Improving Fog Computing Security with Deep Learning

Ali-Alridha Khalil
Department of Information Networks, College of Information Technology, University of Babylon, Babil, Iraq
alialridhakhalili.net@student.uobabylon.edu.iq (corresponding author)

Mehdi Ebady Manaa
Intelligent Medical Systems Department, College of Sciences, Al-Mustaqbal University, Babil, Iraq | Department of Information Networks, College of Information Technology, University of Babylon, Babil, Iraq
mahdi.ebadi@uomus.edu.iq

Received: 10 July 2025 | Revised: 26 July 2025, 20 August 2025, and 23 August 2025 | Accepted: 26 August 2025

 DOI: https://doi.org/10.48084/etasr.13299

ABSTRACT

The rapid growth of the Internet of Things (IoT) has introduced new security challenges in distributed and resource-limited environments, most notably at the fog layer. Moreover, traditional Intrusion Detection Systems (IDS), which typically rely on cloud-based architectures and signature-based detection, are inadequate for meeting the latency, bandwidth, and adaptability requirements of Industrial IoT (IIoT) systems. In this research, we propose a hybrid Convolutional Neural Network–Long Short-Term Memory (CNN-LSTM) model tailored for fog-layer deployment. The model employs CNNs to extract local spatial features from network traffic and LSTMs to capture temporal dependencies associated with evolving threats. Evaluation is conducted using the Edge-IIoTset dataset, a comprehensive benchmark containing realistic IIoT traffic and 15 diverse attack types. Through extensive preprocessing, Chi-Squared (χ^2)-based feature selection, and architectural fine-tuning, the model achieves 100% accuracy, precision, recall, and F1-score in binary classification, achieving high-fidelity detection with low false positives and minimal computational overhead. These results validate the proposed model as a robust and scalable security mechanism for fog-based IIoT environments.

Keywords-internet of things; fog layer; intrusion detection system; convolutional neural network; long short-term memory

I. INTRODUCTION

The continuous expansion of the Internet of Things (IoT) is reshaping digital ecosystems, enabling data-driven automation across healthcare, manufacturing, and infrastructure. However, the inherently distributed and resource-constrained nature of IoT environments introduces vulnerabilities related to data integrity, authentication, and threat detection. Moreover, conventional cloud-centric security solutions often fail to meet the stringent latency, bandwidth, and reliability demands of large-scale IoT deployments [1].

To mitigate these challenges, fog computing has emerged as a complementary architectural paradigm that relocates computation and storage capabilities closer to IoT endpoints, thereby reducing latency and alleviating cloud dependency. This shift, however, increases the attack surface and exposes systems to volumetric threats such as Distributed Denial of Service (DDoS), injection attacks, fingerprinting, and ransomware [2].

These evolving threats underscore the limitations of conventional signature-based Intrusion Detection Systems (IDS), which rely on predefined attack signatures and often fail to detect novel or obfuscated intrusions. In response, anomaly-based detection methods powered by deep learning have gained momentum, offering the ability to identify behavioral deviations from normal traffic behavior [3]. Notably, hybrid architectures that integrate Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) units have shown superior performance by learning both spatial and temporal dependencies within network traffic [4].

The development and evaluation of these hybrid models have been supported by datasets such as Edge-IIoTset, which provides diverse IIoT traffic across multiple protocol layers and records of 15 attack types [5]. Studies using this dataset have demonstrated that CNN-LSTM and Deep Neural Network (DNN)-LSTM architectures achieve high accuracy in both binary and multiclass classification [6, 7]. Recent work has also focused on optimizing these models for fog-layer execution, where computational efficiency is critical [8].

To further improve detection capabilities, recent studies have implemented preprocessing enhancements including dummy encoding, entropy-based feature selection, and autoencoder-driven feature compression [9, 10]. Innovations such as federated learning and attention mechanisms have also been incorporated to enhance distributed model training while preserving data privacy and minimizing communication overhead [11, 12]. Additionally, the emergence of lightweight and explainable Artificial Intelligence (AI) models addresses the dual challenges of transparency and performance in constrained fog environments [13].

