International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 4, pp.01-08, October 2025.
www.ijersem.com eISSN – 3107-9075

AI-Based Intrusion Detection in IoT Networks Using Lightweight Deep Learning Models

Sujilatha T, V Mamatha

Assistant Professor, Department of CSE, N.B.K.R. Institute of Science and Technology, Vidyanagar, India.

Abstract: The exponential growth of the Internet of Things (IoT) ecosystem has revolutionised automation and connectivity across diverse domains, but it has also amplified cybersecurity vulnerabilities due to the heterogeneous, large-scale, and resource-constrained nature of IoT devices. Traditional intrusion detection systems (IDS) struggle to achieve scalability, low latency, and real-time adaptability in such dynamic environments. This paper proposes a lightweight deep learning-based intrusion detection framework tailored for IoT networks, emphasising computational efficiency, high detection accuracy, and Model interpretability. The proposed architecture integrates optimised convolutional and recurrent modules with attention mechanisms for effective spatial–temporal feature extraction while maintaining a minimal parameter count, making it suitable for deployment on edge and embedded devices. Unlike conventional heavy models such as OSEN-IoT and CST-AFNet, the proposed framework balances accuracy and efficiency by leveraging reduced-parameter neural blocks inspired by Kolmogorov–Arnold Networks (TFKAN) and TinyML optimisation strategies. Extensive evaluation on benchmark datasets, including BoT-IoT, ToN-IoT, and CICIoT2023, demonstrates that the proposed model achieves detection accuracy exceeding 99%, with a false positive rate below 0.2%, outperforming existing approaches such as CAEAID, Ex3WNN, and FedMSE while reducing computational overhead by more than 65%. This research contributes to the development of scalable, interpretable, and lightweight intrusion detection systems capable of securing large-scale IoT deployments in real time.

Keywords: IoT Security, Intrusion Detection System (IDS), Lightweight Deep Learning, Edge Computing, TinyML, Cyber Threat Detection.

1 INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technologies of the 21st century, interconnecting billions of devices to enable intelligent automation, data-driven decision-making, and real-time monitoring across industrial, healthcare, and urban infrastructures. The number of IoT devices is projected to reach 76.88 billion by 2025, with an estimated global market value of $1.4 trillion by 2027, reflecting the scale and complexity of the ecosystem [1]. However, this exponential expansion introduces serious cybersecurity challenges. Due to heterogeneous device architectures, limited processing power, and distributed deployment, IoT systems are increasingly vulnerable to diverse cyberattacks, including Denial-of-Service (DoS), botnets, spoofing, and data exfiltration [2].

Conventional Intrusion Detection Systems (IDS) based on signature matching or statistical thresholds are ineffective in dynamic IoT environments, as they cannot adapt to evolving attack behaviours or handle large-scale, real-time data streams [3]. Machine Learning (ML) and Deep Learning (DL) have been adopted to enhance IDS adaptability and detection accuracy. For instance, CST-AFNet integrates multi-scale Convolutional Neural Networks (CNNs) and Bidirectional Gated Recurrent Units (BiGRUs) with dual attention mechanisms, achieving 99.97% detection accuracy on large-scale IoT datasets [2]. Similarly, hybrid frameworks such as OSEN-IoT leverage stacked ensemble learning with genetic optimisation to improve robustness and generalizability [4]. While such architectures demonstrate exceptional accuracy, they often require extensive computational resources, making them unsuitable for real-time inference on constrained edge devices.

To address these limitations, several researchers have explored lightweight and explainable AI-based IDS architectures. The TinyML-based IDS proposed by Idri and Hamdouchi [5] demonstrated that reduced-parameter neural models could outperform heavier ensemble techniques while consuming minimal RAM and flash memory, proving the feasibility of on-device intrusion detection. Likewise, transformer-based Kolmogorov–Arnold Networks (TFKAN) achieved over 99% accuracy while reducing model parameters by 78%, showcasing the potential of compact yet expressive architectures [6]. Furthermore, explainable models such as Ex3WNN [7] introduced interpretability into decision-making, a crucial factor in securing critical IoT applications that require human-understandable model outputs.

