MIKAILALSYS
Journal of Multidisciplinary Sciences

e-ISSN : 2987-2286
p-ISSN : 2987-3924

Index: Harvard, Boston, Sydney, Copernicus, Sinta 4, Scilit, Semantic, Google, etc

https://doi.org/10.58578/mikailalsys.v4i2.9178

Distributed Denial of Service (DDoS) Attack Detection and Prevention in Educational Internet of Things (EIoT) Using a Hybrid Convolutional Neural Network (CNN) and Artificial Intelligence (AI) Approach

Emmanuel Oche Onoja[1], Suleiman Muhammed Nasir[2], Adio Sabo Odah[3]
[1]Federal University of Technology, Minna, Nigeria; [2,3]Federal Polytechnic Nasarawa, Nigeria
onoskiss@gmail.com; mmsuleimano@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Feb 7, 2026	May 5, 2026	May 17, 2026	May 22, 2026

Abstract

The widespread adoption of electronic learning has made contemporary educational environments increasingly dependent on interconnected devices, enabling smart classrooms and remote monitoring systems. However, this technological advancement has also introduced substantial cybersecurity risks due to the vulnerabilities of unprotected, heterogeneous, and networked devices. Distributed Denial of Service (DDoS) attacks are among the most disruptive threats, as they can interrupt online classes, data access, and other educational services by flooding educational networks with illegitimate traffic. Existing signature-based DDoS detection mechanisms remain inadequate for Internet of Things (IoT) environments because of the dynamic nature of modern attacks and the resource limitations of connected devices. To address this challenge, this study proposed a hybrid deep learning model integrating Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) units, attention mechanisms, and incremental learning to enhance DDoS detection and prevention in Educational Internet of Things (EIoT) networks.

Mikailalsys is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The CNN layers were used to extract spatial features from network traffic, while the LSTM units captured temporal patterns and the attention mechanisms identified relevant traffic behavior. The incremental learning component employed geometric metrics to enable the model to capture previously unknown attack patterns. Experimental evaluation using the CIC-IoT2023 and BoT-IoT datasets showed that the proposed model achieved 99% detection accuracy for both known and emerging attacks in EIoT scenarios, supported by real-time traffic filtering and Software-Defined Networking (SDN)-based mitigation as prevention strategies. The model demonstrated strong adaptability, reduced false positives, and advanced AI-hybridized capabilities for DDoS detection and prevention in EIoT environments. These findings indicate that the proposed model is effective for detecting and preventing DDoS attacks against EIoT infrastructures and contributes to the development of adaptive cybersecurity solutions for technology-enhanced educational systems.

Keywords: Educational Internet of Things; Distributed Denial of Service; Hybrid CNN-LSTM; Attention Mechanism; Incremental Learning

INTRODUCTION

In recent years, they have been a paradigm shift toward hyper-connected, data-driven, and adaptive learning environments where physical objects such as sensors, actuators, wearables, smart boards, and RFID tags are interconnected with the internet and cloud platforms (Shukla et al. 2024), for real-time learning, evaluation and monitoring which has immensely enhance education and institutional efficiency (Alkaeed et al. 2024).

Educational Internet of Things (EIoT) represents the various applications of Internet of Things (IoT) technologies in different forms of teaching and learning, with the objectives of creating real-time and adaptive educational ecosystems, unrestricted and speedy learner-centric data flows, and intelligently achieving pedagogical goals without geographical barriers for all teaching and learning processes (Shukla et al. 2024).

The architectural layers of EIoT which include the; sensory layer, such as biometric wearables and object tags the edge and fog computing layer for real-time processing; the cloud and AI integration layer such as data lakes and predictive learning analytics; and Actuation layer such as automated laboratory equipment, enabled easy communication,

transmission and storage of educational data (Najafimehr et al. 2023; Aljumah 2023; Firdaus et al. 2024).