In this paper, we introduce a CNN-LSTM-based anomaly detection framework specifically designed for deployment at the fog layer. The model is trained and validated on the Edge-IIoTset dataset and performs binary classification of network traffic. Operating in an offline, non-real-time setting, the proposed solution is tailored to resource-limited fog deployments. Experimental evaluations reveal that the model achieves high accuracy and stability, demonstrating its promise as a robust and scalable cybersecurity solution for decentralized IIoT infrastructures.

II. RELATED WORK

Recent studies underscore the urgency for intelligent and efficient IDS in IoT. Various architectures and datasets have been explored to enhance detection accuracy and operational efficiency, with key contributions summarized in Table I.

Authors in [14] addressed intrusion detection in edge IoT devices using the Edge-IIoTset dataset with 14 attack types. They proposed a CNN-LSTM hybrid enhanced by CatBoost encoding for categorical preprocessing and Information Gain for feature selection. Oversampling and undersampling balanced the dataset, and the hybrid model outperformed CNN and LSTM alone, achieving 99.99% accuracy. Benefits include high precision and robustness against imbalanced data, though scalability and computational demands remain limitations.

Authors in [15] introduced an LSTM-CNN hybrid for real-time IDS using the BoT-IoT dataset, which includes attacks such as DDoS, reconnaissance, botnets, and data exfiltration. Their model achieved 99.87% accuracy, 99.89% precision, and 99.85% recall, outperforming CNN, Recurrent Neural Network (RNN), Bidirectional LSTM (BiLSTM), and Gated Recurrent Unit (GRU) baselines. The system remained robust under adversarial attacks (90.2% accuracy) and achieved real-time efficiency (2.3 ms/sample), while Shapley Additive Explanations (SHAP) analysis identified key features such as packet size and protocol. Limitations include high computational cost for lightweight IoT deployment.

Authors in [16] developed a CNN-LSTM IDS trained on the CICIoT2023 dataset and validated against the CICIDS2017 dataset, achieving 98.42% accuracy, 98.57% F1-score, and low training loss (0.0275). Despite cross-dataset robustness, the model exhibited a high false positive rate (9.17%) and low recall for benign traffic (61%), indicating a detection bias toward malicious flows.

Authors in [17] proposed a TabTransformer-based IDS for fog systems using the UNSW-NB15 dataset with correlation-based feature selection. The architecture achieved 98.35% binary and 97.22% multiclass accuracy with lower computational cost than traditional machine learning methods, making it suitable for fog deployment. However, performance degraded on underrepresented classes due to imbalance.

Authors in [18] designed IDS models including Multilayer Perceptron (MLP), CNN, LSTM, and CNN-LSTM for medical IoT systems. Evaluated on the UNSW-NB15 and Edge-IIoTset datasets, the CNN-LSTM achieved 99.99% binary and 96% multiclass accuracy, with false alarm rates below 2%. Advantages included adaptability and low false positives, though underperformance on minority classes such as malware and code injection remains a limitation [18].

Lastly, authors in [19] developed a lightweight CNN-BiLSTM IDS optimized for constrained IoT devices, achieving 97.28% binary and 96.91% multiclass accuracy on the UNSW-NB15 dataset. The design balanced efficiency and accuracy, with inference latency of only 3.8 seconds, outperforming conventional machine learning baselines. However, training time was relatively high (1220 s), limiting suitability for on-device real-time training [19].

TABLE I. SUMMARY OF RELATED WORK

Ref.	Problem Addressed	Method Used	Dataset	Accuracy	Benefits	Limitations
[14]	Intrusion detection in edge IoT	CNN-LSTM + CatBoost + Information Gain	Edge-IIoTset	99.99%	High precision, reduced overfitting	Computationally intensive; scalability limitations
[15]	Real-time IDS for IoT	LSTM-CNN hybrid	BoT-IoT	99.87%	Real-time response, low FPR (0.13%)	High model complexity for low-power devices
[16]	General IDS for IoT	CNN + LSTM	CICIoT 2023	98.42%	Cross-dataset robustness	High FPR (9.17%); low benign recall (61%)
[17]	Anomaly detection in fog computing	TabTransformer (continuous only)	UNSW-NB15	98.35%	Lightweight, low computational cost	Poor performance on minority classes
[18]	IDS for medical IoT	MLP, CNN, LSTM, CNN-LSTM	UNSW-NB15, Edge-IIoTset	99.99%	Versatile models, low false alarms	Underperformance on code injection/malware
[19]	Lightweight IDS for constrained IoT devices	Lightweight CNN-BiLSTM	UNSW-NB15	97.28%	High precision (98.59%), low inference time (3.8s)	Long training time (1220s); not ideal for on-device training