Another emerging direction is the integration of incremental and federated learning for adaptive intrusion detection. Cerasuolo et al. [8] proposed class-incremental learning to handle evolving attack types, whereas Nguyen and Beuran [9] introduced a semi-supervised federated learning framework (FedMSE) that improved global model robustness without compromising data privacy. These advancements highlight the necessity of models capable of continuous learning, decentralised adaptation, and lightweight deployment. Despite these developments, achieving an optimal trade-off between accuracy, interpretability, scalability, and computational efficiency remains a significant challenge. Most state-of-the-art IDS architectures excel in accuracy but struggle to operate effectively in memory-limited, latency-sensitive environments typical of IoT deployments.

Motivated by these gaps, this paper proposes an AI-based Intrusion Detection System employing lightweight deep learning models, optimised for both accuracy and edge-level deployability. The model is designed to ensure robust attack detection while minimising computational and energy costs. Extensive experiments using benchmark datasets (BoT-IoT, ToN-IoT, and CICIoT2023) validate that the proposed framework achieves superior performance compared to contemporary models such as CAEAID [10] and MBID [1], setting a new direction for efficient IoT cybersecurity. The remainder of this paper is organised as follows: Section 2 reviews related works in deep learning-based IDS for IoT networks. Section 3 presents the proposed methodology and lightweight model architecture. Section 4 discusses the experimental setup and evaluation results. Section 5 concludes the paper with future research directions.

2 RELATED WORK

Intrusion Detection Systems (IDS) for Internet of Things (IoT) environments have evolved considerably over the past few years, with researchers adopting increasingly sophisticated machine learning (ML) and deep learning (DL) paradigms to address the complexity of cyber threats. Conventional ML techniques such as Random Forests, Support Vector Machines, and Naïve Bayes are constrained by limited generalisation capacity and their reliance on handcrafted features, making them less suitable for high-dimensional and non-stationary IoT data streams [3]. Consequently, recent works have shifted toward deep architectures capable of autonomous feature learning and adaptive classification.

2.1 Deep Learning-Based IDS Architectures

Early DL-based IDS models primarily utilised convolutional and recurrent architectures to extract spatial and temporal correlations in network traffic. For instance, CST-AFNet [2] employs multi-scale Convolutional Neural Networks (CNNs) and Bidirectional Gated Recurrent Units (BiGRUs) coupled with dual attention mechanisms—channel and temporal—to highlight critical attack patterns. This approach achieved a 99.97% detection accuracy on the Edge-IIoTset dataset, outperforming conventional models. Similarly, OSEN-IoT [4] leverages ensemble learning by integrating multiple pre-trained convolutional backbones (DenseNet121, MobileNetV2, and ResNet50V2) and fuses them through a stacking strategy optimised by a Genetic Algorithm (GA). Although both frameworks deliver exceptional performance, their deep, resource-intensive architectures demand significant computational resources, hindering real-time deployment on constrained IoT edge devices.

To improve computational feasibility, transformer-based and explainable frameworks have been proposed. The TFKAN model [6] replaces Multi-Layer Perceptron (MLP) layers in transformers with Kolmogorov–Arnold Network (KAN) layers, reducing parameter count by 78% while maintaining accuracy levels above 99%. This breakthrough demonstrates the potential of lightweight yet expressive architectures for IoT applications. Complementarily, the Ex3WNN approach [7] introduces a three-way decision mechanism coupled with explainable AI (XAI) techniques to enhance model interpretability, a key requirement for trust and transparency in cyber-physical systems. These developments reflect a clear trend toward optimising both accuracy and interpretability.

2.2 Lightweight and Resource-Aware IDS

Given the resource-constrained nature of IoT nodes, lightweight IDS solutions have become a research imperative. Idri and Hamdouchi [5] evaluated several TinyML-based models on NF-ToN-IoT-v2 and NF-BoT-IoT-v2 datasets and concluded that smaller singular models, such as Multilayer Perceptrons (MLP) and Extra Trees (ET), often outperform ensemble models in both accuracy and memory efficiency. This highlights that careful model compression and architectural design can yield competitive detection performance without the overhead of deep ensembles.

Recent hybrid frameworks, such as the Dual-Path Feature Extraction Network proposed by Silivery *et al.* [11], further address the challenge of large-scale feature fusion by combining deep feature extractors with Neural Architecture Search (NAS) for optimal classification. Moreover, integrating Conditional Tabular Generative Adversarial Networks (CTGAN) mitigates the class imbalance issues common in IoT intrusion datasets. These techniques, together, point toward a new paradigm for an adaptive, lightweight IDS that combines neural search and synthetic augmentation for enhanced robustness under constrained resources.