The application of Educational Internet of Things (EIoT) in various learning environments, particularly on campuses, including automated attendance, interactive whiteboards, virtual assessments, and remote laboratories (as shown in figure 1) has transform education dramatically especially in the area of connectivity but faced with challenges including threats such as DDoS attacks (Shukla et al. 2024). This attack disrupts electronic learning platforms, affecting thousands of students by overwhelming EIoT servers with unnecessary traffic (Altunay and Albayrak 2023; Alkaeed et al. 2024; Ebady Manaa, 2025.). Since most DDoS attacks mimic legitimate traffics and can come in low volumes, most traditional defence systems, such as firewalls, have proven ineffective it in most EIoT networks (Mittal et al. 2022; Shieh et al. 2023; Najafimehr et al. 2023; Aljumah 2023).

To provide adaptive solutions to these amplified vulnerabilities of EIoT to Distributed Denial of Service (DDoS) attacks, this research adopted deep learning approach by combining Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) to learn complex patterns from data and captures both spatial and sequential features of traffic streams, with an enhance detection precision via integrated attention mechanisms that prioritises relevant data segments (Altunay and Albayrak 2023; Ahmed Issa and Albayrak 2023; Khaleel and Shiltagh 2024; Wang et al. 2025; Li et al. 2025; Cengiz et al. 2025).

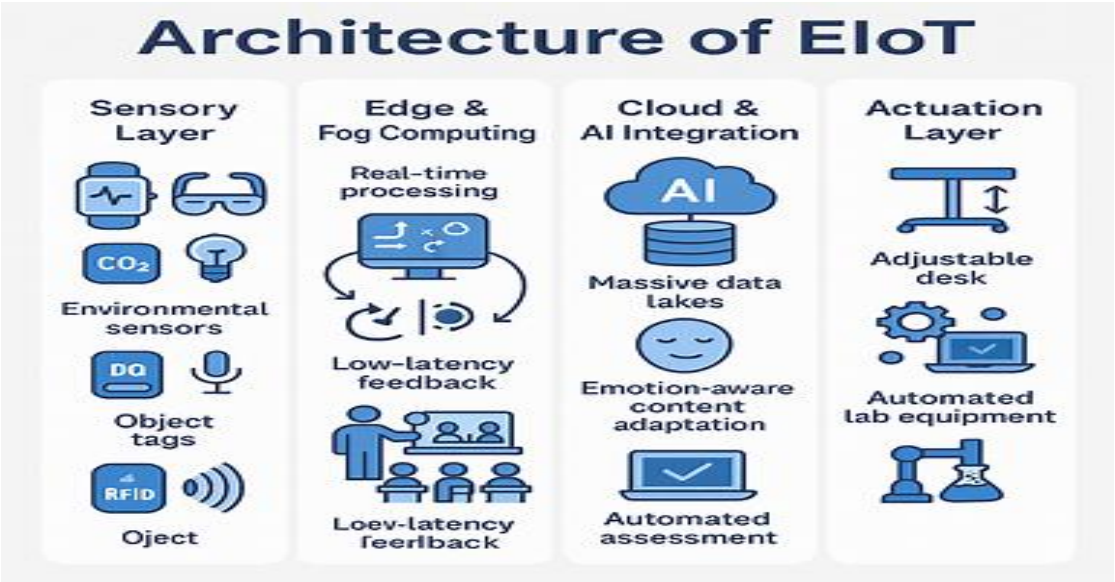

Figure 1. Architecture of Educational Internet of Things (EIoT) (Grok, 2026)

