Computing*, vol. 14, no. 1, Dec. 2025. https://doi.org/10.1186/S13677-025-00762-9.

[4] G. Nassreddine, M. Nassereddine, and O. Al-Khatib, "Ensemble Learning for Network Intrusion Detection Based on Correlation and Embedded Feature Selection Techniques," *Computers*, vol. 14, no. 3, Mar. 2025. https://doi.org/10.3390/COMPUTERS14030082.

[5] S. A. Oyedotun, G. P. Oise, and C. E. Ozobialu, "Towards Intelligent Cybersecurity in SCADA and DCS Environments: Anomaly Detection Using Multimodal Deep Learning and Explainable AI," *Journal of Science Research and Reviews*, vol. 2, no. 3, pp. 20–31, Jul. 2025. https://doi.org/10.70882/josrar.2025.v2i3.76.

[6] M. Abd Elaziz, I. A. Fares, A. Dahou, and M. Shrahili, "Federated learning framework for IoT intrusion detection using tab transformer and nature-inspired hyperparameter optimization," *Front. Big Data*, vol. 8, 2025. https://doi.org/10.3389/FDATA.2025.1526480.

[7] H. Alkahtani and T. H. H. Aldhyani, "Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications," *Security and Communication Networks*, vol. 2021, 2021. https://doi.org/10.1155/2021/3806459.

[8] G. P. Oise, B. S. Olanrewaju, O. A. Orukpe, K. C. Pius, and A. O. Airhiavbere, "A Convolutional Neural Network Framework for Intelligent Intrusion Detection," *Scientific Journal of Computer Science*, vol. 2, no. 1, pp. 50–59, Feb. 2026. https://doi.org/10.64539/sjcs.v2i1.2026.404.

[9] G. P. Oise *et al.*, "Isolation Forest–Based Intrusion Detection for Cyber-Physical Systems," *Scientific Journal of Engineering Research*, vol. 2, no. 2, pp. 222–233, Mar. 2026. https://doi.org/10.64539/sjer.v2i2.2026.434.

[10] J. Kim, M. Shim, S. Hong, Y. Shin, and E. Choi, "Intelligent detection of IoT botnets using machine learning and deep learning," *Applied Sciences (Switzerland)*, vol. 10, no. 19, pp. 1–22, Oct. 2020. https://doi.org/10.3390/app10197009.

[11] D. C. Attota, V. Mothukuri, R. M. Parizi, and S. Pouriyeh, "An Ensemble Multi-View Federated Learning Intrusion Detection for IoT," *IEEE Access*, vol. 9, pp. 117734–117745, 2021. https://doi.org/10.1109/ACCESS.2021.3107337.

[12] G. P. Oise, O. C. Nwabuokei, O. J. Akpowehbve, B. A. Eyitemi, and N. B. Unuigbokhai, "Towards Smarter Cyber Defense: Leveraging Deep Learning for Threat Identification and Prevention," *FUDMA Journal of Sciences*, vol. 9, no. 3, pp. 122–128, Mar. 2025. https://doi.org/10.33003/fjs-2025-0903-3264.

[13] M. M. Forootan, I. Larki, R. Zahedi, and A. Ahmadi, "Machine Learning and Deep Learning in Energy Systems: A Review," *Sustainability (Switzerland)*, vol. 14, no. 8, Apr. 2022. https://doi.org/10.3390/SU14084832.

[14] O. Shahid, V. Mothukuri, S. Pouriyeh, R. M. Parizi, and H. Shahriar, "Detecting Network Attacks using Federated Learning for IoT Devices," *Proceedings - International Conference on Network Protocols, ICNP*, 2021. https://doi.org/10.1109/ICNP52444.2021.9651915.

[15] P. Madan, V. Singh, D. P. Singh, M. Diwakar, B. Pant, and A. Kishor, "A Hybrid Deep Learning Approach for ECG-Based Arrhythmia Classification," *Bioengineering*, vol. 9, no. 4, Apr. 2022. https://doi.org/10.3390/bioengineering9040152.

[16] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Computer Networks*, vol. 204, no. 21, Feb. 2022. https://doi.org/10.1016/j.comnet.2021.108693.

[17] E. M. Campos *et al.*, "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges," *Computer Networks*, vol. 203, pp. 298–301, Feb. 2022. https://doi.org/10.1016/j.comnet.2021.108661.

[18] N. B. Unuigbokhai *et al.*, "Advancements In Federated Learning for Secure Data Sharing in Financial Services," *FUDMA Journal of Sciences*, vol. 9, no. 5, pp. 80–86, May 2025. https://doi.org/10.33003/fjs-2025-0905-3207.

[19] B. Olanrewaju-George and B. Pranggono, "Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models," *Cyber Security and Applications*, vol. 3, p. 100068, Dec. 2025. https://doi.org/10.1016/J.CSA.2024.100068.

[20] B. Wu, "A Wavelet-Based Derivative-Aware Transformer for Network Intrusion Detection," in *2025 22nd International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, IEEE, Dec. 2025. https://doi.org/10.1109/ICCWAMTIP68645.2025.11352641.

[21] G. P. Oise, "E-ViTNet: A lightweight vision transformer with oppositional cat swarm optimization for automated E-Waste sorting," *Next Research*, vol. 6, p. 101373, Apr. 2026. https://doi.org/10.1016/j.nexres.2026.101373.

[22] G. Oise and S. Konyeha, "Environmental impacts in e-waste management using deep learning," *Discover Artificial Intelligence*, vol. 5, no. 1, p. 210, Aug. 2025. https://doi.org/10.1007/s44163-025-00376-9.

