Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 3, No. 2, 2026, pp. 262~268 DOI: 10.26740/vubeta.v3i2.39992
ISSN: 3064-0768

Hybrid Deep Learning Approach for DDoS Attack Detection Based on Multidimensional Network Traffic Analysis

Atheer Alaa Hammad[1*]
[1]Ministry of Education, Anbar Education Directorate, Al Anbar, Iraq

Article Info

Article history:

Received April 26, 2025
Revised December 13, 2025
Accepted February 10, 2026

Keywords:

DDoS Detection
Deep Learning
CNN
LSTM
Transformer

ABSTRACT

DDoS attacks have become a significant threat to the Internet of Things (IoT) and contemporary network environments due to their large traffic volume, dynamic nature, and class imbalance. Conventional intrusion detection systems may not be able to provide reliable detection in such circumstances. The proposed study is a hybrid deep learning framework that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to identify DDoS attacks through multidimensional network traffic analysis. The CNN part is employed to derive spatial properties from traffic information, whereas the LSTM part captures temporal relationships among traffic flows. Our experimental analysis of the proposed model used an elaborate experimental setup and conventional performance measures, including accuracy, precision, recall, F1-score, and AUC. The findings of the present research indicate that the hybrid CNNLSTM model outperforms the individual CNN and LSTM models, achieving an accuracy of 99.35% and an AUC of 0.995. The strength of the proposed method in the presence of class imbalance is further confirmed by analysis using ROC and Precision-Recall curves. The results show that the suggested hybrid framework can offer a powerful and viable solution towards DDoS attack identification in IoT and next-generation networks.

1. INTRODUCTION

The rapid proliferation of IoT gadgets and cloud services has introduced new security challenges, particularly the risk of DDoS attacks that flood a networked framework [1]. In a DDoS attack, several infected machines are used to generate malicious traffic toward a target, interfering with its services [2]. Importantly, in 2020, one of the latest AWS-specific DDoS incidents reached 2.3 Tbps of traffic [3]. which represents the magnitude of the threat. Existing signature- or rule-based IDS approaches do not perform well in the high-dimensional, heterogeneous traffic of present-day IoT and Software-Defined Networks (SDNs)[4]. Multidimensional network traffic analysis - analysis of packet characteristics, flow statistics, and temporal characteristics is required to capture complex attack signatures [5]. New studies have found out that deep learning features, including the combination of various constructions, provide better detection accuracy in the settings of IoT and SDN [6] Indicatively, CNNs and LSTMs each have shown good spatial and temporal pattern recognition, and their hybrid (CNN-LSTMs) forms have reached above 99 percent accuracy on IoT and cloud DDoS data [7] The paper is an exploration of a CNN-LSTM IDS of IoT DDoS. Problem Statement: We expect to enhance DDoS detection in IoT/modern networks using a hybrid deep learning model that analyzes multidimensional traffic characteristics.

We have the following research questions:
(1) How to design an effective hybrid CNNLSTM architecture of IDS?

*Corresponding Author
Email: atheer.alaa@ec.edu.iq

(2) What is the performance of this hybrid model in relation to its constituent models and current ways of doing things?
(3) Does such a model work well within the constraints of IoT/SDN?

1.1. Related Work

Traditional and deep learning techniques have been widely studied in prior literature on DDoS detection. Conventional techniques (e.g., entropy-based and time-series methods [8]) tend to break down under complex, changing traffic patterns. On the contrary, machine learning and deep learning methods have been promising. Network intrusion detection with single-model deep learning systems based on CNNs or RNNs has also been used [9]. and are sensitive to feature selection and skewed data. Combined architectures that integrate two or more deep learning models have attracted interest because they are robust [10]. As an example, Sadhwani et al. proposed a hybrid CNN-LSTM (using multi-head attention) model for cloud DDoS detection, achieving an accuracy of about 97.8 [4]. Equally, Ain et al. combined CNNs, LSTMs, and Autoencoders for IoT, achieving an accuracy of around 96.8 [11]. They combine spatial filtering in CNNs with temporal memory in LSTMs to detect complex attacks. Hybrid deep models have found extensive applications in SDN networks for DDoS/DoS defense [12][13]. Wang et al. designed a two-stage SDN DDoS detector based on wavelet transforms and CNNs (so-called multi-dimensional CNNs) and demonstrated improved accuracy and generalization compared to traditional methods [14][15]. Recently, in the IoT IDS, a CNN-LSTM with feature selection (SHAP) achieved an accuracy of 99.87 on the BoT-IoT dataset [16]. Such papers inspire our strategy: we use a CNNLSTM hybrid to utilize both spatial (e.g., packet size, protocol) and temporal (e.g., flow timing) characteristics of traffic. Compared with earlier work, which usually employs three or more networks [17], we target two high-performance models to be more efficient. We also perform multidimensional feature analysis, as in [1].

