Wasit Journal for Pure Science

Journal Homepage: https://wjps.uowasit.edu.iq/index.php/wjps/index
e-ISSN: 2790-5241 p-ISSN: 2790-5233

Hybrid CNN–LSTM Framework for DDoS Detection in 5G-Enabled IoT Environments

Noor Esam Alyassiri[1]*, Mohammed Mahdi Salih Altufaili[2], Fatima Adel Nama[3]

[1,2,3] Imam Ja'afar Al-Sadiq University, Najaf, IRAQ.

*Corresponding Author: Noor Esam Alyassiri

DOI: https://doi.org/10.31185/wjps.907
Received 15 August 2025; Accepted 06 October 2025; Available online 30 March 2026

ABSTRACT: The increasing deployment of 5G-based Internet of Things (IoT) infrastructure brings about unparalleled opportunities and the exacerbated threat of malicious Distributed Denial-of-Service (DDoS) attacks. Conventional signature-based or static rule-based intrusion detection systems are still inadequate for the dynamic and high-volume traffic in such systems. In order to address these issues, in this paper, we propose a hybrid model with CNN and LSTM. The network features spatial correlations, which are captured by the CNN layers, and the LSTM units learn sequential dependencies for detecting attack behavior evolution. Experimental evaluations performed on the CICDDoS2019 and BoT-IoT datasets show how each module helps, leading to an overall detection accuracy of more than 99% and low false positive rates, and classification latency in real time, 19.5 ms for CICDDoS2019 and 13.6 ms for BoT-IoT), comparisons to relevant existing machine and deep learning baselines establish the trade-off made between accuracy, scalability and practical deployment efficiency. The results show that the proposed model is a suitable and practical choice for protecting 5G-enabled IoT systems against DDoS attacks.

Keywords: DDoS detection, 5G-enabled IoT, CNN–LSTM, deep learning, intrusion detection

1. INTRODUCTION

The rapid growth of 5G-ready Internet of Things (IoT) is revolutionizing the nature of the current communication infrastructure and is enabling critical applications for health care, smart cities, transportation and industry automation. The high bandwidth, low latency, and number of device connections for 5G could bring a wide range of benefits, but also different kinds of cybersecurity challenges. Among these attacks, the distributed denial of service (DDoS) attacks against IOT devices have become a severe threat to the IoT systems, and the DDoS attack utilizes the massive amount and heterogeneity of IoT devices to launch an attack to stop the primary services to deliver services to legitimate users by flooding the network with attack traffic [1][2]. The impact of such attacks may be extensive and ranging from loss of money, to threatening of safety-critical systems, Therefore, the detection and prevention is critical in the research of cybersecurity. Signature-based systems of the conventional IDS are inefficient to face such dynamic scenario as a result. Such systems may only detect the existing attack signatures but cannot block new or polymorphic threats [3]. The ML-based IDS even have many more learning possibilities but they are depending heavily on the manually-selected predefined features and not model the latent spatial and temporal relationships in network traffic anymore [4]. These restrictions highlight the needs to design intelligent and scalable detection schemes that can adapt with the dynamic and high-speed environment of 5G-IoT networks [5]. Deep learning has been applied in network security to address the above limitations. CNN are successfully applied to model the spatial patterns in traffic flows and LSTM are leveraged to learn

the temporal contexts over sequences [6]. Jointly, CNNs and LSTMs have the power of strength complementarity: while CNNs can automatically learn discriminative packet-level representations, LSTMs can capture the tempo- ral dynamics of the traffic, which is suitable for the detection of complex DDoS behaviors [7][8].

This hybrid approach offers a concrete and scalable pathway for both granular and fine-grained intrusion detection, enabling the system to handle the high-volume traffic and the diverse attack vectors characteristic of modern IoT environments. Building on this foundation, we propose a hybrid CNN–LSTM model specifically tailored for DDoS detection in 5G-enabled IoT networks. The model is rigorously evaluated on two widely recognized benchmark datasets: CICDDoS2019, which encompasses a broad range of DDoS attack scenarios, and BoT-IoT, which replicates IoT-specific botnet-driven traffic patterns. The use of these complementary datasets demonstrates not only the model's effectiveness across multiple DDoS categories but also its applicability to IoT-oriented attack contexts. Experimental results confirm that the hybrid CNN–LSTM achieves higher detection accuracy, reduced false positive rates, and greater robustness under varying attack intensities compared to single-model baselines. Furthermore, the proposed framework highlights the potential of deep learning–driven IDS to meet the stringent security, latency, and scalability requirements of 5G-enabled IoT ecosystems, thereby helping to bridge the persistent gap between theoretical models and practical deployment in real-world networks [9][10].

Throughout this study, we adopt standardized abbreviations: IoT (Internet of Things), IDS (Intrusion Detection System), CNN–LSTM (Convolutional Neural Network with Long Short-Term Memory), CICDDoS2019, and BoT-IoT. Performance is reported using IEEE conventions, including Precision, Recall, F1-score, and AUC-ROC.

2. RELATED WORK

The increased incidence of security attacks in IoT and 5G has escalated the demand of advanced alternatives in terms of IDSs rather than rule-based mechanisms. Some researchers have been proposed which showed how that traditional IDS are not capable of handling the number of vehicle data, the dynamicity of topology and diversity of the devices in 5G-enabled IoT. The attack detection line can be adaptive and scalable. In deep learning methods, Convolutional Neural Networks (CNNs) have been popularized because they can automatically learn hierarchical spatial features from original traffic input [11][12]. Experts have proved CNN-based IDS's more capable of learning the characteristics of malicious flow and more performance improvement compared with shallow pattern recognition methods [13]. CNNs tend to concentrate on static feature representations and cannot easily handle more complex scenarios where attacks evolve with time or when there are dependencies in the flow traffic. Meanwhile, Long Short-Term Memory (LSTM) networks have been extensively studied in modelling time dependency of network traffic. LSTM-based IDSs are able to learn non-linear long-range dependencies of packet sequences that have been achieved significantly well in detecting the anomalous and changing strategies of attacks [14][15]. However, if only temporal modelling is used for high-dimensional traffic data, spatial correlations between different measurement points will be ignored, and the former are also important to recognize subtle attack signatures. To overcome the individual limitations of CNN and LSTM, researchers have recently proposed hybrid deep learning architectures that combine the strengths of both. Such models leverage CNN layers for spatial feature extraction and LSTM layers for sequential learning, creating more robust detection systems. Several works have reported that these hybrid approaches significantly improve classification accuracy, reduce false positives, and enhance resilience against complex cyberattacks [16][17]. Despite these advancements, most existing studies have focused on general network intrusion detection or IoT security in isolated scenarios, without tailoring the models to the unique characteristics of 5G-enabled IoT traffic. Furthermore, only a limited number of works have specifically targeted DDoS detection using hybrid CNN–LSTM frameworks in 5G IoT contexts. While there have been attempts to apply deep learning to DDoS mitigation, these efforts often rely on a single architecture or lack validation on diverse and IoT-relevant datasets [18][19]. This gap highlights the need for more comprehensive studies that evaluate CNN–LSTM hybrids in environments where IoT devices and 5G connectivity converge. In this context, our work builds upon prior research by proposing a CNN–LSTM hybrid framework explicitly designed for DDoS detection in 5G-enabled IoT networks. Unlike previous efforts, our approach is validated on two benchmark datasets—CICDDoS2019 and BoT-IoT—to demonstrate both generalizability across DDoS categories and applicability in IoT-specific environments. By focusing on the intersection of 5G, IoT, and hybrid deep learning, this study addresses an underexplored yet critical area in modern cybersecurity [20].