[23] B. Wu, "A Wavelet-Based Derivative-Aware Transformer for Network Intrusion Detection," in *2025 22nd International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, IEEE, Dec. 2025. https://doi.org/10.1109/ICCWAMTIP68645.2025.11352641.

[24] Y. Wang, "A Network Intrusion Detection Method Based on Parameter Optimization and Transformer," in *2026 International Conference on Communication Networks and Machine Learning (CNML)*, IEEE, Jan. 2026, pp. 56–60. https://doi.org/10.1109/CNML68938.2026.11453115.

[25] G. P. Oise, T. Jessa, E. Mintah, F. O. Uloko, O. Sokoya, and O. Ukpebor, "A Hybrid Machine Learning–Optimization Framework for Energy Demand Forecasting and Decision Support in Smart Infrastructure," *Methods in Science and Technology Studies*, vol. 2, no. 1, pp. 68–81, Apr. 2026. https://doi.org/10.64539/msts.v2i1.2026.440.

[26] E. N. Yolaçan and H. Çavşı Zaım, "Temporal Windowed and Internal Feature (TWIF) Transformer for Attack Detection in Robotics," *IEEE Access*, vol. 14, pp. 42674–42690, 2026. https://doi.org/10.1109/ACCESS.2026.3674720.

[27] U. C. Akuthota and L. Bhargava, "Transformer-Based Intrusion Detection for IoT Networks," *IEEE Internet Things J.*, vol. 12, no. 5, pp. 6062–6067, Mar. 2025. https://doi.org/10.1109/JIOT.2025.3525494.

[28] M. Roopak, G. Y. Tian, and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," *2020 10th Annual Computing and Communication Workshop and Conference*, 2020. https://doi.org/10.1109/CCWC47524.2020.9031206.

[29] M. H. Kabir, M. S. Rajib, A. S. M. T. Rahman, Md. M. Rahman, and S. K. Dey, "Network Intrusion Detection Using UNSW-NB15 Dataset: Stacking Machine Learning Based Approach," in *2022 International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE)*, IEEE, Feb. 2022. https://doi.org/10.1109/ICAEEE54957.2022.9836404.

[30] A. Almomani *et al.*, "Phishing Website Detection With Semantic Features Based on Machine Learning Classifiers: A Comparative Study," *Int. J. Semant. Web Inf. Syst.*, vol. 18, no. 1, Jan. 2022. https://doi.org/10.4018/ijswis.297032.

[31] R. Ma, Q. Wang, X. Bu, and X. Chen, "Real-Time Detection of DDoS Attacks Based on Random Forest in SDN," *Applied Sciences (Switzerland)*, vol. 13, no. 13, Jul. 2023. https://doi.org/10.3390/app13137872.

[32] W. David, "UNSW_NB15," 2019, *The IXIA PerfectStorm tool. Australian Centre for Cyber Security (ACCS)*. https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15.

[33] S. Ahmed *et al.*, "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron," *Future Internet*, vol. 15, no. 2, Feb. 2023. https://doi.org/10.3390/fi15020076.

[34] R. Latha and R. M. Bommi, "Hybrid CatBoost Regression model based Intrusion Detection System in IoT-Enabled Networks," *Proceedings of the 9th International Conference on Electrical Energy Systems*, 2023. https://doi.org/10.1109/ICEES57979.2023.10110148.

[35] G. Guo, X. Pan, H. Liu, F. Li, L. Pei, and K. Hu, "An IoT Intrusion Detection System Based on TON IoT Network Dataset," *2023 IEEE 13th Annual Computing and Communication Workshop and Conference*, 2023. https://doi.org/10.1109/CCWC57344.2023.10099144.

[36] Z. Liu, N. Thapa, A. Shaver, K. Roy, X. Yuan, and S. Khorsandroo, "Anomaly detection on Iot network intrusion using machine learning," *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2020 - Proceedings*, Aug. 2020. https://doi.org/10.1109/icABCD49160.2020.9183842.

[37] Z. H. Abdaljabar, O. N. Ucan, and K. M. Ali Alheeti, "An Intrusion Detection System for IoT Using KNN and Decision-Tree Based Classification," *International Conference of Modern Trends in ICT Industry: Towards the Excellence in the ICT Industries, MTICTI 2021*, 2021. https://doi.org/10.1109/MTICTI53925.2021.9664772.

[38] S. K. Kodali and C. H. Muntean, "An Investigation into Deep Learning Based Network Intrusion Detection System for IoT Systems," *Proceedings of 2021 IEEE International Conference on Data Science and Computer Application, ICDSCA 2021*, pp. 374–377, 2021. https://doi.org/10.1109/ICDSCA53499.2021.9650111.

[39] P. O. Adebayo, M. Jubrin Abdulahi, O. M. Lawrence, Y. A. Ibrahim, S. A. Faki, and B. A. Hassan, "An Artificial Intelligence-based Ensemble Technique for Intrusion Detection and Prevention in IoT Systems," *International Conference on Science, Engineering and Business for Driving Sustainable Development Goals, SEB4SDG 2024*, 2024. https://doi.org/10.1109/SEB4SDG60871.2024.10629681.

[40] M. Ramaiah and M. Y. Rahamathulla, "Securing the Industrial IoT: A Novel Network Intrusion Detection Models," *2024 3rd International Conference on Artificial Intelligence for Internet of Things, AIIoT 2024*, 2024. https://doi.org/10.1109/AIIoT58432.2024.10574728.