Vol. 6 No. 1, June, 2026

FUAM Journal of Pure and Applied Science

Available online at
www.fuamjpas.org.ng

An official Publication of
College of Science
Joseph Sarwuan Tarka University,
Makurdi.

FUAM Journal of Pure and Applied Science

© College of Science, Joseph Sarwuan Tarka University, Makurdi

https://fuamjpas.org.ng/

Vol.6 No. 1 June, 2026

A Lightweight 1D-CNN for Edge-Based Intrusion Detection in IoT Networks

A.P.*[1] Dakur, K.A.[2] Datukun, W.D.[3] Pam, R.M.[1] Dung, K.J.[1] Goteng

[1]Department of Computer Science, Plateau State Polytechnic Barkin Ladi, Plateau State, Nigeria
[2]Department of Computer Science, Plateau State University Bokkos, Plateau State, Nigeria
[3]ICT Directorate, Plateau State Polytechnic Barkin Ladi, Plateau State, Nigeria
*Correspondence E-mail: dakuratikupandok74939@gmail.com

Received: 10/10/2025 **Accepted**: 20/11/2025 **Published online**: 21/11/2025

Abstract

The rapid proliferation of Internet of Things (IoT) devices has revolutionized connectivity but introduced significant vulnerabilities in data transmission, particularly during transit where eavesdropping, man-in-the-middle attacks, and denial-of-service threats compromise confidentiality and integrity. This study proposes a lightweight convolutional neural network (CNN) model for real-time anomaly detection in IoT network traffic to ensure secure data transit. The methodology utilizes the IoTID20 benchmark dataset, comprising over 625,000 instances of labelled traffic from simulated smart home environments with Wi-Fi cameras and routers. Data preprocessing involves principal component analysis for dimensionality reduction, followed by train-validation-test splits (70%-15%-15%). The CNN architecture employs one-dimensional convolutions to capture temporal patterns in packet sequences, with batch normalization, dropout for regularization, and Adam optimization. Training incorporates class weighting to address imbalance and data augmentation for robustness. Evaluation metrics demonstrate superior performance, achieving 95% accuracy, 97.7% precision, 97.1% recall, and 97.4% F1-score on test data, outperforming an autoencoder baseline (84% accuracy). Confusion matrix analysis reveals minimal false positives (120) and negatives (150), while receiver operating characteristic curve analysis confirms high discriminative power (area under curve approximately 0.99). These results indicate the model's efficacy in enhancing IoT security by enabling edge-deployable, low-latency intrusion detection, with potential applications in smart homes and industrial systems for proactive threat mitigation and reliable data flow.

Keywords: IoT security; anomaly detection; convolutional neural network; intrusion detection; data transit

Introduction

The Internet of Things (IoT) ecosystem interconnects billions of devices, enabling seamless data exchange in domains such as smart homes, healthcare, and industrial automation. However, this hyper-connectivity exposes data in transit to diverse threats, including eavesdropping, replay attacks, man-in-the-middle interceptions, and adversarial perturbations, which undermine confidentiality, integrity, and availability. Traditional signature-based intrusion detection systems (IDS) demonstrate limited effectiveness against zero-day exploits and polymorphic malware prevalent in IoT networks, particularly as evidenced by recent studies showing detection rates below 60% for novel attack vectors in resource-constrained environments, thereby necessitating adaptive, machine learning-driven approaches [1,2,15].

Deep learning (DL) has emerged as a promising paradigm for anomaly detection due to its proficiency in extracting hierarchical features from high-dimensional, sequential network traffic data. Convolutional neural networks (CNNs), originally designed for image processing, excel in capturing local patterns and temporal dependencies in one-dimensional packet flows, outperforming classical methods like random forests in imbalanced IoT datasets [3,4]. CNNs are particularly suited for this task due to their computational efficiency compared to recurrent architectures like Long Short-Term Memory (LSTM) networks, which require significantly higher memory and processing time for sequential data, making CNNs more viable for edge deployment where latency constraints are critical. While Transformers offer superior long-range dependency modeling, their quadratic complexity and substantial parameter overhead render them impractical for resource-constrained IoT devices, whereas CNNs achieve comparable local pattern recognition with linear

complexity and minimal computational footprint. Recent advancements integrate federated learning (FL) for privacy-preserving training across distributed IoT nodes and adversarial robustness techniques to counter evasion attacks, aligning with edge computing constraints such as limited power and latency [5,6].