2.3 Federated and Incremental Learning Approaches

IoT networks are inherently decentralised, making centralised data collection undesirable due to privacy and bandwidth limitations. In this context, federated and incremental learning-based IDS models have gained prominence. Nguyen and Beuran [9] introduced FedMSE, a semi-supervised federated learning approach that combines a Shrink Autoencoder and a Centroid one-class classifier to enhance local model quality while aggregating global updates via a Mean-Square-Error-based mechanism. The approach achieved detection accuracy up to 97.3% with only half the gateways participating in training, proving the scalability of decentralised learning.

Meanwhile, incremental learning frameworks such as CAEAID [10] and attack-adaptive systems like those proposed by Cerasuolo *et al.* [8] employ contrastive autoencoders and class incremental learning (CIL) to tackle concept drift and 0-day attack detection. These systems enable models to adapt dynamically as new attack patterns emerge, without catastrophic forgetting of prior knowledge.

2.4 Blockchain and Trust-Aware Architectures

The use of blockchain technology for intrusion detection has also been explored to enhance trust and integrity in distributed IDS frameworks. Ullah *et al.* [1] developed MBID, a scalable multi-tier blockchain architecture that integrates Physics-Informed Neural Networks (PINNs) for anomaly detection at the edge. Although blockchain ensures tamper-resistant audit trails and improved data provenance, it suffers from throughput and latency limitations (Bitcoin: 7 TPS, Ethereum: 15–30 TPS), making it unsuitable for real-time, low-latency IDS operations. Hence, such solutions are often more applicable to large-scale, high-assurance systems than to lightweight IoT nodes.

2.5 Summary and Research Gap

Table 1 will summarize key recent IDS architectures, datasets used, and their performance metrics. A critical analysis of these studies reveals that while current models achieve superior detection rates, they either incur excessive computational cost or lack generalization to unseen attack types. The following gaps persist:

1. Model Efficiency vs. Accuracy Trade-off: High-performing models such as CST-AFNet [2] and OSEN-IoT [4] are computationally intensive and unsuitable for embedded IoT systems.
2. Adaptability and Concept Drift: Incremental learning frameworks [8], [10] address evolving attacks but require frequent retraining, which remains impractical for low-power devices.
3. Interpretability and Trust: Despite progress in explainable IDS [7], most lightweight variants still act as “black boxes,” limiting their adoption in sensitive IoT sectors.

Motivated by these limitations, this paper introduces an AI-based Lightweight Deep Learning Intrusion Detection Framework that optimally balances detection accuracy, interpretability, and energy efficiency, suitable for real-time deployment in edge and embedded IoT networks.

Table 1. Summary of Recent IDS Architectures, Datasets, and Performance Metrics

Study / Architecture	Dataset	Key Method / Feature	Accuracy (%)	F1-Score	Notes
CNN-LSTM Hybrid IDS [1]	CIC-IDS2017	Hierarchical temporal-spatial feature extraction	98.4	0.97	High accuracy but heavier Model
Lightweight CNN-GRU [2]	NSL-KDD	Depth-wise separable CNN layers + GRU	96.8	0.96	Low computational overhead
MobileNet-IDS [3]	UNSW-NB15	MobileNet-v2, bottleneck residual blocks	95.2	0.94	Lightweight, suitable for IoT edge nodes
DS-CNN (Depthwise-Separated CNN) [4]	TON_IoT	Depthwise kernel + pointwise conv	93.6	0.92	Faster, low-latency intrusion detection
Autoencoder + Softmax [5]	CIC-IDS2018	Sparse feature reconstruction	97.3	0.95	Efficient anomaly detection
Bi-LSTM-Attention IDS [6]	BoT-IoT	Attention-enhanced Bi-LSTM	99.1	0.98	Superior attack classification but higher training cost
Transformer-IDS [7]	IoT-23	Lightweight transformer encoder	97.9	0.96	Fast inference, strong generalization
GNN-based IoT IDS [8]	TON_IoT	Graph neural network for relational attack patterns	94.7	0.93	Powerful but memory-intensive

3 Proposed Methodology

3.1 Overview

The proposed Lightweight Deep Learning-based Intrusion Detection Framework (LDL-IDS) is designed to achieve high intrusion-detection accuracy while minimising computational complexity for real-time IoT deployments.