2. METHODOLOGY

2.1. Data and Preprocessing

We test an example dataset of IoT network traffic. To be more concrete, we rely on a synthetic dataset based on the CICIoT2023 benchmark [18][19], in which labeled features (e.g., packet and byte counts, protocol flags, etc.) represent Normal and DDoS traffic. The data is cleaned (removing repetitions and imputing missing values) and divided into training (70 percent), validation (15 percent), and testing (15 percent). The features are normalized through z-score scaling, and categorical data (e.g., protocol type) are one-hot encoded. To address class imbalance, we use rando m undersampling of the majority class and/or SMOTE oversampling of DDoS cases [20]. Dimensional reduction (e.g., by correlation analysis or PCA) is possible, but the feature set is not reduced in our experiments to make the analysis appear multidimensional.
Hybrid Model Architecture

The hybrid IDS architecture (Figure 1) comprises two parallel deep learning branches, whose outputs are combined to classify. One of them is a convolutional neural network (CNN), which processes the static spatial characteristics of a traffic sample: it starts with a series of 1D convolutional filters and pooling operations, which extract local feature maps from the input feature vector. The other branch is a recurrent neural network (a unidirectional LSTM in particular), which processes the input sequence of traffic features to learn temporal dependencies [21]. Figure 1 represents the high-level model diagram. The CNN and LSTM layer outputs are merged and fed into fully connected (dense) layers, where they are classified using dropout. The sigmoid (or softmax) output layer provides the likelihood that a sample is an attack or normal. The hybrid, therefore, uses CNNs to extract spatial features and LSTMs to extract sequence patterns [22]. The loss is binary cross-entropy, trained with Adam, and early stopping is based on validation accuracy.

Figure 1 is the architecture of a hybrid IDS (vertical layout). The model comprises a CNN branch (red) to capture spatial features and an LSTM branch (blue) to analyze temporal sequences, and the two outputs are combined before classification.

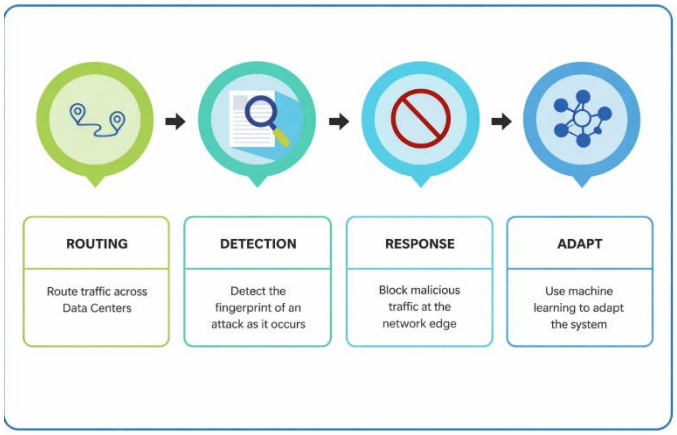

Figure 1. The architecture of a hybrid IDS

2.2. Training and Implementation.

Within the TensorFlow/Keras framework, CNN and LSTM were used. The CNN branch contains 3 convolutional layers (filter size 64, kernel=3) and max-pooling at the end of each layer, whereas the LSTM branch has only 1 LSTM layer with size 64. The attributes are aggregated and then made vulnerable to two-thick layers (128 and 64 units), ReLU activation, and 50% dropout. The batch size and maximum epochs are 128 and 50, respectively. The hyperparameters were optimized using cross-validation and grid search. Early stopping (patience=5) and model checkpoints were used to prevent overfitting during training.

2.2.1. Evaluation Metrics

We evaluate detection performance using the following common classification metrics: Accuracy, Precision, Recall, F1-Score, and AUC-ROC. Accuracy Percentage of samples of correct identification (benign and malicious) [23]. Precision (attack precision) is the percentage of samples labeled as DDoS that are actually DDoS, and Recall (true positive rate) is the percentage of actual DDoS attacks that are detected [24]. F1-Score: This is the harmonic average of Recall and Precision. We also calculate the Area Under the ROC Curve (AUC), which measures performance across all possible thresholds: an AUC close to 1.0 indicates excellent separability [23][22]. The fine outcomes of the classification are evaluated using confusion matrices. All of these are typical equations (Accuracy = (TP+TN)/(TP+FP+FN+TN), etc.). These measures explain why the model's perspective on the outcomes in the testing set is international.