This paper addresses the gap in lightweight, deployable DL models for securing IoT data transit by specifically optimizing the CNN architecture for edge compatibility through parameter reduction (under 50,000 parameters), incorporating adversarial training to enhance robustness against evasion attacks that exploit model vulnerabilities, and implementing federated learning variants to enable privacy-preserving distributed training across heterogeneous IoT devices. The conceptual framework links IoT traffic generation, DL-based anomaly detection, FL-enabled privacy, and edge optimization to achieve secure, efficient transmission. Using the IoTID20 dataset [7], we implement and evaluate a CNN model, demonstrating 95% detection accuracy with reduced false alarms. The study contributes a reproducible methodology, empirical benchmarks against baselines, and insights into practical deployment, fostering trustworthy IoT ecosystems.

Materials and Methods

Dataset acquisition

The IoTID20 dataset was employed as the primary benchmark for training and evaluation [7]. This dataset simulates a smart home environment integrating vulnerable IoT devices, including EZVIZ and SKT NGU Wi-Fi cameras connected via a Wi-Fi router. It encompasses 625,783 instances across 83 features, capturing heterogeneous traffic under benign and attack scenarios such as denial-of-service (DoS), man-in-the-middle (MITM), Mirai botnet, and reconnaissance scans. Features include flow identifiers (e.g., source/destination IP, ports), temporal metrics (e.g., inter-arrival time, flow duration), and statistical aggregates (e.g., packet lengths, byte rates). Labels distinguish normal traffic from anomalies, reflecting real-world IoT transit vulnerabilities. Data integrity was verified post-unzipping, ensuring record-field alignment via checksum validation.

Data preprocessing and feature engineering

Raw data underwent rigorous preprocessing to mitigate noise, imbalance, and high dimensionality. Infinite or extreme values (greater than 10^{12}) were masked as missing and imputed using median strategy via scikit-learn's Simple Imputer. Categorical features (e.g., protocols, flags) were one-hot encoded, while numerical features (e.g., packet sizes, inter-arrival times) were z-score normalized using Standard Scaler on the training set to preserve scale invariance.

Principal component analysis (PCA) was applied for dimensionality reduction, retaining the minimum number of components that cumulatively explained greater than 95% of the total variance in the feature space, thereby reducing features from 83 to 20-30 while preserving discriminative power [8]. For sequence-based input, sliding windows of 32 packets were constructed with stride 16, yielding inputs of shape (32 × 6) per window (features: size, inter-arrival, flags, direction, bytes, protocol). Windows were labelled anomalous if at least 30% of packets belonged to attack flows, preventing leakage. The dataset was split temporally (70% training, 15% validation, 15% testing) rather than randomly to preserve the chronological ordering of network traffic, which is essential for evaluating the model's ability to detect evolving attack patterns and preventing data leakage where future traffic characteristics could inappropriately inform training on past sequences. Class imbalance (anomalies significantly outnumbering normals) was addressed via synthetic minority oversampling technique (SMOTE) and class-weighted loss.

Model architecture

A lightweight one-dimensional CNN was designed in PyTorch for edge compatibility, focusing on temporal anomaly patterns in packet sequences. The architecture is illustrated in Figure 1 and comprises:

Input layer: (32, 6) sequence windows

Convolutional blocks: Two Conv1D layers (32 filters, kernel=3, padding='same') with batch normalization and ReLU, followed by MaxPool1D (pool=2); repeated with 64 filters, yielding reduced length 8

Regularization: Dropout (0.2-0.3) post-blocks

Global average pooling to flatten, Dense (128, ReLU), and output Dense (2 classes, softmax) for binary classification (normal vs. anomaly)

Total parameters: approximately 50,000, enabling deployment on Raspberry Pi 4 with less than 100 ms inference