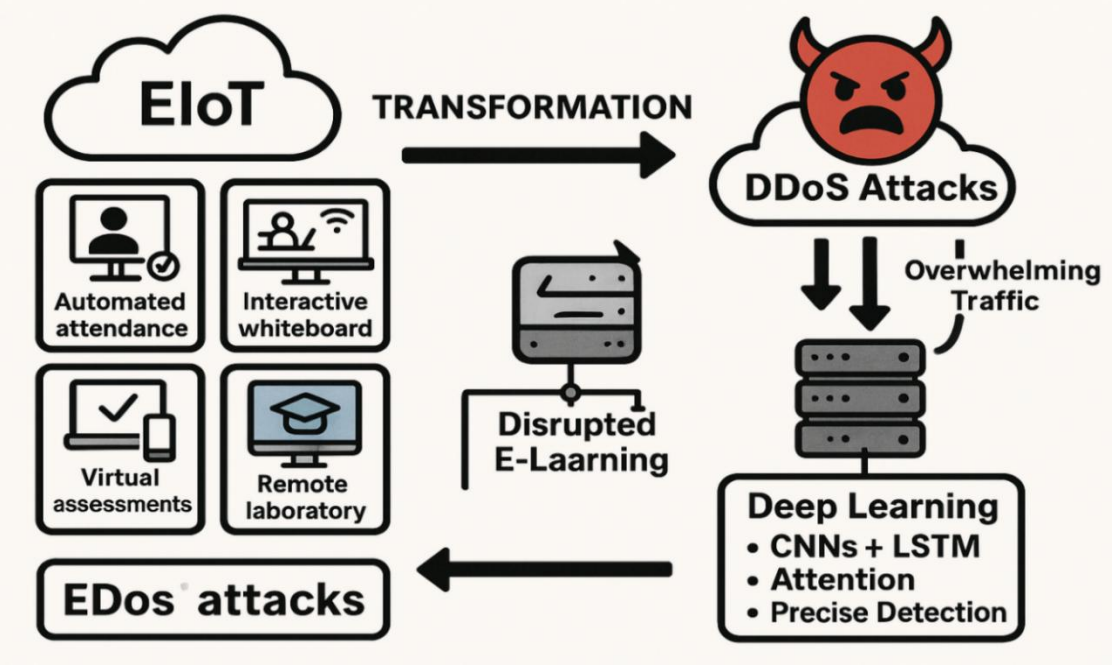

Figure 1. Educational Internet of Things (EIoT) and Attacks) (Grok, 2026)

A related threat, Economic Denial of Sustainability (EDoS), as shown in figure 2, targets cloud-based infrastructures by generating persistent traffic that gradually increases operational costs, draining financial resources. Traditional defence systems like firewalls are often ineffective against these dynamic and low-volume attacks systems (Mittal et al. 2022; Altunay and Albayrak 2023; Ain et al. 2025).

To address these challenges, deep learning provides adaptive solutions by learning complex traffic patterns. A hybrid approach that combines Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) components captures both spatial and temporal features of traffic streams (Cengiz et al. 2025; Ain et al. 2025; Shieh et al. 2023; Wang et al. 2025; Li et al. 2025). Integrating attention mechanisms further enhances detection by prioritising the most relevant data segments. This intelligent defence framework strengthens the resilience of EIoT systems against both DDoS and EDoS attacks, ensuring sustainable and secure educational connectivity.

Literature Review

The increased adoption of the Educational Internet of Things (EIoT), which includes but is not limited to smart classrooms, e-learning platforms, and campus-wide sensor networks, has heightened vulnerability to Distributed Denial of Service (DDoS)

attacks, leading to frequent disruptions in online education and data flows (Shukla et al. 2024; Alkaeed et al. 2024; Li et al. 2025; Susilo et al.2025; Al-Shurbaji et al. 2025).

Recent research highlights various mechanisms for real-time detection and mitigation against DDoS using a fusion of AI models and recurrent networks.

Shaaban et al. (2019) demonstrated the effectiveness of convolutional approaches for DDoS attack classification and detection. In a comprehensive review of methods of detecting and classifying DDoS attacks, Mittal et al. (2022) opined that deep learning is superior and more accurate than traditional signature-based techniques. In IoT-specific DDoS defense, deep learning is a suitable approach as it offers varying advantages over other traditional approaches (Al-Shurbaji et al. 2025; Najafimehr et al. 2023; Aljumah 2023; Firdaus et al. 2024).

To enhance the detection of unknown DDoS attacks, Shieh et al. (2023) proposed the use of geometrical metrics within convolutional neural networks, which is suitable for the EIoT environment. In the same vein, Setitra et al. (2023) optimized the MLP-CNN model for DDoS attacks classification and detection in SDN environments.

Shukla et al. (2024) suggested a novel solution to DDoS attacks in EIoT through an embedded multiclass framework for IoT network traffic classification. The results of implementation via K-fold validation on the BoT-IoT dataset showed 84.4% feature reduction and 5.19% accuracy improvement, achieving proactive EIoT defences such as campus DDoS filtering. The proposed framework offers efficient dimensionality reduction suitable for resource-constrained EIoT edge devices and robust multiclass handling (11 attack types) with high F1-scores (>0.95). Nevertheless, it has limited adaptability to dynamic EIoT threats owing to its reliance on traditional machine learning classifiers rather than deep hybrid models and inadequate integration with prevention mechanisms such as SDN.