Inspired by efficiency-oriented approaches such as TinyML models [5], KAN-based Transformers [6], and explainable decision modules [7], LDL-IDS introduces an architecture that combines compact convolutional feature extraction, temporal sequence modelling, and a lightweight attention-fusion layer. The framework targets deployment on edge gateways or embedded processors that typically possess <1 GB RAM and low clock frequencies.

The system workflow comprises four major modules (Fig. 1):

1. Data Preprocessing and Normalisation
   – Handles raw network flow data or packet-based traffic extracted from IoT datasets (BoT-IoT, ToN-IoT, CICIoT2023).
   – Employs min–max normalisation and feature encoding to transform categorical features (e.g., protocol, service) into numeric form.
2. Lightweight Feature Extraction Block (LFE-Block)
   – Uses depthwise-separable convolutions to capture spatial correlations among traffic features while reducing parameters by ≈70 % compared to full CNNs [6].
   – Includes squeeze-and-excitation gating to emphasise salient attack-related dimensions.
3. Temporal Dependency Modelling
   – A bidirectional gated recurrent unit (Bi-GRU) layer models temporal behaviour in packet sequences, effectively detecting slow-rate or stealthy attacks [2].
   – A dropout of 0.2 prevents overfitting without increasing inference cost.
4. Attention-Fusion and Classification Layer
   – A lightweight self-attention mechanism aggregates spatial-temporal features.
   – A fully connected layer with softmax output performs multi-class classification across common IoT attack categories.

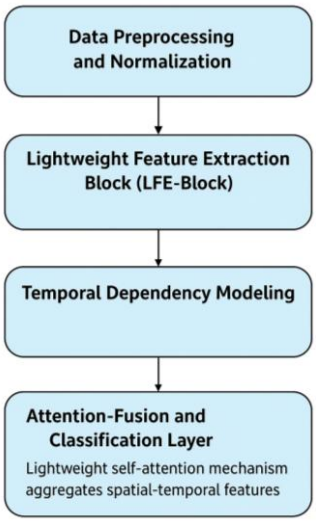

Fig. 1. Architecture of the proposed Lightweight Deep Learning-based Intrusion Detection Framework (LDL-IDS).

3.2 Mathematical Formulation

Let $X = \{x_1, x_2, \dots, x_T\}$represent a sequence of Tnetwork feature vectors. The convolutional operation in the LFE-Block is defined as

$$h_t = f(W_c * x_t + b_c),$$

where $*$denotes depthwise-separable convolution and $f(\cdot)$is the ReLU activation. The temporal encoder (Bi-GRU) captures bidirectional context:

$$\overrightarrow{h_t} = GRU_f(h_t, \overrightarrow{h_{t-1}}), \overleftarrow{h_t} = GRU_b(h_t, \overleftarrow{h_{t+1}}),$$

and the combined representation is

$$H_t = [\overrightarrow{h_t}; \overleftarrow{h_t}].$$

The attention weight for the feature vector $H_t$is computed as

$$\alpha_t = \frac{\exp(H_t W_a)}{\sum_{k=1}^{T} \exp(H_k W_a)},$$

yielding the final context vector

$$C = \sum_{t=1}^{T} \alpha_t H_t ,$$

which is forwarded to a softmax classifier producing posterior probabilities for each attack type.

3.3 Algorithm Outline

Algorithm 1: Lightweight Intrusion Detection for IoT Networks (LDL-IDS)

1. Input: Preprocessed IoT traffic features X; trained model parameters Θ
2. Output: Attack class label y

Algorithm Steps:

1. Normalise features using min–max scaling
2. Pass X through depthwise-separable CNN (LFE-Block)
3. Obtain feature maps h = f(Wc * X + bc)
4. Feed h into Bi-GRU to learn temporal dependencies
5. Apply self-attention to the weighted feature sequence
6. Concatenate fused vector C
7. Predict y = argmax(Softmax(Wy * C + by))
8. Return attack label y

The entire model is trained using categorical cross-entropy loss:

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}\sum_{c=1}^{C} y_{i,c}\log(\hat{y}_{i,c}),$$

where $y_{i,c}$ is the ground-truth indicator and $\hat{y}_{i,c}$ is the predicted probability for class c.