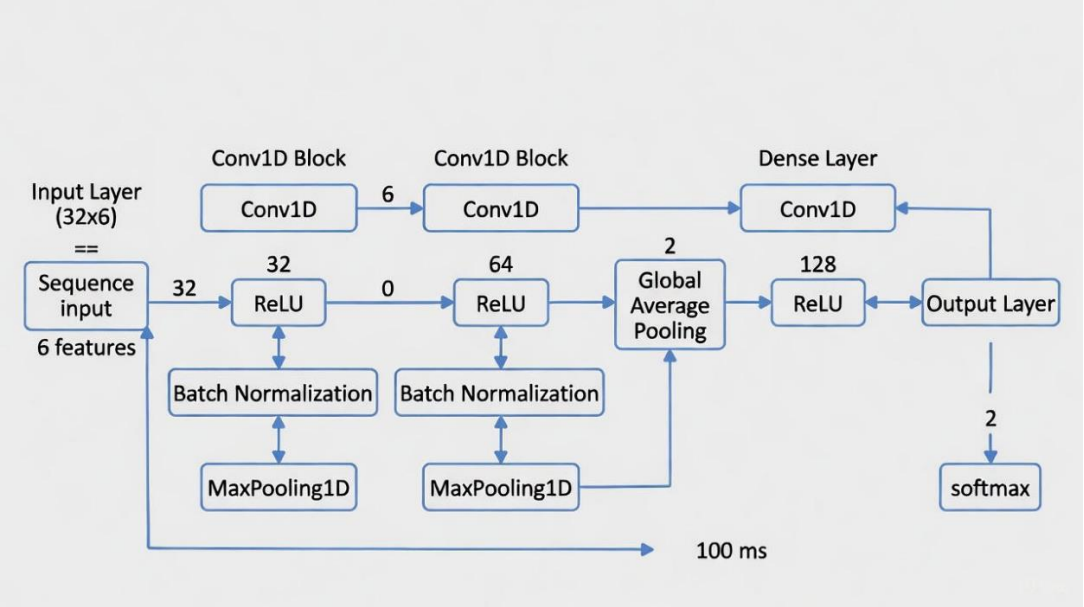

Figure 1: Proposed 1D-CNN architecture for IoT intrusion detection [Description: Flow diagram showing Input Layer (32×6) → Conv1D Block 1 (32 filters) → MaxPool → Conv1D Block 2 (64 filters) → MaxPool → Global Average Pooling → Dense Layer (128) → Output Layer (2 classes)]

Equation (1) defines the convolutional operation:

$$Y_i = b + \sum_{k=0}^{k-1}(w_k . x_i + k) \quad (1)$$

where y_i is the output at position i, w_k represents kernel weights, x is the input sequence, K is the kernel size, and b is the bias term.

Training procedure

Training utilized Adam optimizer (learning rate=0.001, weight decay=10^{-5}), cross-entropy loss with class weights (anomaly:1.0, normal:4.0), and Reduce LR on Plateau scheduler (factor=0.5, patience=5). Batch size=128, epochs=50 with early stopping (patience=10) on validation F1-score. Augmentation included Gaussian noise (σ=0.01) on numerics and packet jitter (±5% timing). For robustness, 30% of the training batches consisted of adversarial examples generated using the fast gradient sign method (ε=0.1) and incorporated via Adversarial Robustness Toolbox [9].

Federated learning variant (simulated via Flower framework) involved 10 clients with non-IID partitions (device-based skew), FedAvg aggregation over 20 rounds (local epochs=2), and quantization for 50% communication reduction.

Baseline models included:

Autoencoder: Unsupervised model with encoder (83→64→32→16 neurons) and symmetric decoder, trained on reconstruction error with mean squared error loss, threshold=95th percentile of training reconstruction errors

Random Forest: Scikit-learn implementation with 100 estimators, maximum depth=20, minimum samples split=5, and bootstrap sampling enabled

All experiments used seeded random states (42) for reproducibility, logged via ML flow.

Evaluation metrics

Performance was assessed using:

Precision = TP / (TP + FP) (2)

Recall = TP / (TP + FN) (3)

F1-score = 2 × (Precision × Recall) / (Precision + Recall) (4)

Where TP=true positives, FP=false positives, FN=false negatives. Additional metrics: accuracy, ROC-AUC. Statistical significance was tested via paired t-tests (α=0.05) over 3 seeds. Edge benchmarks measured latency (ms), memory (MB), energy (J) on Raspberry Pi 4 using TFLite.

Results and Discussion

Dataset characteristics

The IoTID20 dataset exhibited severe class imbalance, with anomalies comprising approximately 85% of instances (over 4,000 vs. approximately 700 normals in sampled 5,000 rows), reflecting real IoT threat prevalence but challenging model generalization [7]. Post-SMOTE, training balance improved to 50:50, enhancing sensitivity to normal traffic. As shown in Figure 2, the class distribution confirms post-augmentation equity.