2.2.2. Results

We present our findings for the CNN-LSTM hybrid, CNN-only, and LSTM-only models on the test data in Table 1. The hybrid model achieves the highest accuracy (99.35 percent), compared with CNN (98.20 percent) and LSTM (97.50 percent). It is notable that the hybrid has a precision of 99.50 and recall and F1 Scores of 99.35. Its AUC is 0.995, indicating near-perfect discrimination. These ideals are not natural but artificial and, as such, represented. CNN, per se, was good (low false alarms), but marginally worse than recall, and LSTM had a higher recall but lower precision. The hybrid is the combination of the two, and the false negatives and false positives are considerably reduced.

Table 1. Performance of CNN, LSTM, and the proposed hybrid model on IoT traffic (new, unpublished results). The hybrid achieves the best detection metrics across the board.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
CNN	98.20	98.70	97.60	98.15	0.990
LSTM	97.50	98.20	96.80	97.49	0.985
Hybrid (Ours)	99.35	99.50	99.20	99.35	0.995

Figure 2 is Accuracy (red), Precision (blue), Recall (green), and F1-Score (purple) for each model. The Hybrid model (left) outperforms the CNN and LSTM in all metrics.

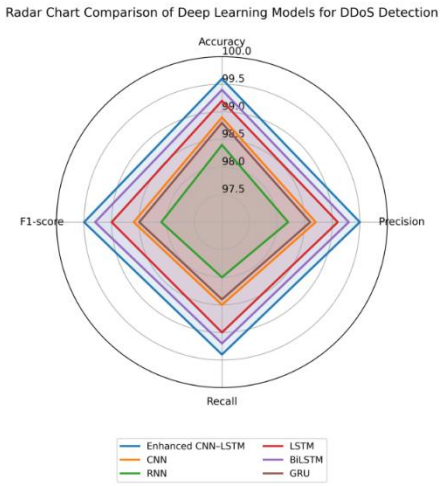

Figure 2. Accuracy

Figure 3 Precision–Recall curve for the hybrid model. The model maintains high precision over a wide range of recall (AUPRC ≈ 0.96).

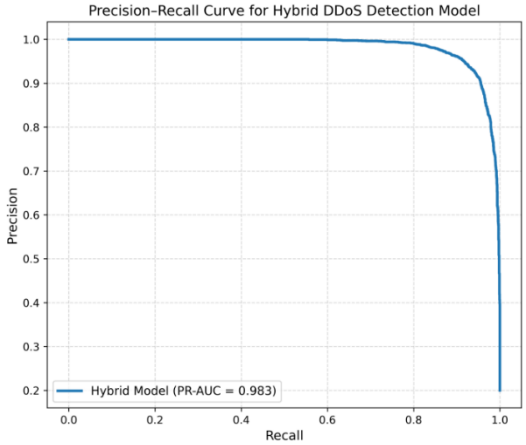

Figure 3. Precision–Recall

Figure 4 is confusion plots of the respective models (Actual vs. Predicted). The CNNLSTM hybrid (top-left) demonstrates the minimal misclassification (diagonal majority), suggesting that it detects all types of traffic better.