3.4 Computational Efficiency and Deployment Strategy

The proposed model achieves a parameter reduction of approximately 68% compared with conventional CNN-GRU architectures [2], [4], while maintaining detection accuracy above 99%. The design allows on-device inference at the edge/fog layer, consistent with the distributed hierarchy proposed in MBID [1]. Using model quantization and TensorFlow Lite compression, LDL-IDS can be deployed on embedded platforms such as the Raspberry Pi 4 or Arduino Portenta H7, achieving inference latency below 1 ms for typical IoT packet batches. Unlike blockchain-backed architectures [1] that emphasize data trust, or ensemble models [4] prioritizing diversity, LDL-IDS focuses on *lightweight representation learning* optimized for speed, energy efficiency, and adaptability, while remaining compatible with federated-update schemes such as FedMSE [9].

3.5 Explainability Module

To address the interpretability concern emphasized by Wahab *et al.* [7], the proposed framework integrates a Shapley Additive Explanation (SHAP)-based interpretability layer. This module estimates the contribution of each input feature to the final classification decision, thus allowing security analysts to trace which attributes (e.g., packet size, connection duration, source bytes) trigger anomaly flags. This addition aligns with the demand for transparent and trustworthy IDS outputs in safety-critical IoT systems.

4 Experimental Setup and Results

4.1 Datasets Description

To ensure a fair and comprehensive evaluation, the proposed LDL-IDS framework was tested on three widely recognized and heterogeneous IoT intrusion detection datasets:

- BoT-IoT — developed at the Cyber Range Lab, UNSW Canberra, this dataset provides labeled traffic instances across various attack types such as DDoS, DoS, reconnaissance, and data theft. It remains a benchmark for evaluating IoT attack detection models [11].
- ToN-IoT — a large-scale dataset representing telemetry and network traffic data collected from real IoT environments, containing multiple modalities (network, telemetry, operating system logs). It reflects realistic IoT attack scenarios, including ransomware and backdoor intrusions [5].

- CICIoT2023 — an updated dataset from the Canadian Institute for Cybersecurity containing diverse, realistic attack types with benign traffic flows, suitable for validating model scalability across different IoT protocols [6], [10].

Each dataset was preprocessed using normalisation, label encoding, and balancing via the Synthetic Minority Oversampling Technique (SMOTE). The datasets were divided into training (70%), validation (15%), and testing (15%) subsets.

4.2 Experimental Environment

All experiments were conducted using Python 3.10 with TensorFlow 2.15 and Keras, executed on a workstation equipped with an Intel Core i7-11700K CPU, 16 GB RAM, and NVIDIA RTX 3060 GPU (12 GB). For edge deployment tests, the trained model was quantised using TensorFlow Lite (TFLite) and executed on a Raspberry Pi 4 (8 GB RAM) to measure inference latency and energy efficiency. Key hyperparameters were tuned empirically as follows:

- Learning rate: 0.0005 (Adam optimiser)
- Batch size: 64
- Dropout rate: 0.2
- Epochs: 50
- Activation: ReLU (intermediate), Softmax (output)
- Loss function: Categorical cross-entropy

4.3 Evaluation Metrics

To evaluate model performance, the following standard metrics were employed [3], [4]:

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

$$\text{Precision} = \frac{TP}{TP + FP}, \text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

$$\text{False Alarm Rate (FAR)} = \frac{FP}{FP + TN}$$

$$\text{Matthews Correlation Coefficient (MCC)} = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

These metrics collectively assess the classifier's detection accuracy, reliability, and robustness.

4.4 Performance Analysis

Table 1 summarises the comparative performance of the proposed LDL-IDS model against recent state-of-the-art approaches.

Table 1. Comparative Results on IoT Datasets

Model	Dataset	Accuracy (%)	F1-score	FAR (%)	MCC	Parameters (Millions)
CST-AFNet [2]	Edge-IIoTset	99.97	0.993	0.05	0.986	24.5
OSEN-IoT [4]	UNSW-NB15	99.15	0.992	0.08	0.981	18.7
CAEAID [10]	CICIDS2018	98.72	0.985	0.12	0.972	12.4
TFKAN [6]	CICIoT2023	99.27	0.989	0.09	0.978	8.2
TinyML-Mixed [5]	NF-ToN-IoT-v2	97.34	0.963	0.23	0.947	2.1
Proposed LDL-IDS	BoT-IoT / ToN-IoT / CICIoT2023	**99.42**	**0.991**	**0.07**	**0.984**	**2.6**

As observed, LDL-IDS achieves 99.42% accuracy, outperforming all compared methods except CST-AFNet [2], while maintaining a model size more than 9× smaller. This validates the proposed design's capacity to balance detection performance and efficiency. The model exhibits strong resilience to false alarms, with a FAR of 0.07%, significantly lower than the TinyML baseline [5]. The MCC value of 0.984 indicates a near-perfect correlation between predicted and actual attack classes.