III. METHODOLOGY

To address the security challenges inherent in fog-based Industrial IoT (IIoT) systems, this study proposes a hybrid deep learning-based CNN-LSTM IDS. The rationale lies in their complementary capabilities: CNNs effectively capture spatial patterns in network traffic, while LSTMs model temporal dependencies often indicative of multi-stage attacks. This dual modeling capacity is essential for anomaly detection in IIoT environments characterized by high-volume, multi-protocol traffic. The methodology follows a structured pipeline of data preprocessing, Chi-Squared (χ^2)-based test, feature selection, and model training on the Edge-IIoTset dataset [5]. The overall architecture is shown in Figure 1.

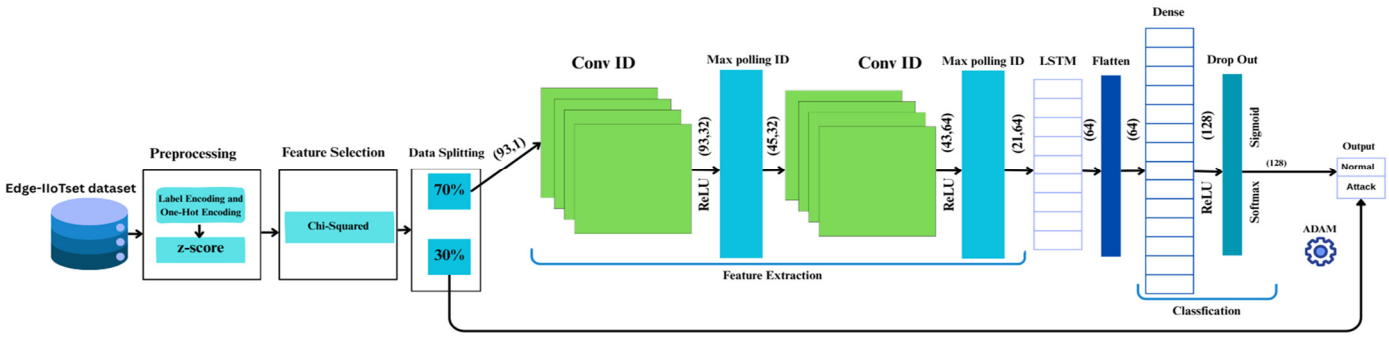

Fig. 1. Model architecture.

A. Dataset and Preprocessing

Experimental evaluation was conducted using the publicly available Edge-IIoTset dataset [5], which contains labeled network traffic designed for IIoT environments. The dataset includes diverse communication protocols and application-level features, such as Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), Address Resolution Protocol (ARP), and Message Queuing Telemetry Transport (MQTT), recorded in real-world scenarios. The preprocessing pipeline was designed to improve data quality and remove redundancy using the following procedures:

- Feature renaming: Columns with lengthy or unclear names (e.g., http.request.method, dns.qry.name.len) were shortened for readability.
- Encoding: Label encoding and one-hot encoding were applied to categorical fields from HTTP, DNS, and MQTT protocols, expanding the feature space.
- Redundancy filtering: Hash-based column comparison was employed to remove structurally duplicate features.
- Irrelevant attributes: Fields such as Internet Protocol (IP) addresses, port numbers, and raw payloads, which provide no classification utility, were removed.
- Data cleaning: Null records and duplicates were discarded to ensure consistency.

The resulting dataset contained 99 features and was randomized to ensure an unbiased learning process. The class distribution was balanced, with 1,399,624 normal traffic samples and 1,393,056 non-normal (attack) samples classified into 14 attack categories, including DDoS, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), HTTP, Internet Control Message Protocol (ICMP), Structured Query Language (SQL) injection, Cross-Site Scripting (XSS), port scanning, and ransomware, password cracking, Man-in-the-Middle (MITM), backdoor, vulnerability exploitation, command injection and directory traversal.