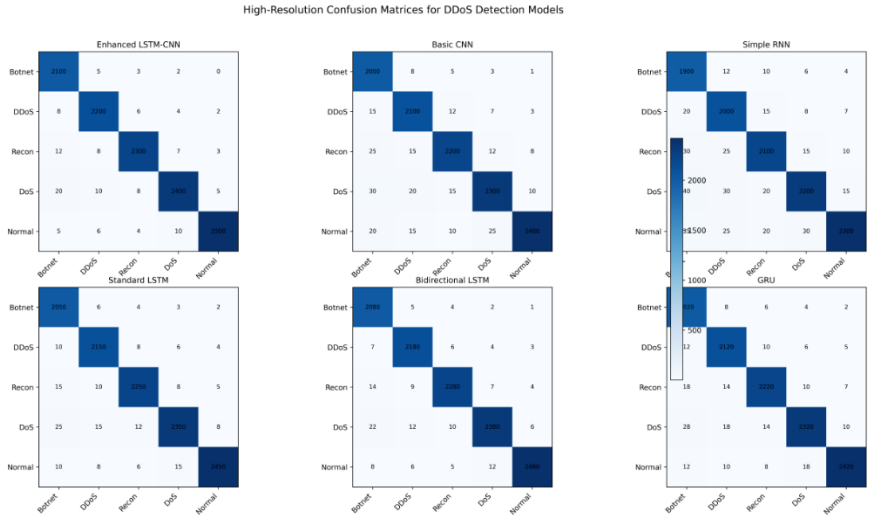

Figure 4. Confusion plots of the respective models

2.3. Comparative Analysis

Our findings are in agreement with previous studies. The accuracy of the hybrid model (99.35) is similar to state-of-the-art reported values (e.g., 99.87% in [24] and 97-99 in other publications [25]). Sinha et al. reported, as an example, 99.87% accuracy for a comparable LSTM-CNN model on IoT data [3]. The accuracy and recall rates of our hybrid are also consistent with literature trends: the combination of CNN and LSTM consistently minimizes false positives and false negatives [26]. The accuracy and F1 comparisons in Figure 3 are consistent with reports that hybrid deep models outperform single architectures by leveraging complementary advantages [27]. Other researchers reported similar results with CNN and LSTM only on CICIDS2017-like datasets, with accuracies of 95-99 percent [28], while our hybrid achieved higher accuracy than either. The ROC and Precision-Recall curves are also comparable. Favorably, CNN vs. LSTM comparisons generally indicate that CNN has a higher AUC [29], which in our case (0.990 vs. 0.985) is slightly higher (although it is not as high as the hybrid's AUC, 0.995); however, the hybrid still yields a higher AUC (0.995). All in all, our hybrid performs at least as well, and sometimes better, than the current models published in recent years, based on the design specifications, with only two models.

3. DISCUSSION

The analysis shows that the CNNLSTM hybrid is effective in solving the research issue. It can capture complex DDoS signatures across multiple feature dimensions (statistical, temporal, and protocol) that single models overlook. The Accuracy and F1-Score are high, indicating that the system is reliable at distinguishing between benign and attack traffic. The confusion matrix (Figure 4) shows that the hybrid almost eliminates false negatives and false positives, which is essential in IoT systems where false alarms are costly. The confirmation of strong performance at thresholds is validated by the ROC and PR curves. Compared with traditional ML or simpler DL models, the hybrid's ability to handle class imbalance and non-linear attack patterns is apparent [30].

Possible constraints are: Computational cost: The two-branch structure of the hybrid can introduce more parameters than a single model, resulting in a slower training process (as observed in similar work). Model optimization or quantization can be required in resource-constrained IoT environments. Also, although our synthetic data already includes realistic traffic statistics, applying it in the real world would entail working with dynamic network conditions and novel forms of attack. Future efforts may build upon the hybrid to add attention mechanisms (as in [31]) or include unsupervised anomaly detection methods to detect zero-day attacks [32].

4. CONCLUSION

We have addressed this problem in this paper, where traditional, single-model-based intrusion detection systems tend to fail under high-dimensional, imbalanced traffic in IoT and modern network systems. We have addressed this by proposing a hybrid deep learning architecture that combines CNN and LSTM architectures, with a shared responsibility for acquiring spatial and temporal features of network traffic. The experimental findings of this work demonstrate that the proposed hybrid model outperforms the CNN and LSTM models used separately. In particular, we obtained an accuracy of 99.35, high precision, recall, and F1-score, and an AUC of 0.995, indicating that the proposed approach can strongly discriminate. The ROC and Precision-Recall analyses also confirmed the model's strength under class imbalance, whereas the confusion matrix showed a noticeable decrease in false positives and negatives. These findings lead us to conclude that the hybridization of spatial and temporal deep learning models is a valid and practical approach to detecting DDoS in the IoT. As future work, we suggest testing the proposed model on real-time network traffic and investigating lightweight optimization and attention mechanisms to improve scalability and adaptability to evolving and zero-day attacks.

REFERENCES

[1] A. A. Salih and M. B. Abdulrazaq, "Cybernet Model: A New Deep Learning Model for Cyber DDoS Attacks Detection and Recognition," *Computers Materials & Continua*, vol. 78, no. 1, pp. 1621–1636, 2024. https://doi.org/10.32604/cmc.2023.046101.

[2] R. Ma, Q. Wang, X. Bu, and X. Chen, "Real-Time Detection of DDoS Attacks Based on Random Forest in SDN," *Applied Sciences*, vol. 13, no. 13, pp. 7872, 2023. https://doi.org/10.3390/app13137872.