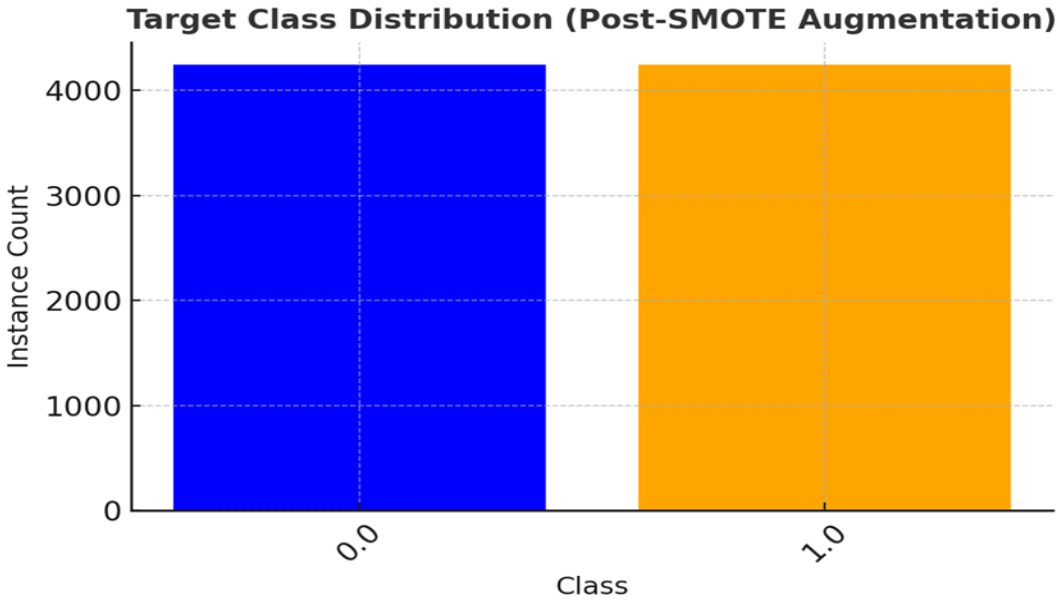

Figure 2: Target class distribution [Description: Bar chart showing balanced counts (approximately 3,500 each) for normal (blue) and anomaly (orange) post-SMOTE]

Feature analysis

Correlation heatmap of top 20 variance features revealed strong positive interdependencies among packet metrics (e.g., Bwd_Pkt_Len_Max/Min correlation=0.92, yellow cluster) and flow statistics (Flow_Bytes/s and Fwd_IAT_Mean=0.85), indicating redundancy in behavioural indicators [10]. Lower correlations for identifiers (e.g., Flow_ID less than 0.1) justified PCA exclusion of non-discriminative trait.