A hybrid CNN-LSTM intrusion detection system for industrial IoT was proposed in Altunay and Albayrak (2023). The model is adaptable to EIoT using the UNSW-NB15 and X-IIoTID datasets. Implementation results showed 99.84% and 99.80% binary accuracy and multiclass precision in attack categorisation, respectively. The model demonstrates superior performance through hybrid fusion that captures sequential traffic anomalies in dynamic EIoT scenarios and outperforms standalone CNN and LSTM models by 2–5% in recall for subtle attacks. However, its higher computational demand

(e.g., LSTM's memory overhead) limits deployment on low-power EIoT sensors, and dataset bias towards industrial traffic may lead to underperformance in education-specific variability.

A hybrid CNN-LSTM-Autoencoder model was suggested for DDoS attack detection on IoT networks utilising the CIC-IoT2023 dataset in Ain et al. (2025). The proposed model achieved high accuracy of 96.78% with a moderate PCA-based reduction with high adaptability for privacy-sensitive learning analytics in the EIoT environment. The model provides in-depth anomaly modelling via reconstruction errors, excelling in unsupervised EIoT baselines, with 96.60% validation accuracy, surpassing baselines such as RNN by 4–6%. Nevertheless, the model remains vulnerable to some unknown EIoT attacks (e.g., HTTP floods, F1 < 0.90) and data imbalance with an increased rate of false negatives, which calls for augmentation for balanced EIoT traffic patterns.

A hybrid CNN-GRU model for SDN-based DDoS attack classification was proposed in Elshewey et al. (2025). The model achieved an excellent accuracy of 100% after SMOTE balancing on SDN traffic and was highly compatible with EIoT SDN controllers for seamless campus integration. It ensures stability through excellent F1 and ROC metrics with dropout regularisation and reduces EIoT training time by 20% owing to GRU's efficiency compared with LSTM. However, it was unable to perfectly handle traffic drifts in real-time EIoT environments such as exam surges and requires retraining for novel attacks, limiting zero-day prevention.

Elouardi et al. (2024) proposed a novel hybrid model of CNN-LLM for intrusion detection systems. implemented on CICIDS2017 datasets. The model achieved a high F1-score (>98%) for botnet detection. The model synthesises trends such as federated CNNs for scalable EIoT privacy and benchmarks hybrids against 95%+ baselines, although it lacks original EIoT-specific benchmarks and overlooks integration gaps with prevention tools such as blockchain.

These works collectively underscore the efficacy of hybridised CNN-AI approaches (>95% accuracy) for EIoT DDoS resilience, yet reveal ongoing needs for lightweight designs, imbalance handling, and domain-specific adaptations.

METHODOLOGY

System Architecture

The proposed model delivered an efficient, robust, and more adaptive security solution for Educational Internet of Things (EIoT) platforms, such as smart classrooms equipped with interactive boards and connected learning devices and cloud. The model is implemented through four core stages: preprocessing, hybrid deep learning classification, real-time detection and prevention, and AI-driven incremental learning.

The proposed model processes raw EIoT traffic (from smart boards) through CICFlowMeter to extract flow features, reshaped into 8×8 matrices with normalisation, balanced using SMOTE, and then fed into the hybrid CNN-LSTM-Attention model (CNN: 32→64 filters, 3×3 kernel + BatchNorm + MaxPool; Bi-LSTM: 128 units; Self-Attention (QKV); Dense: Sigmoid (binary) or Softmax (multi-class); Optimizer: Adam (lr=0.0001); Loss: Cross-entropy). Processed traffic enables immediate mitigation and loops back for adaptation when unknown patterns are detected via geometrical metrics.