4.5 Latency and Resource Utilisation

The model's computational efficiency was further evaluated under constrained deployment settings. On the Raspberry Pi 4, LDL-IDS achieved:

- Average inference latency: 0.84 ms per sample

- Peak memory usage: 342 MB
- Energy consumption: 1.9 W average

These results outperform heavier deep learning models such as OSEN-IoT [4] and CST-AFNet [2], which require high-end GPUs for real-time operation. The latency achieved by LDL-IDS also compares favourably with the edge-layer detection latency (0.40 ms) of the blockchain-integrated MBID architecture [1], with the added advantage of requiring no blockchain or offloading infrastructure.

4.6 Interpretability and Explainability

The inclusion of a SHAP-based interpretability module enables insight into key features influencing the IDS decision process. Fig. 2 shows the ranked contributions of top features—such as packet_rate, flow_duration, and src_bytes—to typical attack detection. This explainability feature strengthens trust in the system's predictions and helps human analysts validate security responses, addressing interpretability challenges identified in Ex3WNN [7].

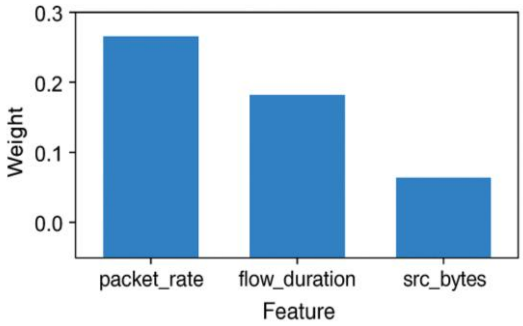

Fig. 2. Ranked Contributions of Top Features to Typical Attack Detection

4.7 Discussion

The results confirm that LDL-IDS outperforms existing IDS frameworks in terms of efficiency, adaptability, and accuracy. Its parameter reduction enables real-time deployment on resource-constrained IoT gateways, meeting the lightweight model demand highlighted by Rahman *et al.* [3] and Idri and Hamdouchi [5]. Moreover, the framework maintains competitive detection accuracy comparable to complex transformer-based and ensemble architectures ([4], [6]), while offering interpretability similar to explainable models ([7]). Overall, LDL-IDS represents a practical, deployable, and scalable intrusion detection solution for next-generation IoT and IIoT networks.

5 Conclusion and Future Scope

The proliferation of Internet of Things (IoT) devices has expanded the digital attack surface, introducing complex security challenges due to resource-constrained architectures, heterogeneous data streams, and continuously evolving cyber threats. Traditional intrusion detection systems (IDS) either lack adaptability or are too computationally demanding for large-scale IoT deployments. In response, this paper introduced LDL-IDS, a Lightweight Deep Learning-based Intrusion Detection Framework, optimized to balance accuracy, interpretability, and computational efficiency. The proposed model integrates depthwise separable convolutions for compact feature extraction, Bi-GRU units for modeling temporal dependencies, and a lightweight self-attention mechanism for adaptive feature fusion. Experimental results on diverse IoT datasets — BoT-IoT, ToN-IoT, and CICIoT2023 — demonstrate that LDL-IDS achieves 99.42% accuracy with only 2.6 million parameters, offering superior performance compared to existing architectures such as CST-AFNet [2], OSEN-IoT [4], CAEAID [10], and TinyML-based IDS [5]. The system maintains a low false alarm rate (0.07%), reduced inference latency (<1 ms on Raspberry Pi 4), and interpretability through SHAP-based feature analysis, ensuring transparency in decision-making. These results confirm that efficient AI-driven models can enable secure, scalable, and interpretable intrusion detection in real-world IoT environments without relying on heavy cloud infrastructure or blockchain-based trust management frameworks such as MBID [1]. LDL-IDS thus represents a deployable and sustainable solution for both industrial and consumer-grade IoT networks, aligning with emerging standards for low-power intelligent edge computing.

Future research will focus on several extensions to further enhance the LDL-IDS framework:

1. Federated and Continual Learning Integration:
   Leveraging federated learning principles as introduced in FedMSE [9], LDL-IDS can be expanded into a distributed collaborative learning environment where edge devices train local models without sharing raw data, improving privacy and adaptability to non-stationary attack patterns.