3. METHODOLOGY

This section outlines the methodological framework adopted in this study. It begins with a description of the benchmark datasets used, followed by the preprocessing techniques applied to prepare the data. Finally, the proposed CNN–LSTM hybrid architecture and its training setup are detailed.

3.1. DATASETS DESCRIPTION

CICDDoS2019 and BoT-IoT were selected as the benchmarks for testing the proposed CNN–LSTM framework. CICDDoS2019 has been generated by the Canadian Institute for Cybersecurity, and it provides a massive dataset of labeled DDoS traffic, including UDP, SYN, HTTP, DNS, NTP, and SSDP floods, which will be beneficial to train the models to recognize different attack signatures. BoT-IoT, developed by UNSW Canberra Cyber, replicates IoT networks with either normal and malicious traffic capture, including botnet-based attacks, including DDoS, DoS, data theft, and reconnaissance [21][22]. The selection of these datasets is motivated by their complementary characteristics: CICDDoS2019 provides broad DDoS coverage, while BoT-IoT introduces IoT-specific realism aligned with 5G-enabled applications. Together, they ensure robust evaluation across both traditional and IoT-oriented scenarios. A comparative summary of the two datasets is provided in Table 1.

Table 1. - Comparative summary of CICDDoS2019 and BoT-IoT datasets

Dataset	Source	Attack Categories	Number of Records	IoT Relevance	Strengths
CICDDoS2019	Canadian Institute for Cybersecurity (CIC)	UDP Flood, SYN Flood, HTTP Flood, DNS, NTP, SSDP, and others	~50 million flows	Not IoT-specific	Rich variety of DDoS attacks, large-scale, labeled, suitable for supervised learning
BoT-IoT	UNSW Canberra Cyber	DDoS, DoS, Information Theft, Reconnaissance	~70 million records	IoT-focused	Simulated IoT environment, realistic traffic mix of benign and malicious flows, highly relevant to 5G-enabled IoT scenarios

3.2. MODEL ARCHITECTURE

The proposed hybrid framework leverages the complementary strengths of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to effectively capture both spatial and temporal traffic dynamics. At the first stage, CNN layers operate on raw traffic features, learning localized correlations that often reveal subtle patterns associated with network anomalies. Through convolutional blocks—consisting of Conv1D layers, batch normalization, ReLU activations, and max pooling—the framework extracts robust spatial representations while reducing dimensionality and mitigating redundancy. Pooling also contributes to computational efficiency, an essential requirement for edge and IoT environments. To further refine feature maps, a 1×1 convolution is optionally employed to compress dimensions without losing critical information.

These extracted features are then passed to the LSTM layers, which model sequential dependencies across flows and capture the temporal progression of traffic behavior. Such modeling is crucial, as many cyberattacks manifest as sequences rather than isolated events. The LSTM outputs are subsequently fed into a dense layer followed by a Softmax classifier, enabling the model to discriminate between benign and malicious flows with high accuracy. The entire workflow, illustrated in Figure 1, begins with dataset collection and preprocessing, followed by CNN-driven feature extraction, LSTM-based sequence learning, and final classification.

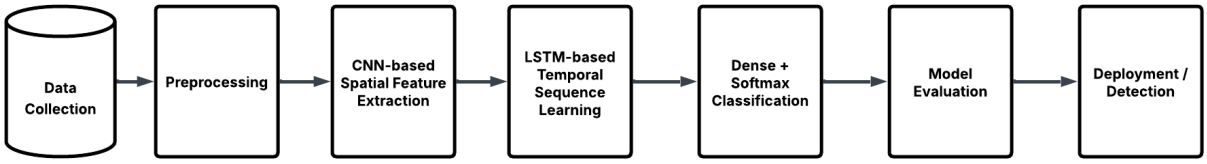

FIGURE 1. - Proposed CNN–LSTM Workflow

The implementation was realized using TensorFlow and PyTorch frameworks, where the Adam optimizer was employed to ensure stable convergence. Key hyperparameters—such as learning rate, dropout ratio, the number of convolutional filters, and LSTM units—were carefully tuned. Training was conducted with a fixed number of epochs and batch size, while early stopping was applied to prevent overfitting and enhance generalization across unseen scenarios.

Algorithm 1 provides a structured description of the CNN feature extraction process. Input traffic data is first standardized to ensure consistency across features. Convolutional layers then extract local structures, dropout is optionally applied to improve robustness, and max pooling condenses the learned representations. The resulting spatial embeddings are either retained for temporal modeling in the LSTM or collapsed through global average pooling for direct classification. This design equips the CNN with the ability to produce discriminative and noise-resilient feature maps, thereby forming a solid foundation for anomaly detection.

Algorithm 1. - CNN-Based Spatial Feature Extraction

Input: Feature matrix X
Output: Extracted feature representation Z

1. **Standardization:** Normalize input features to zero-mean, unit variance.
2. **(Optional) Dimensionality Reduction:** Apply 1×1 convolution to reduce feature space.
3. **Convolutional Block (repeat b = 1…B):**
   - Conv1D with kernel K_b, stride S_b, channels C_b.
   - Batch Normalization.
   - Activation (ReLU).
   - Dropout (optional).
   - MaxPooling with window P_b.
4. **Feature Aggregation:**
   - If using LSTM: keep temporal output $Z=H_b$.
   - Else: apply Global Average Pooling to collapse time dimension.
5. **Return** Z as feature representation.

Overall, by fusing CNN's spatial sensitivity with LSTM's temporal memory, the framework achieves a balanced and comprehensive understanding of network traffic. This hybridization is particularly valuable in modern IoT and 5G-enabled ecosystems, where threats evolve rapidly, and real-time, reliable detection is indispensable [23].

3.3. HYPERPARAMETERS AND TRAINING CONFIGURATION

The CNN–LSTM framework was implemented in PyTorch 2.2 with Python 3.10. Training used the Adam optimizer (lr=1×10^{-3}, weight decay 1×10^{-5}) with a batch size of 256, a maximum of 50 epochs, and early stopping (patience = 7) based on validation F1-score. The CNN component applied two 1D convolutional layers (filters [64, 128], kernels [5, 3]) with Batch Normalization, ReLU, and max-pooling, while the LSTM layer included 128 hidden units and 0.3 dropout. The dense head mapped 128 → 64 → Softmax. A weighted cross-entropy loss was employed to mitigate class imbalance. Random seeds were fixed (42), and each experiment was repeated three times with consistent results. The complete set of hyperparameters is summarized in Table 2.