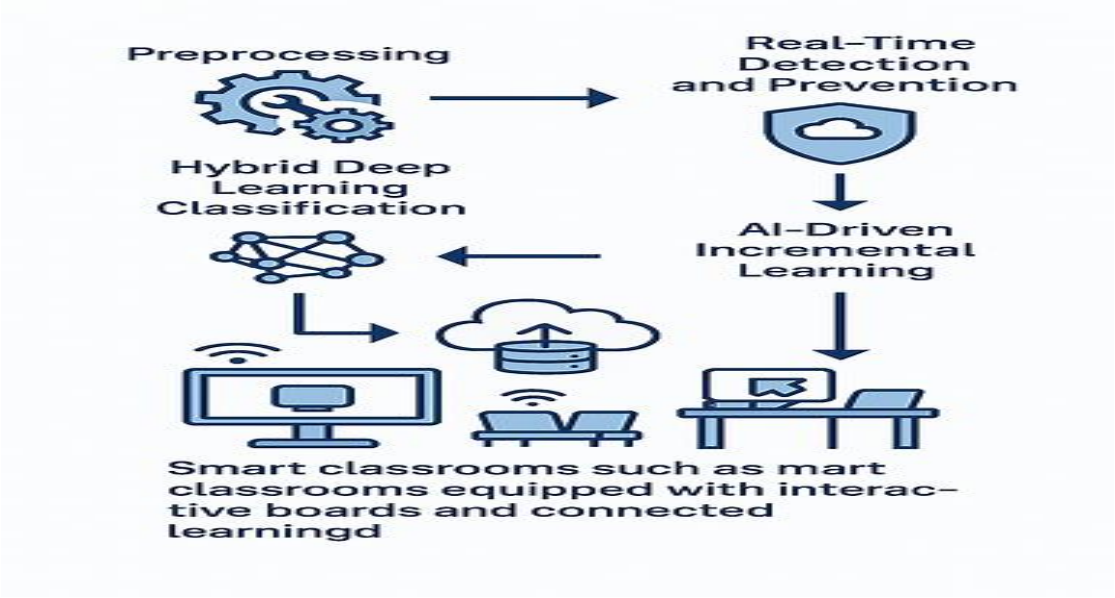

Figure 3. System Architecture (Grok, 2026)

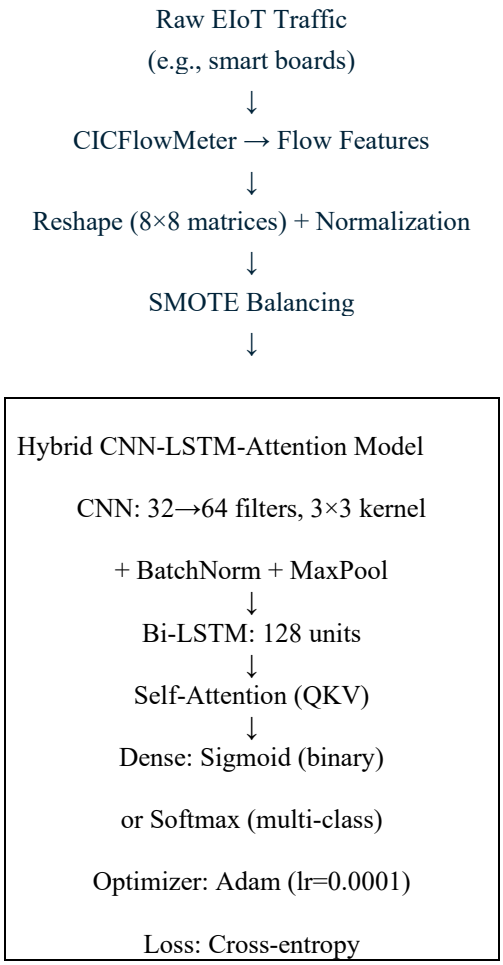

Figure 4. Overview of the Proposed EIoT Security Model

i. Preprocessing

EIoT network flows were captured using CICFlowMeter, extracting over 80 statistical features (e.g., packet sizes, inter-arrival times, protocol flags, flow duration), which were reshaped into 8×8 matrices to enable 2D convolutional processing, normalised to [0,1], and balanced via SMOTE to mitigate severe class imbalance inherent in intrusion datasets.

ii. Hybrid CNN-LSTM-Attention Model

The model systematically identifies and captures spatial patterns, temporal dependencies, and salient anomalies in irregular EIoT traffic. It was trained end-to-end using the Adam optimizer (learning rate = 0.0001) and cross-entropy loss.