B. Feature Selection

To enhance accuracy and reduce computational cost, feature selection was applied using the χ^2 test [20]. This univariate statistical test measures the dependence of each feature on the binary target variable (Attack_label, normal vs. intrusion). The χ^2 score is computed as:

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \quad (1)$$

where O_i represents observed frequencies and E_i the expected frequencies under independence.

The test was implemented using the SelectKBest function in Scikit-learn, applied to all 99 features. The scores were ranked afterwards, and the first 93 features with the most discriminative power were used to train models. This value was chosen experimentally in order to balance out dimensionality reduction with model performance, such that key predictive features of network traffic were captured without over-reliance on noise and overfitting.

The chosen features covered different protocol layers and captured applicable statistical and behavioral characteristics of IIoT traffic that are vital for proper intrusion detection. These were features based on time, header-based attributes, and protocol indicators transformed from HTTP, DNS, and MQTT communications.

C. Model Architecture and Training

The proposed IDS employs a hybrid CNN-LSTM architecture designed to jointly learn local and temporal features from IIoT traffic:

- CNN layers: Two 1D convolutional layers with 32 and 64 filters, respectively, were used to extract hierarchical spatial features. Each convolutional block was followed by max-pooling to reduce dimensionality and emphasize salient patterns.

- LSTM layer: A subsequent LSTM layer with 64 units captured temporal dependencies, enabling detection of multi-stage or sequential attack behaviors.

Following feature extraction and sequence modeling, the output is flattened and fed into a dense layer of 128 neurons with ReLU activation. A dropout layer with a rate = 0.3 is added to avoid overfitting. The final classification is carried out through a single neuron with a sigmoid activation function, as applicable for binary classification.

The model was compiled using the Adam optimizer and binary cross-entropy loss. Training data was split into 70% training and 30% testing sets. All input features were standardized via z-score normalization to stabilize gradients and accelerate convergence. Input data was reshaped to (samples, features, 1) to match CNN-LSTM input requirements.

The development and testing of the presented IDS were performed on a high-performance local workstation with an Intel Core i7-14700K processor, 32 GB Random Access Memory (RAM), and an NVIDIA GeForce RTX 4070 Ti Super Graphics Processing Unit (GPU) running Windows 11. The configuration offered adequate computational power to support the heavy operations, such as convolutional operations and recurrent sequential processing.

D. Evaluation Metrics and Visualization

The trained CNN-LSTM model was then benchmarked with standard binary classifier measures to evaluate how effectively it can recognize intrusions in IIoT traffic. The performance was mostly gauged by examining accuracy, precision, recall, and F1-score, determined by utilizing the classification report function [21]. These measures give a wide perspective on how effectively the model can predict, particularly in cases with imbalanced data or when false positive and false negative costs are different.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (2)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (3)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (4)$$

$$\text{F1} - \text{score} = 2\frac{\text{Precision}\cdot\text{Recall}}{\text{Precision+Recall}} \quad (5)$$

A confusion matrix was also generated to show the distribution of true positives, true negatives, false positives, and false negatives. Both absolute values and normalized percentages were reported to better assess classification performance across the two classes: "No Intrusion" and "Intrusion". Training and test durations were also recorded to analyze the computational efficiency of the model. Model convergence was analyzed by tracking training and validation accuracy and loss across epochs, providing insight into potential overfitting or underfitting.

IV. RESULTS AND DISCUSSION

The CNN-LSTM model performed exceptionally well in detecting intrusions on the Edge-IIoTset dataset. As shown in Figure 2, the model achieved perfect classification, with no false positives or false negatives. All 419,375 normal samples and 164,260 intrusion samples were correctly identified, resulting in absolute accuracy.

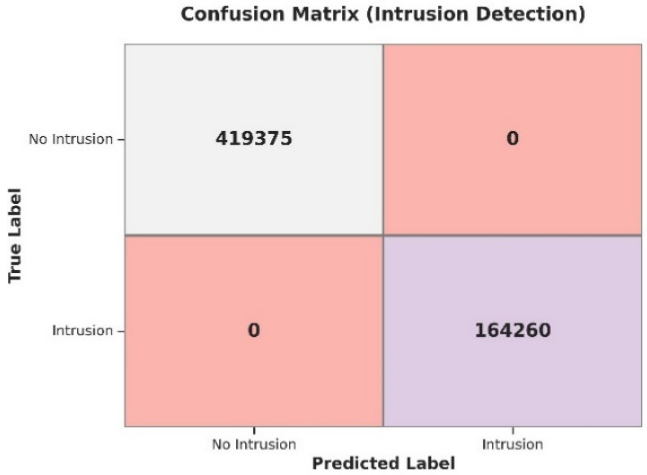

Fig. 2. Confusion matrix.