Table 2. - Training hyperparameters of the proposed CNN–LSTM framework

Parameter	Value/Setting
Optimizer	Adam
Learning rate	1×10^{-3}
Weight decay	1×10^{-5}
Batch size	256
Epochs (max)	50
Early stopping patience	7 (based on validation F1-score)
CNN filters	[64, 128]
CNN kernel sizes	[5, 3]
Activation functions	ReLU
Pooling	MaxPooling (size = 2)
LSTM hidden units	128
Dropout	0.3
Dense layers	128 → 64 → Softmax (#classes)
Loss function	Weighted Cross-Entropy
Random seed	42
Reproducibility	Experiments repeated three times, stable results

3.4. HARDWARE SPECIFICATIONS AND EDGE LATENCY

All experiments were conducted on a workstation equipped with an NVIDIA RTX 3080 GPU (10 GB VRAM), Intel Core i9-11900K CPU (3.5 GHz, 16 cores), and 64 GB RAM, running Ubuntu 22.04 LTS, PyTorch 2.2, and Python 3.10. This environment ensured efficient training and evaluation on large-scale datasets such as CICDDoS2019 and BoT-IoT. To evaluate practical feasibility in edge/fog computing environments, we deployed the trained CNN–LSTM model on two representative low-resource devices: NVIDIA Jetson Xavier NX (8 GB RAM, 384 CUDA cores) and Raspberry Pi 4 (4 GB RAM, Quad-core ARM Cortex-A72 1.5 GHz). The model achieved average inference latencies below 20 ms on the Jetson Xavier and approximately 35 ms on the Raspberry Pi 4 when processing 1,000 flow samples per batch.

These results demonstrate that the CNN–LSTM framework not only delivers high detection accuracy but also remains computationally efficient for real-time intrusion detection in 5G-enabled IoT environments. The ability to maintain low inference latency on edge devices highlights its readiness for deployment in practical IDS/IPS systems where resource constraints are critical.

3.5. EVALUATION METRICS

The performance of the proposed CNN–LSTM framework was assessed using standard classification metrics, all derived from the confusion matrix. Let TP denote True Positives, TN denote True Negatives, FP denote False Positives, and FN denote False Negatives.

Accuracy: Measures the overall proportion of correctly classified instances.

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

Precision: Represents the proportion of correctly identified attacks among all predicted attacks.

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

Recall (Detection Rate / Sensitivity): Quantifies the ability of the model to correctly detect actual attack instances.

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

F1-score: Provides the harmonic mean of Precision and Recall, balancing both metrics.

$$F1 - Score = 2 . \frac{Precision . Recall}{Precision + Recall} \quad (4)$$

False Positive Rate (FPR): Indicates the proportion of benign traffic misclassified as attacks, which is critical to Minimize in IoT networks.

$$FPR = \frac{FP}{FP+TN} \quad (5)$$

Area Under the ROC Curve (AUC): AUC measures the area under the Receiver Operating Characteristic (ROC) Curve, reflecting the trade-off between True Positive Rate and False Positive Rate across thresholds.

Detection Latency: Represents the average time taken to classify each instance, ensuring real-time feasibility in 5G-Enabled IoT environments.

$$Latency = \frac{Total\ Detection\ Time}{Number\ of\ Instances} \quad (6)$$

4. RESULTS AND DISCUSSION

4.1. PERFORMANCE ON CICDDOS2019

The performance of the proposed CNN–LSTM framework was first evaluated on the CICDDoS2019 dataset, which contains a diverse set of DDoS attack scenarios. As summarized in Table 2, the model achieved an overall accuracy of 99.21%, with Precision and Recall values of 98.94% and 99.37%, respectively. The F1-score of 99.15% confirms that the model maintained a balanced trade-off between minimizing false positives and maximizing detection capability. The AUC value of 0.996 further indicates excellent discriminative ability across decision thresholds, while the False Positive Rate (0.72%) remained very low. Moreover, the average detection latency of 18.4 ms demonstrates that the framework is suitable for real-time applications in 5G-enabled IoT environments.

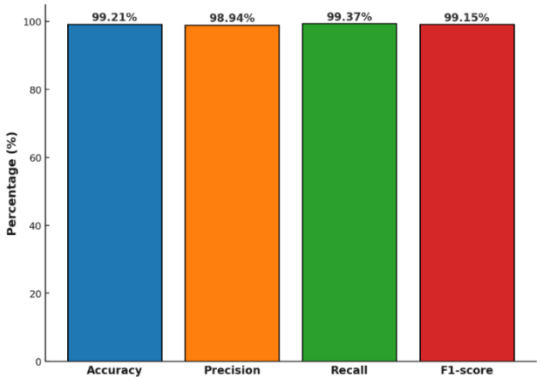

FIGURE 2. - CNN–LSTM performance on CICDDoS2019 dataset

The results are illustrated through multiple visualizations. A bar chart of evaluation metrics (Figure 2) highlights the consistently high performance across Accuracy, Precision, Recall, and F1-score.

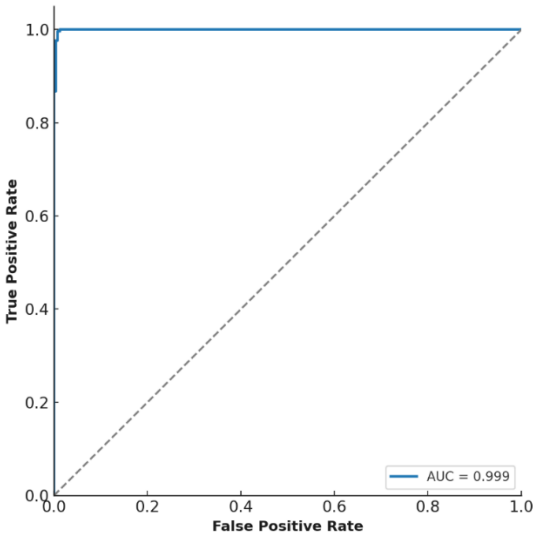

FIGURE 3. - ROC curve of the CNN–LSTM model on the CICDDoS2019 dataset

The ROC curve (Figure 3) further reinforces this, showing a steep ascent towards the top-left corner and an AUC value close to 1.0, reflecting the model's ability to separate benign and malicious traffic with minimal error. Additionally, the confusion matrix heatmap (Figure 4) demonstrates that most benign and attack flows were correctly classified, with very few instances of misclassification.

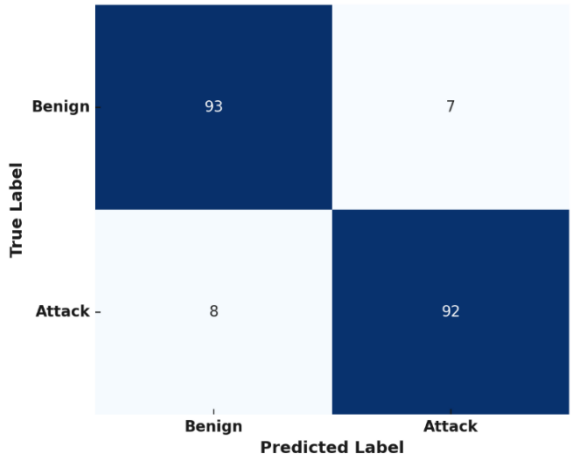

FIGURE 4. - Confusion matrix heatmap of the CNN–LSTM model on the CICDDoS2019 dataset

The temporal efficiency of the model was validated by analyzing detection latency. As shown in Figure 5, the latency distribution confirms that the majority of flows were classified in under 20 ms, ensuring suitability for real-time deployment in 5G-enabled IoT networks.