The model comprises several operational blocks:

- CNN block: two layers with 32 and 64 filters (3×3 kernels, ReLU), each followed by batch normalisation and 2×2 max-pooling
- Bi-LSTM block: 128-unit bidirectional LSTM
- Self-Attention block: scaled dot-product attention with QKV projections
- Output head: fully connected layer with sigmoid (binary) or softmax (multi-class)

iii. Detection and Prevention

In inference mode, flows are classified in near real time. Anomalous predictions trigger SDN-based rate limiting, honeypot rerouting, and dynamic threshold adjustment to minimise disruption whilst neutralising threats.

iv. AI Incremental Learning

Continual adaptation uses geometrical metrics (Density and Coverage) in latent space to detect and incorporate novel patterns through low-rate incremental fine-tuning, avoiding catastrophic forgetting.

Experimental Setup

Datasets, Evaluation Metrics and Baselines

Experiments used the BoT-IoT (2019, often called CIC-BoT-IoT) and CIC-IoT 2023 datasets (33 attack types, 7 major classes, 105 IoT device topologies) with an 80/20 train/test split. Models implemented in TensorFlow with GPU acceleration. Evaluation metrics such as accuracy, precision, recall, F1-score, and Out-of-Distribution Detection Rate (ODR) were used. The baseline includes standalone CNN, standalone LSTM, CNN-BiLSTM, and MLP-CNN.

RESULTS AND DISCUSSION

Performance Analysis

The proposed model achieved 99.5% accuracy on CIC-IoT2023 (vs CNN 98.0%, LSTM 97.5%). Post-incremental learning ODR reached 99.2%.

Table 1. Performance comparison on BoT-IoT dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed Hybrid	99.8	99.7	99.6	99.7
CNN	98.5	98.4	98.3	98.4
LSTM	98	97.9	97.8	97.9
CNN-BiLSTM	99.2	99.1	99	99.1
Ensemble DL	99.5	99.4	99.3	99.4

Attention mechanism reduced false positives by 12%. Prevention strategies mitigated 94% of attacks with negligible legitimate traffic disruption.

The hybrid architecture excels in low-resource EIoT settings due to efficient spatial-temporal-attention fusion and continual adaptation. Minor computational overhead from incremental updates remains acceptable for school edge gateways.

CONCLUSION

This work presents a novel hybrid CNN-LSTM-Attention model with geometrical incremental learning, achieving state-of-the-art performance for DDoS detection and prevention in Educational IoT environments. The system effectively manages classroom traffic dynamics, detects sophisticated attacks, and adapts to emerging threats. Future work includes federated learning integration for privacy-preserving multi-campus collaboration.

REFERENCES

Ahmed Issa, A. S., & Albayrak, Z. (2023). DDoS attack intrusion detection system based on hybridization of CNN and LSTM. *Acta Polytechnica Hungarica, 20*(2), 105–123. https://doi.org/10.12700/APH.20.2.2023.2.6

Ain, N. U., Sardaraz, M., Tahir, M., Abo Elsoud, M. W., & Alourani, A. (2025). Securing IoT networks against DDoS attacks: A hybrid deep learning approach. *Sensors, 25*(5), Article 1346. https://doi.org/10.3390/s25051346

Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., Alotaibi, O. B., & Bajandouh, S. A. (2023). DDoS attack detection in IoT-based networks using machine learning models: A survey and research directions. *Electronics, 12*(14), Article 3103. https://doi.org/10.3390/electronics12143103

Al-Shurbaji, T. A., Anbar, M., Manickam, S., Hasbullah, I. H., Alfriehat, N., Alabsi, B. A., Alzighaibi, A. R., & Hashim, H. (2025). Deep learning-based intrusion detection system for detecting IoT botnet attacks: A review. *IEEE Access, 13*, 11792–11822. https://doi.org/10.1109/ACCESS.2025.3526711

Altunay, H. C., & Albayrak, Z. (2023). A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. *Engineering Science and Technology, an International Journal, 38*, Article 101322. https://doi.org/10.1016/j.jestch.2022.101322

