KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

Journal of Advanced Research in Social and Behavioural Sciences

Journal homepage:
https://karyailham.com.my/index.php/jarsbs/index
ISSN: 2462-1951

Design and Evaluation of a Hybrid CNN–LSTM Model for Distributed Denial of Service Detection in The Internet of Medical Things

Md Foysal[2], Azuan Ahmad[1,*], Mohd Ilias M. Shudud[2], Madihah Mohd Saudi[2]

[1] Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Malaysia,71800,Nilai,Negari Sembilan, Malaysia
[2] Cybersecurity and Systems Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Malaysia,71800, Nilai,Negari Sembilan, Malaysia

ARTICLE INFO

Article history:
Received 10 March 2026
Received in revised form 23 March 2026
Accepted 24 March 2026
Available online 26 March 2026

Keywords:
IoMT security; DDoS detection; deep learning; convolutional neural network; long short-term memory

ABSTRACT

The Internet of Medical Things (IoMT) has greatly revolutionized modern healthcare by allowing for real-time patient monitoring, effective medical data exchange, and improved clinical decision-making. However, the rapid growth and interconnectivity of IoMT devices have also heightened their susceptibility to cybersecurity threats, particularly Distributed Denial of Service (DDoS) attacks. Such attacks can disrupt vital healthcare services, reduce system availability, and compromise sensitive patient information, thereby posing significant risks to patient safety and operational reliability. Standard intrusion detection systems (IDS), including signature-based and rule-based techniques, often lack the adaptability required to detect the evolving and sophisticated DDoS attack patterns in IoMT environments. This study aims to design and assess a hybrid deep learning-based intrusion detection framework that integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for effective DDoS detection in IoMT networks. The CNN component is used to extract distinctive spatial features from network traffic data, while the LSTM component models the temporal dependencies associated with sequential attack behaviours. The proposed framework was evaluated using the publicly available CICIoMT2024 dataset, which contains realistic IoMT traffic scenarios comprising over two million network records. To ensure controlled experimentation and computational feasibility, a stratified subset of 100,000 samples was selected for training and testing. The experimental results reveal that the proposed CNN–LSTM model reaches a detection accuracy of 99.60% and an F1-score of 99.61%, with a false positive rate of 2.06% and a false negative rate of 0.38%. A comparative assessment with standalone CNN and LSTM baseline models substantiates the effectiveness of integrating spatial–temporal features in bolstering detection reliability. Although the false positive rate is a concern in high-volume healthcare environments, the overall outcomes indicate that the proposed hybrid framework delivers a scalable, reliable, and effective solution for enhancing IoMT cybersecurity against DDoS threats.

* *Corresponding author.*
E-mail address: azuan@usim.edu.my

https://doi.org/10.37934/arsbs.42.1.310318

1. Introduction

The Internet of Things (IoT) has greatly revolutionized the healthcare field by allowing for effective transfer, storage, and real-time processing of medical information. The IoMT, a specific extension of IoT, merges medical sensors, wearable devices, and healthcare infrastructures to facilitate ongoing patient monitoring and enhance clinical decision-making. According to Allied Market Research (2023), the global IoMT market is expected to reach approximately USD 332.67 billion by 2027, showcasing rapid integration within healthcare systems. However, the increasing reliance on interconnected medical devices also brings forth serious challenges concerning data privacy, system availability, and cybersecurity vulnerabilities [1]. Malicious software and network-based attacks signify increasingly intricate threats to IoMT environments [2]. Among these threats, Distributed Denial of Service (DDoS) attacks represent a particularly severe risk. DDoS attacks exploit weaknesses in IoT and IoMT devices by compromising them and launching large-scale flooding attacks that overwhelm network infrastructures [3]. Such attacks can disrupt critical healthcare services, impair system performance, and compromise sensitive patient data, potentially endangering patient safety and operational reliability [4]. Recent threat intelligence reports also indicate that large-scale DDoS campaigns have targeted IoT and operational technology infrastructures, emphasizing the expanding and evolving threat landscape [5].

Conventional security mechanisms, including rule-based and signature-based IDS, encounter notable limitations in recognizing modern DDoS attacks. These traditional strategies depend on predefined patterns and static rules, which hinder their ability to adapt to evolving and previously unseen attack behaviors. Furthermore, the rapid expansion of IoMT devices generates substantial volumes of diverse network traffic, presenting scalability challenges for conventional detection systems. Thus, there is a necessity for more adaptive and intelligent detection frameworks to effectively address the dynamic and high-dimensional nature of IoMT network traffic.