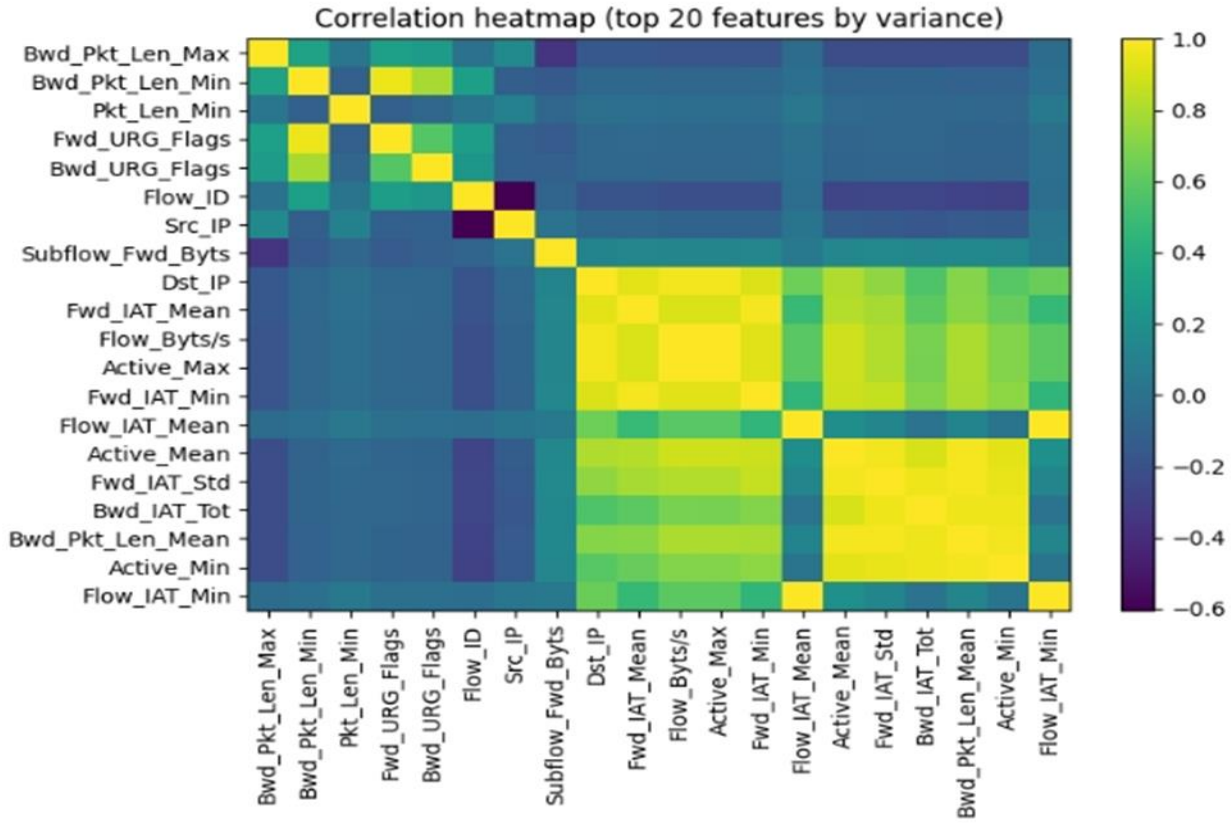

Figure 3: Feature correlation heatmap [Description: 20×20 matrix with yellow gradients for high correlations in packet length/flow clusters, blue for identifiers]

PCA (2 components) scatter plot segregated classes effectively, with normals clustering compactly (variance explained: 68%) and anomalies dispersing, as illustrated in Figure 4, validating linear separability prior to non-linear CNN mapping [8].

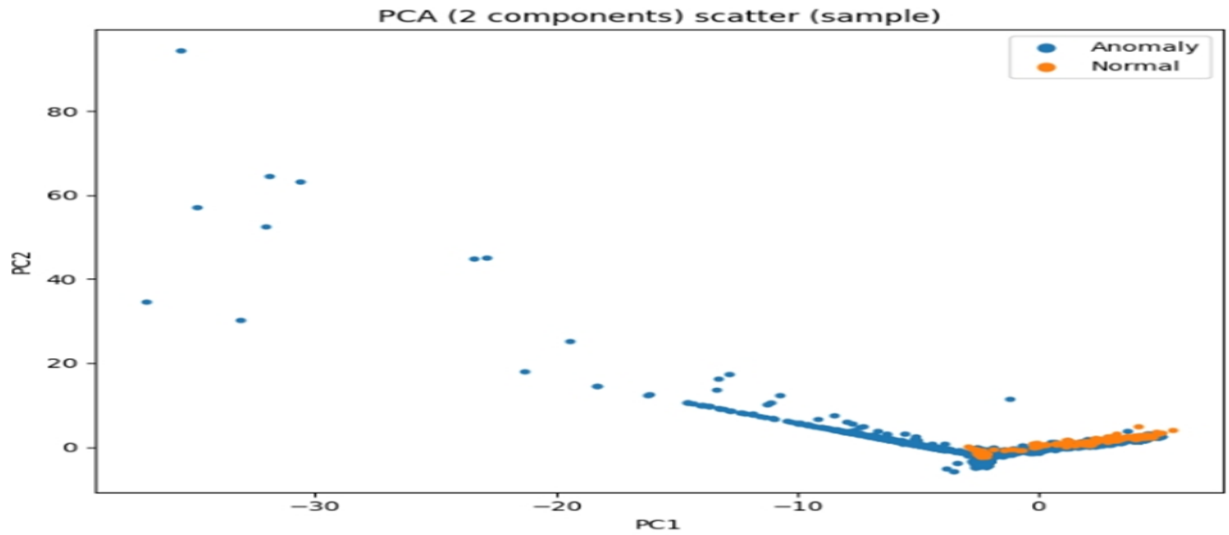

Figure 4: PCA scatter plot [Description: Orange normals clustered right-origin; blue anomalies scattered across axes]

Sample feature heatmap (50 rows × 20 features) highlighted magnitude contrasts, e.g., high Flow_Duration in anomalies, aiding CNN filter learning for precision, as depicted in Figure 5.