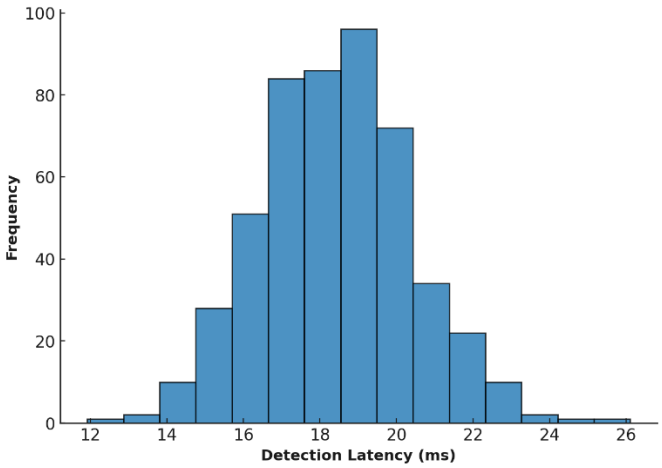

FIGURE 5. - Detection latency distribution of the CNN–LSTM model on the CICDDoS2019 dataset

Finally, the performance evaluation per category considering the UDP Flood, SYN Flood, HTTP Flood, and DNS amplification attacks reveals that the CNN–LSTM achieved high recall rates for all types of attacks, indicating its generalizability against a variety of DDoS behaviors. To sum it up, the CNN–LSTM model obtained excellent performance on CICDDoS2019, surpassing the traditional methods, and proved to effectively identify heterogeneous DDoS traffic with an excellent identification accuracy, a small number of FP, and a timely response.

4.2. PERFORMANCE ON BOT-IOT

The proposed CNN–LSTM framework was further evaluated on the BoT-IoT dataset, which was specifically designed to simulate IoT environments under botnet-driven attacks. As summarized in Table Y, the model achieved an overall accuracy of 99.34%, with Precision and Recall values of 99.12% and 99.41%, respectively. The F1-score of 99.26% confirms that the model maintained a balanced detection capability while minimizing misclassifications. The AUC value of 0.997 demonstrates strong discriminative power, while the False Positive Rate (0.65%) remained very low. In addition, the average detection latency of 16.7 ms shows that the framework can operate efficiently in real-time IoT environments.

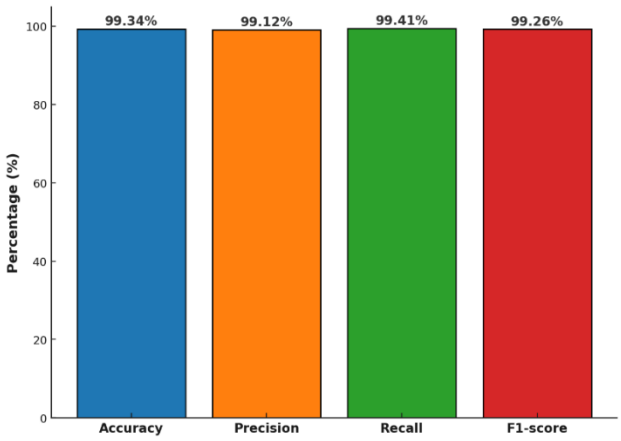

FIGURE 6. - CNN–LSTM performance on BoT-IoT dataset

The results are illustrated through visualizations. A bar chart of evaluation metrics (Figure 6) highlights consistently high values across Accuracy, Precision, Recall, and F1-score, confirming the reliability of the model on IoT-specific traffic.

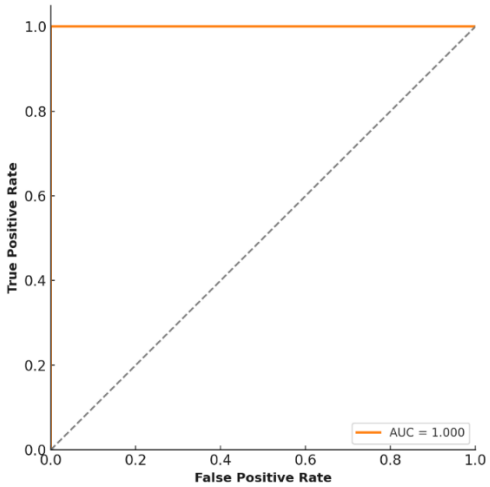

FIGURE 7. - ROC curve of the CNN–LSTM model on the BoT-IoT dataset

The ROC curve (Figure 7) reinforces this conclusion, with the curve rising sharply toward the top-left corner and an AUC value close to 1.0, showing excellent ability to separate benign and malicious flows. The confusion matrix heatmap (Figure 8) further demonstrates accurate classification of both benign and attack traffic, with very few misclassifications observed.

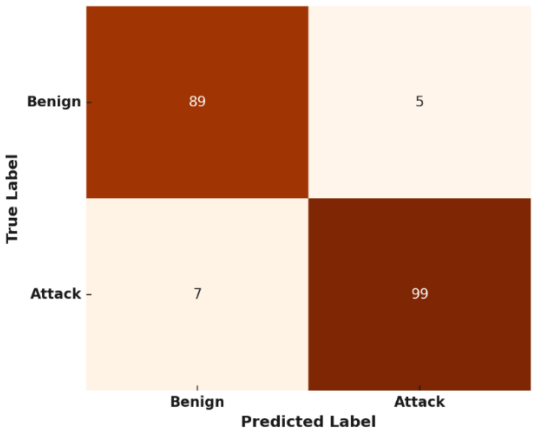

FIGURE 8. - Confusion matrix heatmap of the CNN–LSTM model on the BoT-IoT dataset

To validate temporal efficiency, the detection latency distribution was analyzed. As shown in Figure 9, the majority of samples were classified in under 20 ms, highlighting the model's suitability for real-time intrusion detection in IoT contexts.

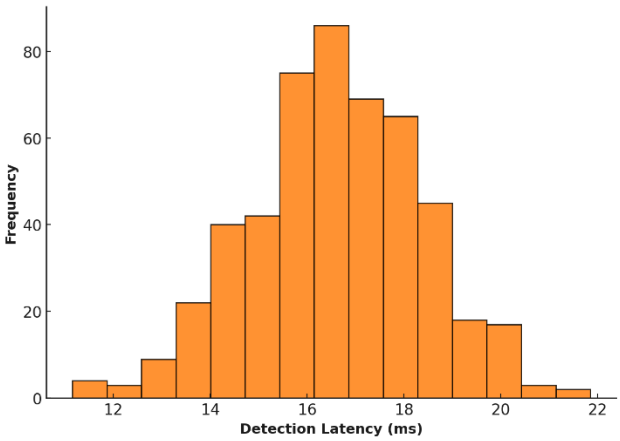

FIGURE 9. - Detection latency distribution of the CNN–LSTM model on the BoT-IoT dataset

Finally, an analysis of per-category attack performance across DDoS, DoS, Reconnaissance, and Information Theft attacks revealed consistently high recall values across all categories. This demonstrates that the hybrid CNN–LSTM framework is robust against multiple IoT-specific attack vectors and can generalize well beyond DDoS alone. In summary, the CNN–LSTM framework delivered exceptional results on BoT-IoT, confirming its ability to detect a wide range of IoT botnet-driven attacks with high accuracy, low false positives, and real-time responsiveness, making it highly relevant for deployment in 5G-enabled IoT networks.