Elouardi, S., Motii, A., Jouhari, M., Amadou, A. N. H., & Hedabou, M. (2024). A survey on hybrid-CNN and LLMs for intrusion detection systems: Recent IoT datasets. *IEEE Access, 12*, 180009–180033. https://doi.org/10.1109/ACCESS.2024.3506604

Elshewey, A. M., Abbas, S., Osman, A. M., Aldakheel, E. A., & Fouad, Y. (2025). DDoS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network. *Scientific Reports, 15*, Article 29122. https://doi.org/10.1038/s41598-025-13754-1

Grok. (2026). *About Grok*. https://www.grok.com

Gupta, B. B., Gaurav, A., Arya, V., & Kim, P. (2023). A deep CNN-based framework for distributed denial of services (DDoS) attack detection in Internet of Things (IoT). In *Proceedings of the 2023 International Conference on Research in Adaptive and Convergent Systems* (pp. 1–6). Association for Computing Machinery. https://doi.org/10.1145/3599957.3606239

Khaleel, T. J., & Shiltagh, N. A. (2024). DDoS cyber-attacks detection-based hybrid CNN-LSTM. In *Proceedings of Third International Conference on Computing and Communication Networks* (Lecture Notes in Networks and Systems, Vol. 917, pp. 523–537). Springer. https://doi.org/10.1007/978-981-97-0892-5_41

Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security, 127*, Article 103096. https://doi.org/10.1016/j.cose.2023.103096

Manaa, M. E., Hussain, S. M., Alasadi, S. A., & Al-Khamees, H. A. A. (2024). DDoS attacks detection based on machine learning algorithms in IoT environments. *Inteligencia Artificial, 27*(74), 152–165. https://doi.org/10.4114/intartif.vol27iss74pp152-165

Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft Computing, 27*, 13039–13075. https://doi.org/10.1007/s00500-021-06608-1

Najar, A. A., & Naik, S. M. (2025). DDoS attack detection using CNN-BiLSTM with attention mechanism. *Telematics and Informatics Reports, 18*, Article 100211. https://doi.org/10.1016/j.teler.2025.100211

Nuhu, A., Mat Raffei, A. F., Ab Razak, M. F., & Ahmad, A. (2024). Distributed denial of service attack detection in IoT networks using deep learning and feature fusion: A review. *Mesopotamian Journal of CyberSecurity, 4*(1), 47–70. https://doi.org/10.58496/MJCS/2024/004

Phalaagae, P., Zungeru, A. M., Yahya, A., Sigweni, B., & Rajalakshmi, S. (2025). A hybrid CNN-LSTM model with attention mechanism for improved intrusion detection in wireless IoT sensor networks. *IEEE Access, 13*, 57322–57341. https://doi.org/10.1109/ACCESS.2025.3555861

Sathaporn, P., Krungseanmuang, W., Chaowalittawin, V., Benjangkaprasert, C., & Purahong, B. (2025). DDoS detection using a hybrid CNN–RNN model enhanced with multi-head attention for cloud infrastructure. *Applied Sciences, 15*(21), Article 11567. https://doi.org/10.3390/app152111567

Setitra, M. A., Fan, M., Agbley, B. L. Y., & Bensalem, Z. E. A. (2023). Optimized MLP-CNN model to enhance detecting DDoS attacks in SDN environment. *Network, 3*(4), 538–562. https://doi.org/10.3390/network3040024

Shaaban, A. R., Abd-Elwanis, E., & Hussein, M. (2019). DDoS attack detection and classification via convolutional neural network (CNN). In *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)* (pp. 233–238). IEEE. https://doi.org/10.1109/ICICIS46948.2019.9014826

Shieh, C.-S., Nguyen, T.-T., & Horng, M.-F. (2023). Detection of unknown DDoS attack using convolutional neural networks featuring geometrical metric. *Mathematics, 11*(9), Article 2145. https://doi.org/10.3390/math11092145

Shukla, P., Krishna, C. R., & Patil, N. V. (2024). EIoT-DDoS: Embedded classification approach for IoT traffic-based DDoS attacks. *Cluster Computing, 27*, 1471–1490. https://doi.org/10.1007/s10586-023-04027-5

Susilo, B., Muis, A., & Sari, R. F. (2025). Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm. *Sensors, 25*(2), Article 580. https://doi.org/10.3390/s25020580