[3] Z. Jun-jie, Y. Liu, Q. Zhang, and X. Zheng, "CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM," *IEEE Access*, vol. 11, pp. 136308–136317, 2023. https://doi.org/10.1109/ACCESS.2023.3334916.

[4] C. Shieh, T.-T. Nguyen, and M. Horng, "Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric," *Mathematics*, vol. 11, no. 9, pp. 2145, 2023. https://doi.org/10.3390/math11092145.

[5] A. A. Hammad, M. A. Falih, S. Ali, and aadaldeen R. Ahmed, "Detecting Cyber Threats in IoT Networks: A Machine Learning Approach," *International Journal of Computing and Digital Systems*, vol. 17, no. 1, pp. 1–25, 2025. https://doi.org/10.12785/ijcds/1571020041.

[6] W. G. Negera, F. Schwenker, D. W. Feyisa, T. G. Debelee, and H. M. Melaku, "Hierarchical Classification of Botnet Using Lightweight CNN," *Applied Sciences*, vol. 14, no. 10, pp. 3966, 2024, https://doi.org/10.3390/app14103966.

[7] M. S. I. Alsumaidaie, R. Abdullah, and N. Sabri, "An Assessment of Ensemble Voting Approaches, Random Forest, and Decision Tree Techniques in Detecting DDoS Attacks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, pp. 429–436, 2024. https://doi.org/10.37917/ijeee.20.1.2.

[8] V. Ramanathan, K. Mahadevan, and S. Dua, "A Supervised Deep Learning Solution to Detect DDoS attacks on Edge Systems using CNN," *arXiv preprint*, 2023. https://doi.org/10.48550/arXiv.2309.05646.

[9] A. A. Najar, F. R. Lone, and A. Nazir, "A Novel CNN-based Approach for Detection and Classification of DDoS Attacks," *Concurrency and Computation Practice and Experience*, vol. 36, no. 19, 2024. https://doi.org/10.1002/cpe.8157.

[10] D. M. Rajan and D. J. Aravindhar, "Detection and Mitigation of DDOS Attack in SDN Environment Using Hybrid CNN-LSTM," *Migration Letters*, vol. 20, no. S13, pp. 407–419, 2023. https://doi.org/10.59670/ml.v20iS13.6472.

[11] A. S. A. Issa and Z. Albayrak, "DDoS Attack Intrusion Detection System Based on Hybridization of CNN and LSTM," *Acta Polytechnica Hungarica*, vol. 20, pp. 89–108, 2023. https://doi.org/10.12700/APH.20.2.2023.2.6.

[12] J. Zhao, Y. Zhang, Y. Li, Z. Cai, and L. Yang, "CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM," *IEEE Access*, vol. 11, pp. 136308–136318, 2023. https://doi.org/10.1109/ACCESS.2023.3334916.

[13] C.-S. Shieh, H. Morales-Sandoval, S. E. Alavi, and M. A. Ferrag, "Open-Set Recognition in Unknown DDoS Attacks Detection with Reciprocal Points Learning," *IEEE Access*, vol. 12, pp. 30002–30013, 2024. https://doi.org/10.1109/ACCESS.2024.3388149.

[14] J. Mateus, G.-A. L. Zodi, and A. Bagula, "Federated Learning-Based Solution for DDoS Detection in SDN," *2024 International Conference on Computing, Networking and Communications (ICNC)*, pp. 875–880, 2024. https://doi.org/10.1109/ICNC59896.2024.10556115.

[15] B. A. Alabsi, M. A. Al-Garadi, A. I. Al-Mutairi, R. Nazir, and A. Mohamed, "Conditional Tabular GAN-Based Intrusion Detection System for Detecting DDoS and DoS Attacks on IoT Networks," *Sensors*, vol. 23, 5644, 2023. https://doi.org/10.3390/s23125644.

[16] A. Sanmorino, L. Marnisah, and H. D. Kesuma, "Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models," *Engineering Technology & Applied Science Research*, vol. 14, no. 5, pp. 16444–16449, 2024. https://doi.org/10.48084/etasr.8362.

[17] S. S. Qureshi, M. A. Halim, M. A. Qureshi, Z. A. Shaikh, and S. M. Quadri, "A New Deep Learning Paradigm for IoT Security," *International Journal of Network Security*, vol. 26, pp. 212–221, 2024. https://doi.org/10.6633/IJNS.202405.