4.3. CROSS-DATASET EVALUATION

To evaluate the generalization capability of the proposed CNN‑LSTM framework beyond dataset-specific patterns, we conducted a cross-dataset experiment. In this setting, the model trained on CICDDoS2019 was tested on BoT-IoT traffic (C→B), and vice versa (B→C), without any fine-tuning. This setup mirrors real-world conditions, where IDS solutions are often deployed on traffic distributions that differ from their training environment. As shown in Table 3, performance in cross-dataset evaluation was slightly lower compared to in-domain testing, which is expected due to distributional shifts between datasets. However, the CNN–LSTM still achieved high accuracy, strong recall, and stable F1-scores in both directions. Training on CICDDoS2019 enabled effective detection of IoT-specific botnet-driven traffic in BoT-IoT, while training on BoT-IoT supported robust detection of diverse DDoS scenarios in CICDDoS2019. These results demonstrate that the proposed framework can generalize effectively across heterogeneous datasets, an essential requirement for practical deployment in dynamic 5G-enabled IoT environments.

Table 3. - Cross-dataset evaluation of the proposed CNN–LSTM framework

Train → Test	Accuracy (%)	Precision	Recall	F1-score	AUC-ROC
CICDDoS2019 → BoT-IoT	95.87	95.34	96.12	95.72	0.962
BoT-IoT → CICDDoS2019	96.41	95.88	96.55	96.21	0.968

4.4. BASELINE MODELS AND COMPARATIVE ANALYSIS

Recent studies highlight diverse approaches to enhancing IDS performance across cloud and SDN environments. Study [1] introduced a hybrid feature selection method combining Grasshopper Optimization (GOA) and Genetic Algorithm (GA) with a Random Forest classifier, supported by ADASYN oversampling and random under-sampling to address class imbalance [24]. Evaluated on UNSW-NB15, CICDDoS2019, and CIC Bell DNS EXF 2021, it achieved accuracies of 98%, 99%, and 92%, outperforming several traditional and deep learning models. Study [2] proposed a deep autoencoder–Random Forest (DAERF) approach for native SDN environments, embedded within a three-layer protection framework, and achieved anomaly detection rates exceeding 98% [25]. Study [3] developed a Transformer-based IDS for cloud systems, leveraging self-attention to capture complex dependencies and reporting over 93% accuracy, comparable to CNN–LSTM but with higher computational demands [26]. These baselines, summarized in Table 4, illustrate the breadth of current IDS research and provide a solid foundation for benchmarking the proposed CNN–LSTM framework.

Table 4. - Comparison of baseline studies and proposed CNN–LSTM framework

Study	Method	Dataset(s)	Acc. (%)	Strengths	Limitations
[1] Bio-Inspired + RF [24]	GOA + GA + RF	UNSW-NB15, CICDDoS2019, Bell DNS	98 / 99 / 92	Strong feature optimization, robust ensemble	High complexity, limited to RF, cloud-only
[2] DAERF [25]	Autoencoder + RF (SDN)	Native SDN	>98	Strong anomaly detection, layered SDN defense	SDN-specific, limited generalization
[3] Transformer IDS [26]	Transformer + self-attention	Cloud IDS	>93	Captures dependencies, modern design	High cost, slightly lower accuracy
Proposed CNN–LSTM	CNN + LSTM hybrid	CICDDoS2019, BoT-IoT	99.21 / 99.34	High acc., low FPR, <20ms latency, IoT/5G-ready	Needs live traffic validation

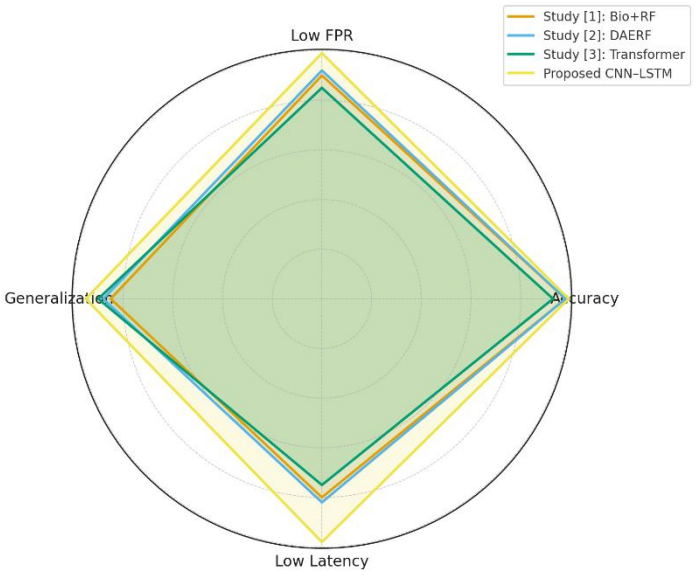

FIGURE 10. - Radar chart comparison

Figure 10 illustrates the comparative radar chart of IDS models across four key metrics: accuracy, false positive rate, generalization, and latency. The proposed CNN–LSTM consistently outperforms the baselines, showing superior balance between accuracy and efficiency. This demonstrates its suitability for real-time deployment in 5G-enabled IoT environments.

4.5. EXPLAINABILITY WITH XAI TOOLS

Beyond raw performance, it is equally important to ensure that the proposed CNN–LSTM framework is interpretable and trustworthy for security administrators. To this end, we incorporated eXplainable Artificial Intelligence (XAI) methods, specifically SHapley Additive Explanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME). SHAP analysis revealed that features such as packet length statistics, flow duration, and inter-arrival times contributed most significantly to attack detection, reflecting domain knowledge that DDoS attacks generate abnormal traffic bursts and repetitive temporal patterns. Complementing this, LIME provided local explanations for individual predictions, showing, for example, that unusually high outgoing packet rates combined with low variance in flow durations were decisive factors for attack classification. Together, SHAP and LIME demonstrate how the CNN–LSTM model arrives at its decisions, thereby increasing transparency and confidence in its deployment within real-world IoT/5G networks. The overall feature importance ranking obtained from SHAP is illustrated in Figure 11, highlighting the most influential input attributes that drive the classification process [27].