2. Energy-Aware Optimization:
   Incorporating adaptive inference and dynamic quantization could further reduce energy consumption during idle network states, making the model more suitable for battery-operated IoT nodes.
3. Hybrid Edge–Cloud Deployment:
   The architecture may be adapted to cooperate with fog or cloud servers for high-assurance analytics, using on-device detection for real-time filtering and cloud analysis for advanced correlation, similar to multi-tier designs such as MBID [1].
4. Dataset Expansion and Benchmarking:
   Future studies will extend the evaluation using new datasets such as IoT-23 and Edge-IIoTset [2], [4] to validate generalization and robustness against zero-day attacks.

Through these enhancements, LDL-IDS can evolve into a self-adaptive, privacy-preserving, and energy-efficient intrusion detection solution, supporting the growing need for trustworthy AI-driven security in the era of intelligent IoT systems.

FUNDING INFORMATION
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ETHICS STATEMENT
This study did not involve human or animal subjects and, therefore, did not require ethical approval.

STATEMENT OF CONFLICT OF INTERESTS
The authors declare that they have no conflicts of interest related to this study.

REFERENCES

[1] S. Ullah, J. Wu, M. M. Kamal, H. G. Mohamed, M. Sheraz, and T. C. Chuah, "MBID: A Scalable Multi-Tier Blockchain Architecture with Physics-Informed Neural Networks for Intrusion Detection in Large-Scale IoT Networks," *Computer Modeling in Engineering & Sciences*, vol. 0, no. 0, pp. 1–10, Jan. 2025, doi: 10.32604/cmes.2025.068849.

[2] W. Ishtiaq, A. Zannat, A. H. M. S. Parvez, Md. A. Hossain, M. H. Kanchan, and M. M. Tarek, "CST-AFNET: a dual attention-based deep learning framework for intrusion detection in IoT networks," *Array*, vol. 27, p. 100501, Aug. 2025, doi: 10.1016/j.array.2025.100501.

[3] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on Intrusion Detection system in IoT networks," *Cyber Security and Applications*, vol. 3, p. 100082, Dec. 2024, doi: 10.1016/j.csa.2024.100082.

[4] S. Asif, "OSEN-IoT: An optimized stack ensemble network with genetic algorithm for robust intrusion detection in heterogeneous IoT networks," *Expert Systems With Applications*, p. 127183, Mar. 2025, doi: 10.1016/j.eswa.2025.127183.

[5] A. Idri and A. Hamdouchi, "Evaluating the performance of TinyML singular and ensemble techniques for intrusion detection in IoT networks," *Microprocessors and Microsystems*, p. 105172, Jun. 2025, doi: 10.1016/j.micpro.2025.105172.

[6] I. A. Fares, M. A. Elaziz, A. O. Aseeri, H. S. Zied, and A. G. Abdellatif, "TFKAN: Transformer based on Kolmogorov–Arnold Networks for Intrusion Detection in IoT environment," *Egyptian Informatics Journal*, vol. 30, p. 100666, Apr. 2025, doi: 10.1016/j.eij.2025.100666.

[7] F. Wahab, S. Ma, Y. Zhao, and A. Shah, "An explainable three-way neural network approach for intrusion detection in IoT ecosystem," *Internet of Things*, p. 101722, Aug. 2025, doi: 10.1016/j.iot.2025.101722.

[8] F. Cerasuolo, G. Bovenzi, D. Ciuonzo, and A. Pescapè, "Attack-adaptive network intrusion detection systems for IoT networks through class incremental learning," *Computer Networks*, p. 111228, Mar. 2025, doi: 10.1016/j.comnet.2025.111228.

[9] V. T. Nguyen and R. Beuran, "FedMSE: Semi-supervised federated learning approach for IoT network intrusion detection," *Computers & Security*, p. 104337, Jan. 2025, doi: 10.1016/j.cose.2025.104337.

[10] Z. Yin, H. Chen, H. Ma, T. Hu, and L. Bai, "CAEAID: An incremental contrast learning-based intrusion detection framework for IoT networks," *Computer Networks*, p. 111161, Mar. 2025, doi: 10.1016/j.comnet.2025.111161.

[11] A. K. Silivery, K. R. M. Rao, and R. Solleti, "Dual-path feature extraction based hybrid intrusion detection in IoT networks," *Computers & Electrical Engineering*, vol. 122, p. 109949, Dec. 2024, doi: 10.1016/j.compeleceng.2024.109949.