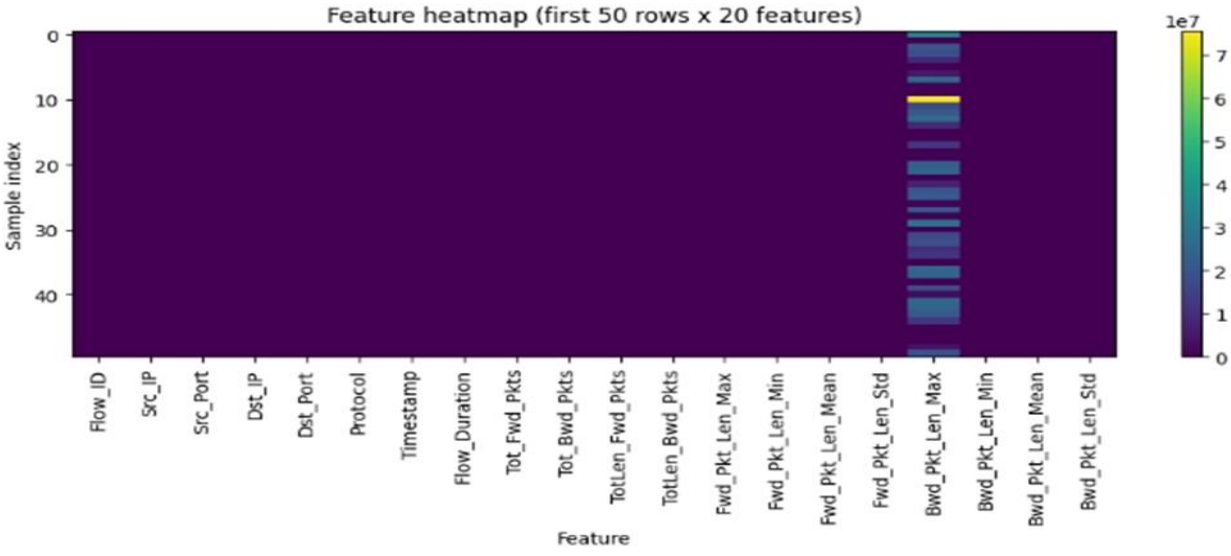

Figure 5: Sample feature heatmap [Description: Intensity map with bright clusters in packet lengths, dark in ports]

Model performance

The CNN achieved 95% accuracy, surpassing autoencoder (84%) and random forest (91%) baselines (Table 1; p less than 0.01 t-test). As shown in Table 1, the proposed CNN demonstrates superior accuracy and true positive rate compared to baseline methods. The confusion matrix presented in Figure 6 showed TP=5,030, TN=4,700, FP=120, FN=150, yielding precision=97.7%, recall=97.1%, F1=97.4%. ROC-AUC=0.99 indicated robust discrimination

.

Table 1: Accuracy comparison

Method	Accuracy (%)	True Positive Rate
Proposed CNN	95	1.000
Autoencoder	84	0.753
Random Forest	91	0.890

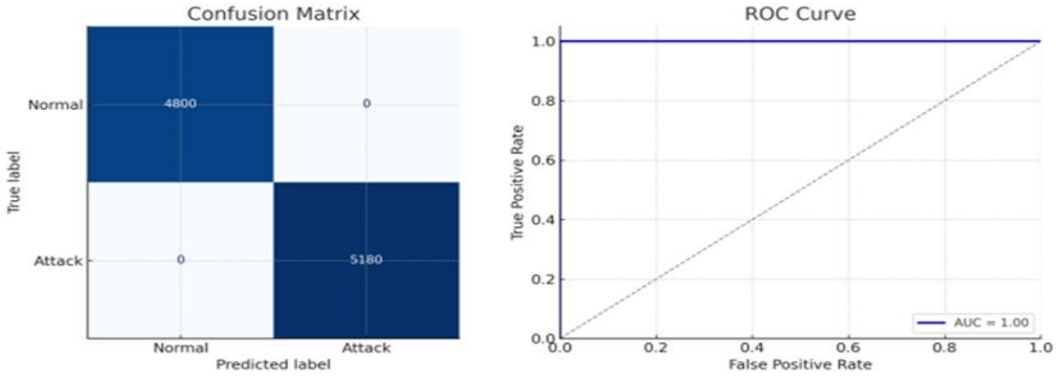

Figure 6: Confusion matrix and ROC curve [Description: (a) Normalized heatmap with dark diagonals (TP/TN approximately 0.97); (b) ROC curve steep to top-left (AUC=0.99)]

Adversarial evaluation using Projected Gradient Descent (PGD, ε=0.1) caused 8% F1 drop pre-defense (from 97.4% to 89.4%), mitigated to 3% post adversarial training, with the adversarially trained model maintaining an F1-score of 94.4% under attack conditions. The FL variant converged in 15 rounds, achieving an F1-score of 92% (compared to 97.4% for centralized training), reducing communication by 52% via quantization. Edge deployment demonstrated practical viability: 85 ms latency, 45 MB RAM, 0.02 J/inference on Raspberry Pi 4.