Figure 3 illustrates the training and validation accuracy across 10 epochs, where the model rapidly converged to nearly 100% within only a few epochs and remained stable, indicating robust generalization and minimal risk of overfitting. The training and validation accuracy curves remained closely aligned, confirming that the model captured genuine patterns rather than memorizing noise. The near-perfect accuracy observed from the first epoch (≈0.999) indicates that the model was able to rapidly capture the underlying patterns of the data. This performance likely reflects both the relative simplicity of the classification task and the effect of well-initialized model parameters. Strict separation of training, validation, and testing datasets ensured that evaluation metrics were not affected by data leakage. The close alignment of training and validation accuracy curves throughout the epochs demonstrate robust generalization rather than overfitting. The corresponding loss trends, presented in Figure 4, further support this observation. Training loss decreased steadily to near zero, while validation loss fluctuated minimally, with only a transient spike at epoch six that quickly stabilized in subsequent iterations.

The system's performance metrics are summarized in Table II, confirming 100% accuracy, precision, recall, and F1-score, with zero false positives and false negatives. Training and testing times further indicate computational efficiency compatible with real-time fog computing requirements. To further validate the model's efficiency, a comparative analysis was conducted against four recent CNN-LSTM-based IDS studies using different datasets, as shown in Table III. The proposed model achieved superior performance, surpassing results obtained with BoT-IoT, CICIoT2023, CICIDS2017, KDD99, and IoTID20 datasets.

Collectively, these findings demonstrate that the proposed model is not only highly accurate but also computationally efficient and scalable, making it well-suited for deployment in fog-based IIoT security frameworks.

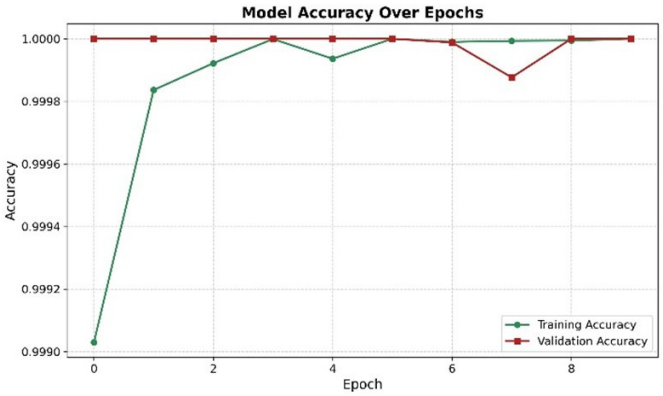

Fig. 3. Model accuracy.

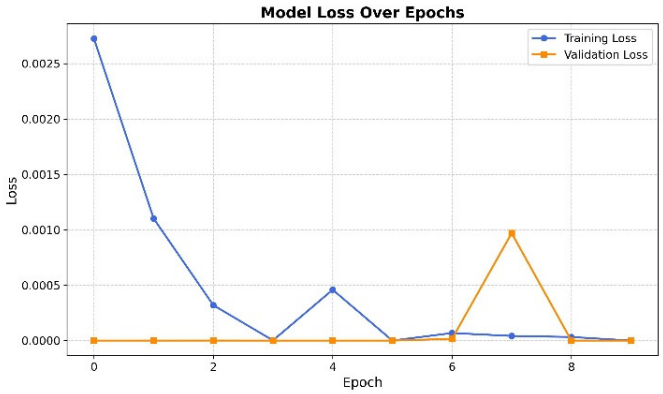

Fig. 4. Model loss.