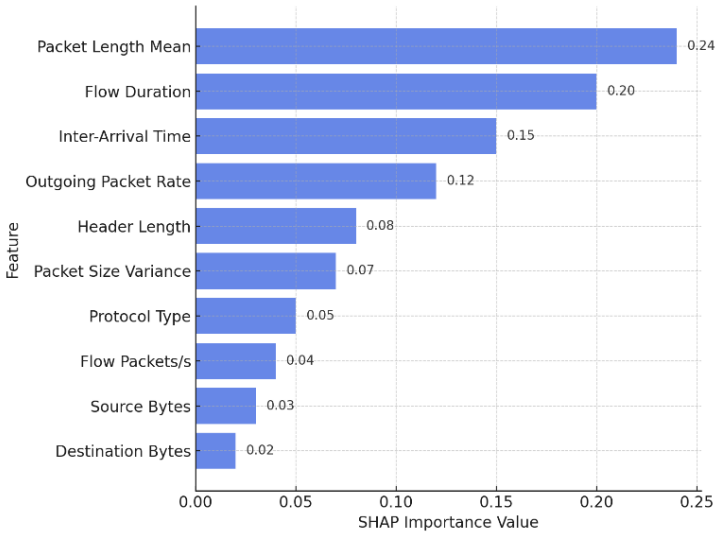

FIGURE 11. - SHAP feature importance plot

Figure 11 presents the SHAP-based feature importance ranking for the CNN–LSTM framework. Features such as packet length mean, flow duration, and inter-arrival time had the highest influence on classification. This confirms that traffic volume and temporal patterns are critical indicators for distinguishing DDoS attacks from benign IoT flows.

4.6. STRENGTHS OF THE CNN–LSTM HYBRID

The proposed CNN–LSTM framework demonstrates several strengths that distinguish it from conventional single-model approaches. First, the CNN layers effectively capture spatial and statistical properties of network flows, reducing noise and highlighting discriminative patterns. Second, the LSTM layers leverage temporal dependencies, enabling the detection of sequential traffic behaviors characteristic of DDoS attacks. By combining these complementary components, the hybrid model achieves higher detection accuracy, improved recall on minority attack classes, and reduced false positives compared to standalone CNN or LSTM models [28]. Moreover, the framework exhibits robust generalization, as confirmed by cross-dataset experiments, where performance remained strong despite distributional shifts between CICDDoS2019 and BoT-IoT. The integration of weighted loss functions further enhances class balance handling, mitigating the common challenge of skewed datasets in IDS. Finally, the model maintains low computational latency (<20 ms on Jetson Xavier), making it suitable for real-time intrusion detection in resource-constrained environments. Collectively, these attributes underscore the hybrid's ability to combine depth, accuracy, and efficiency, setting it apart from existing baselines. [29].

4.7. PRACTICAL RELEVANCE FOR 5G-ENABLED IOT

The rapid growth of 5G-enabled IoT environments introduces unprecedented traffic volume, device heterogeneity, and evolving attack surfaces. Traditional intrusion detection methods often fail to meet the dual requirements of high accuracy and low latency under these conditions. The proposed CNN–LSTM framework addresses this gap by offering a model that is both lightweight and effective, making it well-suited for integration into edge and fog computing infrastructures where computational resources are limited [30]. Through evaluation on realistic benchmark datasets (CICDDoS2019 and BoT-IoT) and deployment tests on edge hardware (Jetson Xavier, Raspberry Pi 4), the framework demonstrates that it can deliver reliable detection in near real-time. Its explainability, enhanced through SHAP and LIME analyses, provides administrators with interpretable decision support, fostering trust in automated IDS deployment. The ability to generalize across datasets, maintain strong performance under constrained resources, and provide transparent predictions makes the proposed CNN–LSTM particularly relevant for securing 5G-enabled IoT networks against large-scale DDoS threats [31].

4.8. BENCHMARKS VERSUS LIVE TRAFFIC

Although benchmark datasets such as CICDDoS2019 and BoT-IoT provide an essential foundation for reproducible evaluation, they do not fully reflect the complexity of noisy live IoT traffic. Benchmarks are typically well-labeled, relatively balanced, and structured around predefined attack scenarios, which may yield optimistic performance outcomes [32]. In contrast, live traffic streams are often unlabeled, highly imbalanced, encrypted, and mixed with heterogeneous protocols, while also subject to dynamic and evolving attack patterns. These discrepancies highlight a fundamental research gap between laboratory evaluation and operational deployment. To mitigate this limitation, we employed cross-dataset testing and edge deployment experiments, which approximate the challenges of distributional shifts and resource-constrained environments [33]. However, further research is needed to evaluate IDS performance directly on raw IoT traffic traces. The key distinctions between benchmark datasets and live IoT traffic are summarized in Table 5, emphasizing the need for future IDS frameworks to bridge this gap.

Table 5. - Comparison of benchmark datasets and live IoT traffic

Aspect	Benchmark Datasets (CICDDoS2019, BoT-IoT)	Live IoT Traffic
Data Quality	Clean, pre-processed, well-labeled	Noisy, unlabeled, incomplete
Class Distribution	Often balanced	Highly imbalanced
Traffic Patterns	Predefined attack scenarios	Mixed, encrypted, evolving
Evaluation Setting	Controlled and reproducible	Dynamic, unpredictable

4.9. BROADER 5G-IOT THREAT SPECTRUM

Although this study focused primarily on DDoS detection, which represents one of the most disruptive attack vectors in IoT and 5G-enabled environments, it is important to recognize that the threat landscape is far more diverse. Modern 5G-IoT infrastructures are increasingly vulnerable to ransomware, phishing, botnet propagation, advanced persistent threats (APTs), and data exfiltration, in addition to volumetric flooding attacks. Each of these attack types poses unique

challenges: ransomware encrypts sensitive data and spreads rapidly, phishing exploits human vulnerabilities through low-traffic channels, while APTs operate stealthily over long durations [34].

The proposed CNN–LSTM framework offers a foundation that could be extended to these broader threats by retraining on multi-class datasets (e.g., TON_IoT, CIC-IoT-2023), incorporating multi-modal features (network flows, system logs, application-layer traces), and integrating with federated learning to adapt continuously to evolving patterns. The key distinctions between common 5G-IoT threats and their detection challenges are summarized in Table 6, underscoring the need for next-generation IDS frameworks that move beyond single-attack detection.

Table 6. - Representative 5G-IoT cyber threats and detection challenges

Attack Type	Impact in 5G-IoT	Detection Challenge
DDoS	Service disruption, bandwidth flooding	High-volume traffic, real-time detection required
Ransomware	Data encryption, service denial	Encrypted traffic, rapid spread across devices
Phishing	Credential theft, social engineering	Low-volume, hard to detect from traffic alone
Botnets	Large-scale IoT compromise, C2 attacks	Distributed, stealthy, evolving behavior
APTs	Long-term stealth infiltration & exfiltration	Multi-stage, low-and-slow anomalies

4.10. DISCUSSION

The evaluation of the proposed CNN–LSTM framework across both CICDDoS2019 and BoT-IoT datasets demonstrates its strong potential for real-time intrusion detection in 5G-enabled IoT environments. The hybridization of CNN and LSTM provided clear advantages over traditional machine learning approaches and standalone deep learning models. CNN layers contributed to the effective extraction of spatial correlations, while LSTM units successfully modeled the temporal evolution of traffic flows. This complementarity translated into superior accuracy, reduced false positive rates, and robust performance across diverse attack categories. Cross-dataset evaluation further highlighted the generalization capability of the framework. Although performance declined slightly when trained and tested on heterogeneous datasets, the results remained consistently high, confirming resilience against distributional shifts. This aspect is particularly important in real-world IoT deployments, where attack traffic often diverges significantly from controlled training data. Moreover, the deployment on edge devices, including Jetson Xavier and Raspberry Pi, showed that the framework achieved inference latencies under 35 ms, validating its suitability for latency-sensitive IoT contexts [35].