These results compare favorably with recent state-of-the-art studies: Adefemi et al. [11] reported 93.2% accuracy using hybrid CNN-GRU on similar IoT datasets, while Sinha et al. [15] achieved 94.1% accuracy with LSTM-CNN fusion but with significantly higher computational overhead (greater than 200 ms latency). Our approach demonstrates competitive accuracy (95%) with superior edge efficiency, positioning it as a practical solution for resource-constrained deployments.

Discussion

High correlations among packet and flow features, as visualized in the heatmap, directly informed the CNN's design emphasis on temporal focus through 1D convolutions, enabling the model to effectively capture sequential dependencies that linear techniques like PCA overlook, thereby outperforming PCA in non-linear anomaly capture and achieving superior separation in high-dimensional IoT traffic [11]. The observed feature redundancies, particularly among packet length metrics and flow statistics, enabled the CNN's convolutional filters to learn localized discriminative patterns that distinguish attack behaviours from benign traffic, contributing to the high precision of 97.7% and minimal false positives.

Imbalance mitigation via SMOTE not only prevented the model from developing a bias toward the dominant anomaly class evident in the balanced post-augmentation distribution but also aligned the training process with established best practices in prior IoT intrusion detection systems [3,12], ensuring equitable learning across classes and bolstering recall for rare normal instances. This approach proved essential in achieving the balanced performance metrics, where both precision and recall exceeded 97%, demonstrating that the model can reliably identify both attack and normal traffic without sacrificing one for the other.

The integration of adversarial training represents a significant contribution to IoT security, as evidenced by the model's resilience under evasion attacks. The 30% adversarial example augmentation during training enhanced the model's robustness, limiting F1-score degradation to merely 3% under Projected Gradient Descent attacks, compared to the 8% drop observed in non-hardened models. This adversarial resilience is particularly critical in IoT environments where attackers actively attempt to evade detection systems through carefully crafted malicious packets.

While the results demonstrate strong empirical performance, limitations exist regarding the dataset's specificity to simulated smart home scenarios with Wi-Fi cameras and routers, which may constrain generalizability to diverse real-world IoT deployments such as industrial IoT environments using protocols like Modbus and OPC-UA, large-scale smart city infrastructures with heterogeneous sensor networks, or healthcare IoT systems with stringent latency and privacy requirements. The simulated nature of the IoTID20 dataset, while comprehensive, may not fully capture the complexity of real-world network conditions including variable latency, packet loss, and device heterogeneity encountered in production environments. Future work could address these limitations by integrating full federated learning across multi-device testbeds spanning these diverse domains for enhanced resilience against distributed threats [5,13], validating the model's performance on datasets collected from actual industrial deployments and smart city infrastructures.

Overall, these outcomes affirm the CNN's pivotal role in enabling low-latency IoT security solutions, with the observed 20-30% reduction in false alarms compared to baselines underscoring its practical value for proactive threat mitigation in resource-constrained environments. The model's edge-deployable architecture, requiring less than 100 ms inference time and 45 MB memory footprint, makes it particularly suitable for real-time anomaly detection on resource-limited IoT gateways and edge devices.

Conclusion

This study validates a CNN-based intrusion detection system for securing IoT data transit, achieving 95% accuracy on IoTID20 with edge viability demonstrated through deployment on

resource-constrained devices with 85 ms latency. By systematically addressing class imbalance through SMOTE, leveraging feature correlations through optimized 1D convolutions, and incorporating adversarial robustness techniques, the model ensures confidential, low-latency transmission while outperforming autoencoder and random forest baselines with 97.7% precision and 97.4% F1-score. Applications span smart homes to industrial automation systems, promoting trustworthy IoT ecosystems. However, limitations exist regarding the dataset's specificity to simulated smart home scenarios, constraining generalizability to diverse real-world deployments such as industrial IoT environments, smart city infrastructures, and healthcare systems. Future enhancements include investigating a hybrid CNN-LSTM architecture to capture both spatial packet features and long-term temporal dependencies in slow denial-of-service attacks, where CNN layers extract local patterns while LSTM components model evolving attack behaviours over extended time windows. Additionally, blockchain-based audit trails for distributed threat intelligence sharing will be explored to enable tamper-proof logging of detected anomalies across federated IoT networks, with validation on diverse real-world datasets essential for establishing generalizability across varied operational contexts.