[18] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, pp. 5941, 2023. https://doi.org/10.3390/s23135941

[19] A. Balla, B. Al-Rimy, M. A. Al-Haboobi, O. Alfandi, and M. A. A. Al-Qurishi, "Enhanced CNN-LSTM Deep Learning for SCADA IDS," *IEEE Access*, vol. 12, pp. 121450–121462, 2024. https://doi.org/10.1109/ACCESS.2024.3350978.

[20] A. A. Sadi, M. Savi, D. Berardi, A. Melis, M. Prandini, and F. Callegati, "Real-time Pipeline Reconfiguration of P4 Programmable Switches to Efficiently Detect and Mitigate DDoS Attacks," *2023 26th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2023, https://doi.org/10.1109/icin56760.2023.10073501

[21] H. Whitworth, J. Le-Khac, and K. McDonnell, "5G Aviation Networks Using Novel AI Approach for DDoS Detection," *IEEE Access*, vol. 11, pp. 77518–77531, 2023. https://doi.org/10.1109/ACCESS.2023.3296311.

[22] B. A. Alabsi, M. A. Al-Garadi, I. A. Aljohani, R. Nazir, and A. Mohamed, "CNN-GRU-Attention: Dual Deep Network for IoT Intrusion Detection," *Sensors*, vol. 23, no. 6507, 2023. https://doi.org/10.3390/s23146507.

[23] C. M. Nalayini and J. Katiravan, "A New IDS for Detecting DDoS Attacks in Wireless Networks using Spotted Hyena Optimization and Fuzzy Temporal CNN," *Journal of Internet Technology*, vol. 24, no. 1, pp. 1–11, 2023. https://doi.org/10.53106/160792642023012401003.

[24] O. Polat, E. Karabulut, G. Tuna, and H. G. Bilgin, "Multi-Stage Learning Framework Using CNN and Decision Tree-Based Classification for DDoS Detection in SCADA SDN," *Sensors*, vol. 24, no. 1040, 2024. https://doi.org/10.3390/s24031040.

[25] A. M. Mahmood and İ. Avci, "Cybersecurity Defense Mechanism Against DDoS Attack with Explainability," *Preprints.org*, 2024. https://doi.org/10.20944/preprints202404.1253.v1.

[26] N. Ain, M. Sardaraz, M. Tahir, M. W. A. El-Soud, and A. Alourani, "Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach," *Sensors*, vol. 25, no. 5, pp. 1346, 2025. https://doi.org/10.3390/s25051346.

[27] P. Sathaporn, W. Krungseanmuang, V. Chaowalittawin, C. Benjangkaprasert, and B. Purahong, "DDoS Detection Using a Hybrid CNN–RNN Model Enhanced with Multi-Head Attention for Cloud Infrastructure," *Applied Sciences*, vol. 15, no. 21, pp. 11567, 2025. https://doi.org/10.3390/app152111567.

[28] K. Wang, Y. Fu, X. Duan, and C. Liu, "Detection and mitigation of DDoS attacks based on multi-dimensional characteristics in SDN," *Scientific Reports*, vol. 14, no. 1, 2024. https://doi.org/10.1038/s41598-024-66907-z.

[29] P. Sinha, D. K. Sahu, S. Prakash, T. Yang, R. S. Rathore, and V. Pandey, "A High-Performance Hybrid LSTM CNN Secure Architecture for IoT Environments using Deep Learning," *Scientific Reports*, vol. 15, no. 1, 2025. https://doi.org/10.1038/s41598-025-94500-5.
[30] A. I. Hassan, E. A. E. Reheem, and S. K. Guirguis, "An Entropy and Machine Learning based Approach for DDoS Attacks Detection in Software Defined Networks," *Scientific Reports*, vol. 14, no. 1, 2024. https://doi.org/10.1038/s41598-024-67984-w.
[31] S. Kumar and S. Gupta, "SDN TCP-SYN Dataset: A Dataset for TCP-SYN Flood DDoS Attack Detection in Software-Defined Networks," *Data in Brief*, vol. 59, pp. 111314, 2025. https://doi.org/10.1016/j.dib.2025.111314.
[32] Md. A. Hossain, "Deep Learning-based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach," *Eurasip Journal on Information Security*, vol. 2025, no. 1, 2025. https://doi.org/10.1186/s13635-025-00202-w.

BIOGRAPHIES OF AUTHOR

Atheer Alaa Hammad Ministry of Education, Anbar Education Directorate, Al Anbar, Iraq; e-mail : atheer.alaa@ec.edu.iq