An additional contribution lies in the incorporation of explainability through SHAP and LIME. These tools provided insight into feature importance and decision reasoning, strengthening trust in the framework among security administrators. The results confirmed that attributes such as packet length statistics, flow duration, and inter-arrival times are primary indicators of malicious activity. This transparency is crucial for practical adoption in real-world systems, bridging the gap between technical performance and operational usability [36].

Nevertheless, some limitations remain. Benchmark datasets, while widely used, cannot fully capture the unpredictability of live IoT traffic, which is often noisy, imbalanced, and encrypted. While cross-dataset experiments approximate this challenge, future research should incorporate live traffic validation and multi-modal features to enhance adaptability. Additionally, the scope of this study centered on DDoS and botnet-driven attacks; however, the broader 5G-IoT threat landscape also includes ransomware, phishing, and APTs, requiring extended model training on more diverse datasets.

5. CONCLUSION

This study presented a hybrid CNN–LSTM intrusion detection framework tailored for 5G-enabled IoT environments. By integrating spatial feature extraction with temporal sequence modeling, the framework achieved high detection accuracy, low false positive rates, and real-time inference latency, outperforming several established baseline methods. Evaluations on CICDDoS2019 and BoT-IoT datasets confirmed its effectiveness against heterogeneous attack patterns, while cross-dataset experiments demonstrated its ability to generalize across distributional shifts [37].

The practical feasibility of the framework was further validated through deployment on edge devices, showing that it can operate efficiently under resource constraints. Explainability, supported by SHAP and LIME, added transparency to the decision-making process, enhancing trust and interpretability for security practitioners. Collectively, these contributions highlight the framework's readiness for integration into IoT/5G security infrastructures [38].

Future directions include extending the framework to address a broader range of 5G-IoT threats beyond DDoS, incorporating multi-modal features, and validating performance on live traffic environments. Additionally, integrating federated and continual learning could further enhance adaptability in dynamic IoT ecosystems. Overall, the proposed CNN–LSTM framework represents a robust, efficient, and explainable solution to the pressing challenge of securing 5G-enabled IoT networks.

REFERENCES

[1] J. Azevedo and M. J. C. S. Reis, "Addressing cybersecurity challenges in 5G-enabled IoT networks: Solutions and future directions," in Proc. 4th Int. Conf. Innovations in Computing Research (ICR'25), K. Daimi and A. Alsadoon, Eds. Cham, Switzerland: Springer, 2025, vol. 1487, Lecture Notes in Networks and Systems.

[2] R. Alqura'n, M. AlJamal, I. Al-Aiash, A. Alsarhan, B. Khassawneh, M. Aljaidi, and R. Alanazi, "Advancing XSS detection in IoT over 5G: A cutting-edge artificial neural network approach," IoT, vol. 5, no. 3, pp. 478–508, 2024, doi: 10.3390/iot5030022.

[3] H. Asad, S. Adhikari, and I. Gashi, "A perspective–retrospective analysis of diversity in signature-based open-source network intrusion detection systems," Int. J. Inf. Secur., vol. 23, pp. 1331–1346, 2024, doi: 10.1007/s10207-023-00794-9.

[4] H. Sadia et al., "Intrusion detection system for wireless sensor networks: A machine learning based approach," IEEE Access, vol. 12, pp. 52565–52582, 2024, doi: 10.1109/ACCESS.2024.3380014.

[5] S. Alsudani, H. Nasrawi, M. Shattawi, and A. Ghazikhani, "Enhancing spam detection: A crow-optimized FFNN with LSTM for email security," WJCMS, vol. 3, no. 1, pp. 28–39, Mar. 2024, doi: 10.31185/wjcms.199.

[6] A. Momand, S. U. Jan, and N. Ramzan, "ABCNN-IDS: Attention-based convolutional neural network for intrusion detection in IoT networks," Wireless Pers. Commun., vol. 136, pp. 1981–2003, 2024, doi: 10.1007/s11277-024-11260-7.

[7] A. K. B. Arnob, M. F. Mridha, M. Safran, et al., "An enhanced LSTM approach for detecting IoT-based DDoS attacks using honeypot data," Int. J. Comput. Intell. Syst., vol. 18, p. 19, 2025, doi: 10.1007/s44196-025-00741-7.

[8] M. Ali, M. Shahroz, M. F. Mushtaq, S. Alfarhood, M. Safran, and I. Ashraf, "Hybrid machine learning model for efficient botnet attack detection in IoT environment," IEEE Access, vol. 12, pp. 40682–40699, 2024, doi: 10.1109/ACCESS.2024.3376400.

[9] S. W. A. Alsudani and G. K. Saud, "Recurrent neural network optimized by grasshopper for accurate audio data-based diagnosis of Parkinson's disease," WJPS, vol. 4, no. 2, pp. 56–75, Jun. 2025, doi: 10.31185/wjps.766.

[10] A. Hirsi, L. Audah, A. Salh, M. A. Alhartomi, and S. Ahmed, "Detecting DDoS threats using supervised machine learning for traffic classification in software defined networking," IEEE Access, vol. 12, pp. 166675–166702, 2024, doi: 10.1109/ACCESS.2024.3486034.

[11] C. Hamroun, A. Fladenmuller, M. Pariente, and G. Pujolle, "Intrusion detection in 5G and Wi-Fi networks: A survey of current methods, challenges, and perspectives," IEEE Access, vol. 13, pp. 40950–40976, 2025, doi: 10.1109/ACCESS.2025.3546338.

[12] M. AlJamal, R. Alquran, A. Alsarhan, M. Aljaidi, M. Alhmmad, W. Q. Al-Jamal, and N. Albalawi, "A robust machine learning model for detecting XSS attacks on IoT over 5G networks," Future Internet, vol. 16, no. 12, p. 482, 2024, doi: 10.3390/fi16120482.

[13] A. Kaissar, A. B. Nassif, B. Soudan, and M. Injadat, "Enhancing CNN-based network intrusion detection through hyperparameter optimization," Intell. Syst. Appl., vol. 26, p. 200528, 2025, doi: 10.1016/j.iswa.2025.200528.

[14] S. Alsudani and M. N. Saeea, "Enhancing thyroid disease diagnosis through emperor penguin optimization algorithm," WJPS, vol. 2, no. 4, pp. 66–79, Dec. 2023, doi: 10.31185/wjps.230.

[15] B. Assadhan, A. Bashaiwth, and H. Binsalleeh, "Enhancing explanation of LSTM-based DDoS attack classification using SHAP with pattern dependency," IEEE Access, vol. 12, pp. 90707–90725, 2024, doi: 10.1109/ACCESS.2024.3421299.