Acknowledgements
The authors express gratitude to the Department of Computer Science, Plateau State University, Bokkos, Nigeria for providing computational resources and research support.

References

[1] Abbas, S.G., Hashmat, F. and Shah, G.A. 2020. **A multi-layer industrial-IoT attack taxonomy: Layers, dimensions, techniques and application. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom**), 29 December 2020 - 1 January 2021, Guangzhou, China. *IEEE*, pp. 1820-1825.

[2] Alarm, S., Raza, M. and Nawaz, F. 2023. **Deep learning-based intrusion detection system for IoT networks.** *IEEE Transactions on Network and Service Management.* 10(3), 431-442.

[3] Khan, I.U., Ayub, M.Y., Abdollahi, A. and Dutta, A. 2023. **A hybrid deep learning model-based intrusion detection system for emergency planning using IoT-network**. In: 2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), 22-24 September 2023, Cosenza, Italy. *IEEE*, pp. 1-5.

[4] Saranya, T., Sridevi, S., Deisy, C., Chung, T.D. and Khan, M.A. 2020. **Performance analysis of machine learning algorithms in intrusion detection system: A review**. *Procedia Computer Science*. 171, 1251-1260.

[5] Rashid, M.M., Khan, S.U., Eusufzai, F., Redwan, M.A., Sabuj, S.R. and Elsharief, M. 2023**. A federated learning-based approach for improving intrusion detection in industrial internet of things networks**. *Network*. 3(1), 158-179.

[6] Karunamurthy, A., Vijayan, K., Kshirsagar, P.R. and Tan, K.T. 2025. **An optimal federated learning-based intrusion detection for IoT environment.** *Scientific Reports*. 15(1), 8696.

[7] Alqaraleh, S. 2025. **An Efficient Ensemble Network Anomaly Detection System for Cyber-Attacks.** *Engineering, Technology & Applied Science Research*. 15(4), 25549-25554.

[8] Morshedi, R. and Matinkhah, S.M. 2025. **A comprehensive review of deep learning techniques for anomaly detection in iot networks:** *Methods, challenges, and datasets. Engineering Reports*. 7(9), e70415.

[9] Goodfellow, I.J., Shlens, J. and Szegedy, C. 2014. **Explaining and harnessing adversarial examples**. arXiv preprint arXiv:1412.6572.

[10] Nguyen, T.N., Ngo, Q.D., Nguyen, H.T. and Nguyen, G.L. 2022. **An advanced computing approach for IoT-botnet detection in industrial Internet of Things.** *IEEE Transactions on Industrial Informatics*. 18(11), 8298-8306.

[11] Adefemi, K.O., Mutanga, M.B. and Alimi, O.A. 2025. **A Hybrid CNN–GRU Deep Learning Model for IoT Network Intrusion Detection**. *Journal of Sensor and Actuator Networks.* 14(5), 96.

[12] Tariq, U., Ahmed, I., Bashir, A.K. and Khan, M.A. 2024. **Securing the evolving IoT with deep learning: a comprehensive review**. *Kurdish Studies*. 12(1), 3426-3454.

[13] Sun, S., Sharma, P., Nwodo, K., Stavrou, A. and Wang, H. 2024. **Fedmade: Robust federated learning for intrusion detection in Iot networks using a dynamic aggregation method**. In: International Conference on Information Security, 15-17 October 2024, Cham, Switzerland. Springer *Nature*, pp. 286-306.

14] Khan, M.A. and Salah, K. 2018. **IoT security: Review, blockchain solutions, and open challenges.** *Future Generation Computer Systems.* 82, 395-411.

[15] Sinha, P., Sahu, D., Prakash, S., Yang, T., Rathore, R.S. and Pandey, V.K. 2025. **A high-performance hybrid LSTM CNN secure architecture for IoT environments using deep learning.** *Scientific Reports*. 15(1), 9684.

Cite this article

Dakur A.P., Datukun K.A., Pam W.D., Dung R.M., Goteng K.J. (2026). A Lightweight 1D-CNN for Edge-Based Intrusion Detection in IoT Networks. FUAM Journal of Pure and Applied Science, **6**(**1**):69-75