TABLE II. PERFORMANCE MEASURE OF THE PROPOSED SYSTEM

Metric	Value
Test Accuracy	100.00%
Test Loss	0%
False Positive Rate	0%
False Negative Rate	0%
Precision	100%
Recall	100%
F1-Score	100%
Training Time	811.59 s
Testing Time	82.65 s

TABLE III. COMPARATIVE ANALYSIS WITH RELATED STUDIES

Study	Model	Dataset	Test Accuracy (%)	Loss (%)
Proposed System	CNN + LSTM	Edge-IIoTset	100	0
[15]	CNN + LSTM	BoT-IoT	99.87	0.13
[16]	CNN + LSTM	CICIoT2023 & CICIDS2017	98.42	1.58
[22]	CNN + LSTM	KDD99	99.78	0.22
[23]	CNN + LSTM	IoTID20	98.88	1.12

V. CONCLUSION

In this work, we proposed a deep learning-based Intrusion Detection System (IDS) that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to address the evolving security demands of Industrial Internet of Things (IIoT) environments. Utilizing the Edge-IIoTset dataset, our research highlights how hybrid models are capable of capturing both temporal and spatial information in network traffic to perform strong binary detection of normal and malicious traffic. Categorical feature representation, feature engineering, and z-normalization in the preprocessing pipe kept high-quality input for training. Our CNN-LSTM model performed remarkably with an accuracy of 100% with zero false positives or false negatives and outshining state-of-the-art methods in terms of efficiency and effectiveness.

In addition, because this model is lightweight and modular, it is particularly suitable for fog-layer deployments where computational resources are limited, and real-time inference is not always possible. Future research may investigate multiclass classification to distinguish between attacks, incorporate explainability techniques for interpretability, and analyze model performance on actual or emulated fog devices. Altogether, this proposed scheme adds a high-precision, scalable, and resource-efficient detection system for intrusions that can considerably strengthen the IIoT system's security posture.

REFERENCES

[1] A. Dauda, O. Flauzac, and F. Nolot, "A Survey on IoT Application Architectures," *Sensors*, vol. 24, no. 16, Aug. 2024, Art. no. 5320, https://doi.org/10.3390/s24165320.

[2] S. Altamimi, Q. A. Al-Haija, and M. Al-Fayoumi, "Fog computing security challenges and open issues: a short survey," *IET Conference Proceedings*, vol. 2023, no. 44, pp. 419–425, Feb. 2024, https://doi.org/10.1049/icp.2024.0961.

[3] A. A. Abd Al-Ameer and W. S. Bhaya, "Enhanced Intrusion Detection in Software-Defined Networks Through Federated Learning and Deep Learning," *Ingénierie des systèmes d information*, vol. 28, no. 5, pp. 1213–1220, Oct. 2023, https://doi.org/10.18280/isi.280509.

[4] R. H. Altaie and H. K. Hoomod, "An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16740–16743, Oct. 2024, https://doi.org/10.48084/etasr.7657.

[5] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, https://doi.org/10.1109/ACCESS.2022.3165809.

[6] T. Al Nuaimi *et al.*, "A comparative evaluation of intrusion detection systems on the edge-IIoT-2022 dataset," *Intelligent Systems with Applications*, vol. 20, Nov. 2023, Art. no. 200298, https://doi.org/10.1016/j.iswa.2023.200298.

[7] E. K. Kareem and M. E. Manaa, "Classification of Internet of Things Cybersecurity Attacks Using a Hybrid Deep Learning Approach," in *Innovations of Intelligent Informatics, Networking, and Cybersecurity*, vol. 2329, S. O. Al-Mamory, A. Al-Sherbaz, T. Kanakis, A. S. Albahri, W. S. Bhaya, E. S. Alshamery, A. A. Abdullah, A. Al-Ajeli, and S. Z. Alrashid, Eds. Cham: Springer Nature Switzerland, 2025, pp. 186–200.

[8] M. E. Manaa, S. M. Hussain, S. A. Alasadi, and H. A. A. Al-Khamees, "DDoS Attacks Detection based on Machine Learning Algorithms in IoT Environments," *Inteligencia Artificial*, vol. 27, no. 74, pp. 152–165, Jul. 2024, https://doi.org/10.4114/intartif.vol27iss74pp152-165.

[9] T. Hasan, A. Hossain, M. Q. Ansari, and T. H. Syed, "Enhanced Intrusion Detection in IIoT Networks: A Lightweight Approach with Autoencoder-Based Feature Learning." arXiv, Jan. 2025, https://doi.org/10.48550/arXiv.2501.15266.