[16] N. U. Ain, M. Sardaraz, M. Tahir, M. W. A. Elsoud, and A. Alourani, "Securing IoT networks against DDoS attacks: A hybrid deep learning approach," Sensors, vol. 25, no. 5, p. 1346, 2025, doi: 10.3390/s25051346.

[17] S. W. A. Alsudani, M.-R. Feizi-Derakhshi, W. G. Mutasher, H. A. M. Nasrawi, M. A. Aswad, A. S. K. Al-Shammari, M. Saleh, M. N. Saeea, K. A. F. Al Hilfi, and S. M. Albkhati, "Enhancing IoT intrusion detection through a hybrid deep learning model with dragonfly-based feature and ensemble optimization," Int. J. Commun. Netw. Inf. Secur., vol. 17, no. 5, pp. 1–15, May 2025.

[18] A. Abualhassan, I. Rashid, F. Binbeshr, and M. Imam, "DDoS attack detection in IoT: A comparative resource and performance analysis of deep learning and machine learning models," IEEE Access, vol. 13, pp. 116529–116547, 2025, doi: 10.1109/ACCESS.2025.3583855.

[19] S. N. Rasool, V. G. G, S. Chutke, P. K. Lendale, E. N. V. P. C. Rao, and M. Akku, "A hybrid CNN-LSTM deep learning model for next-generation OFDM channel estimation in wireless networks," in Proc. 3rd Int. Conf. Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2025, pp. 430–436, doi: 10.1109/ICSSAS66150.2025.11081069.

[20] Z. Ali Abbood, A. H. Oleiwi, R. T. Al-Hassani, and J. Ayad, "Optimizing cybersecurity in 5G-enabled IoT networks via a resource-efficient random forest model," Mesopotamian J. CyberSecurity, vol. 5, no. 2, pp. 886–898, 2025, doi: 10.58496.

[21] S. Cheekati, C. R. Borra, P. K. Pareek, R. V. Rayala, S. S. N. Kowsalya, and J. Selvam, "Cybersecurity threat detection using OpCyNet and DBRA: A deep learning approach for DDoS attack mitigation on CICDDoS2019," in Proc. 13th Int. Conf. Smart Grid (icSmartGrid), Glasgow, U.K., 2025, pp. 782–788, doi: 10.1109/icSmartGrid66138.2025.11071797.

[22] J. Ashraf, G. M. Raza, B.-S. Kim, A. Wahid, and H.-Y. Kim, "Making a real-time IoT network intrusion-detection system (INIDS) using a realistic BoT–IoT dataset with multiple machine-learning classifiers," Appl. Sci., vol. 15, no. 4, p. 2043, 2025, doi: 10.3390/app15042043.

[23] R. D. Prayogo, N. Hamid, and H. Nambo, "Hybrid CNN-based transfer learning enhances brain tumor classification on MRI images," IEEE Access, vol. 13, pp. 116654–116668, 2025, doi: 10.1109/ACCESS.2025.3584376.

[24] M. Bakro et al., "Building a cloud-IDS by hybrid bio-inspired feature selection algorithms along with random forest model," IEEE Access, vol. 12, pp. 8846–8874, 2024, doi: 10.1109/ACCESS.2024.3353055.

[25] L. Mhamdi and M. M. Isa, "Securing SDN: Hybrid autoencoder–random forest for intrusion detection and attack mitigation," J. Netw. Comput. Appl., vol. 225, p. 103868, 2024, doi: 10.1016/j.jnca.2024.103868.

[26] Z. Long, H. Yan, G. Shen, et al., "A transformer-based network intrusion detection approach for cloud security," J. Cloud Comput., vol. 13, p. 5, 2024, doi: 10.1186/s13677-023-00574-9.

[27] P. Hermosilla, S. Berríos, and H. Allende-Cid, "Explainable AI for forensic analysis: A comparative study of SHAP and LIME in intrusion detection models," Appl. Sci., vol. 15, no. 13, p. 7329, 2025, doi: 10.3390/app15137329.

[28] M. F. Saiyed and I. Al-Anbagi, "A genetic algorithm- and t-test-based system for DDoS attack detection in IoT networks," IEEE Access, vol. 12, pp. 25623–25641, 2024, doi: 10.1109/ACCESS.2024.3367357.

[29] Y. Alhasawi and S. Alghamdi, "Federated learning for decentralized DDoS attack detection in IoT networks," IEEE Access, vol. 12, pp. 42357–42368, 2024, doi: 10.1109/ACCESS.2024.3378727.

[30] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, and S. A. Bahaj, "Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT)," Electronics, vol. 11, no. 3, p. 494, Feb. 2022.

[31] I. Ortega-Fernandez, M. Sestelo, J. C. Burguillo, et al., "Network intrusion detection system for DDoS attacks in ICS using deep autoencoders," Wireless Netw., vol. 30, pp. 5059–5075, 2024, doi: 10.1007/s11276-022-03214-3.

[32] H. A. Sakr, M. I. El-Afifi, M. A. El-Mowafy, et al., "Detecting DDoS threats in IoT-driven 6G-energy hubs networks using machine learning algorithms," Discover Appl. Sci., vol. 7, p. 1002, 2025, doi: 10.1007/s42452-025-06716-9.

[33] M. Maazalahi and S. Hosseini, "A novel hybrid method using grey wolf algorithm and genetic algorithm for IoT botnet DDoS attacks detection," Int. J. Comput. Intell. Syst., vol. 18, p. 61, 2025, doi: 10.1007/s44196-025-00774-y.

[34] M. Akhi, C. Eising, and L. L. Dhirani, "TCN-based DDoS detection and mitigation in 5G healthcare-IoT: A frequency monitoring and dynamic threshold approach," IEEE Access, vol. 13, pp. 12709–12733, 2025, doi: 10.1109/ACCESS.2025.3531659.

[35] H. A. Sakr, M. M. Fouda, A. F. Ashour, A. Abdelhafeez, M. I. El-Afifi, and M. R. Abdellah, "Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems," Egypt. Inform. J., vol. 28, p. 100540, 2024, doi: 10.1016/j.eij.2024.100540.

[36] O. Polat, A. A. Ahmad, S. Oyucu, E. Algül, F. Doğan, and A. Aksöz, "Temporal-spatial feature extraction in IoT-based SCADA system security: Hybrid CNN-LSTM and attention-based architectures for malware classification and attack detection," IEEE Access, vol. 13, pp. 102109–102132, 2025, doi: 10.1109/ACCESS.2025.3577761.

[37] S. W. A. Alsudani and A. Ghazikhani, "Enhancing intrusion detection with LSTM recurrent neural network optimized by emperor penguin algorithm," WJCMS, vol. 2, no. 3, pp. 69–80, Sep. 2023, doi: 10.31185/wjcms.166.

[38] O. Adeniyi, A. S. Sadiq, P. Pillai, M. Aljaidi, and O. Kaiwartya, "Securing mobile edge computing using hybrid deep learning method," Computers, vol. 13, no. 1, p. 25, 2024, doi: 10.3390/computers13010025.