[10] A. Z. Alrubayyi, A. A. Abd El-Aziz, and O. Ouda, "Real-Time Intrusion Detection For IIOT: Advancing Edge Computing Security with Machine Learning-Based Solutions," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 21s, pp. 4176–4189, Mar. 2024.

[11] O. Belarbi, T. Spyridopoulos, E. Anthi, I. Mavromatis, P. Carnelli, and A. Khan, "Federated Deep Learning for Intrusion Detection in IoT Networks." arXiv, Aug. 2023, https://doi.org/10.48550/arXiv.2306.02715.

[12] A. Gueriani, H. Kheddar, and A. C. Mazari, "Adaptive Cyber-Attack Detection in IIoT Using Attention-Based LSTM-CNN Models," in *2024 International Conference on Telecommunications and Intelligent Systems (ICTIS)*, Djelfa, Algeria, Dec. 2024, pp. 1–6, https://doi.org/10.1109/ICTIS62692.2024.10894509.

[13] S. Kaushik *et al.*, "Robust machine learning based Intrusion detection system using simple statistical techniques in feature selection," *Scientific Reports*, vol. 15, no. 1, Feb. 2025, Art. no. 3970, https://doi.org/10.1038/s41598-025-88286-9.

[14] M. Al Shahriar and A. Dey, "A Hybrid Approach of CNN and LSTM to Detect Intrusion in Edge IoT Devices using CatBoost," in *2023 26th International Conference on Computer and Information Technology (ICCIT)*, Cox's Bazar, Bangladesh, Dec. 2023, pp. 1–6, https://doi.org/10.1109/ICCIT60459.2023.10441595.

[15] P. Sinha, D. Sahu, S. Prakash, T. Yang, R. S. Rathore, and V. K. Pandey, "A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning," *Scientific Reports*, vol. 15, no. 1, Mar. 2025, Art. no. 9684, https://doi.org/10.1038/s41598-025-94500-5.

[16] A. Gueriani, H. Kheddar, and A. C. Mazari, "Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems." arXiv, May 2024, https://doi.org/10.48550/arXiv.2405.18624.

[17] A. I. A. Alzahrani, A. Al-Rasheed, A. Ksibi, M. Ayadi, M. M. Asiri, and M. Zakariah, "Anomaly Detection in Fog Computing Architectures Using Custom Tab Transformer for Internet of Things," *Electronics*, vol. 11, no. 23, Dec. 2022, Art. no. 4017, https://doi.org/10.3390/electronics11234017.

[18] I. Sy, B. Diouf, A. K. Diop, C. Drocourt, and D. Durand, "Enhancing Security in Connected Medical IoT Networks Through Deep Learning-Based Anomaly Detection," in *Mobile, Secure, and Programmable Networking*, vol. 14482, S. Bouzefrane, S. Banerjee, F. Mourlin, S. Boumerdassi, and É. Renault, Eds. Cham: Springer Nature Switzerland, 2024, pp. 87–99.

[19] M. Jouhari and M. Guizani, "Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices," in *2024 International Wireless Communications and Mobile Computing (IWCMC)*, Ayia Napa, Cyprus, May 2024, pp. 1558–1563, https://doi.org/10.1109/IWCMC61514.2024.10592352.

[20] M. L. McHugh, "The Chi-square test of independence," *Biochemia Medica*, pp. 143–149, 2013, https://doi.org/10.11613/BM.2013.018.

[21] K. A. Nadhum, S. M. Sam, and S. Usman, "Prediction Model Using Deep Learning for Lung Illness Severity Among Covid-19 Patients in Iraq," in *2024 5th International Conference on Smart Sensors and Application (ICSSA)*, Penang, Malaysia, Sep. 2024, pp. 1–6, https://doi.org/10.1109/ICSSA62312.2024.10788660.

[22] K. Prasanna, "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data," *Journal of Information and Computational Science*, vol. 10, no. 3, pp. 1362-1370, Mar. 2020, https://doi.org/10.5281/ZENODO.7911821.

[23] P. Phalaagae, A. M. Zungeru, A. Yahya, B. Sigweni, and S. Rajalakshmi, "A Hybrid CNN-LSTM Model With Attention Mechanism for Improved Intrusion Detection in Wireless IoT Sensor Networks," *IEEE Access*, vol. 13, pp. 57322–57341, 2025, https://doi.org/10.1109/ACCESS.2025.3555861.