Despite recent advancements in deep learning-based intrusion detection, many current studies emphasize general IoT environments rather than the specific traffic characteristics associated with IoMT. Additionally, standalone machine learning and deep learning models often do not adequately capture both spatial and temporal dependencies that are inherent in the evolving patterns of DDoS attacks. There is limited research that has explored hybrid spatial-temporal architectures using recent healthcare-oriented datasets such as CICIoMT2024. Moreover, operational considerations, including the impact of false positives in critical healthcare environments, remain insufficiently discussed.

To address these deficiencies, this study aims to design and evaluate a hybrid deep learning-based intrusion detection framework that integrates CNN and LSTM networks for DDoS detection in IoMT networks. The proposed architecture employs CNN layers for effective spatial feature extraction and LSTM layers for modeling temporal dependencies in network traffic sequences. By merging spatial-temporal learning with evaluation on a recent IoMT-specific dataset, this research contributes to enhancing detection reliability while critically analyzing performance implications in healthcare-oriented deployment scenarios.

2. Literature review

2.1 Wireless IoMT Network Technology

Wireless network technology forms the basis of the IoMT by allowing seamless interaction among medical sensors, wearable devices, and healthcare infrastructures. By employing wireless protocols such as Wi-Fi, Bluetooth, and cellular networks, IoMT systems facilitate real-time patient monitoring,

remote diagnostics, and continuous data transfer without the need for physical connections [6]. Nonetheless, the dependence on wireless connectivity considerably broadens the attack surface of IoMT environments. Unlike standard wired medical systems, IoMT devices frequently operate with limited processing power and minimal built-in security measures, which makes them more exposed to network-based cyber threats. Thus, safeguarding wireless IoMT communication has become an essential focus of research.

2.2 DDoS Attacks in IoMT Environments

Distributed Denial of Service (DDoS) attacks are among the most critical threats to Internet of Medical Things (IoMT) infrastructures. The heterogeneous and resource-constrained nature of IoMT devices makes them particularly appealing targets for botnet recruitment. Attackers exploit inadequate authentication mechanisms and unpatched vulnerabilities to compromise these devices, resulting in the generation of large-scale malicious traffic [7]. In the context of healthcare, DDoS attacks can disrupt essential services, delay the transmission of medical data, and interfere with emergency response systems. A number of studies have explored DDoS detection in IoT networks; however, many of them focus on generic IoT datasets rather than on traffic patterns that are specific to IoMT. García *et al*., [5] conducted early empirical comparisons of various botnet detection methods, highlighting the challenges associated with detecting evolving attack behaviors. Recent studies have employed machine learning techniques such as Random Forest, Support Vector Machines, and Artificial Neural Networks for intrusion detection in IoT environments. While these approaches yield promising results, they often rely on handcrafted features and encounter difficulties in modeling temporal dependencies.

2.3 Deep Learning-Based Intrusion Detection

Deep learning has emerged as a crucial method for detecting network intrusions, primarily due to its ability to automatically learn hierarchical feature representations from extensive and high-dimensional traffic data. In contrast to conventional machine learning techniques that rely heavily on manual feature engineering, deep learning models are capable of directly extracting intricate patterns from either raw or preprocessed network traffic.

CNNs are frequently utilized in intrusion detection systems to identify spatial correlations among traffic features. Through the application of convolutional filters, CNNs can acquire discriminative feature representations that improve classification accuracy in tasks related to attack detection. However, CNN-based models are predominantly effective for recognizing static patterns and may not adequately capture the temporal dependencies inherent in sequential network traffic data.

To address these limitations, hybrid CNN–LSTM architectures have been proposed to concurrently model both the spatial and temporal characteristics of network traffic. By combining convolutional layers for feature extraction with LSTM layers for sequential modeling, these hybrid approaches have demonstrated improved performance in detecting complex and evolving cyberattacks. Nonetheless, many existing studies evaluate these architectures using general IoT datasets rather than focusing on healthcare-specific IoMT traffic, and there has been a lack of attention to operational implications, such as the effects of false positives in medical environments. These shortcomings highlight the need for further investigation into hybrid deep learning models within IoMT-focused intrusion detection frameworks.

2.4 Research Gap

Considering the significant strides made in deep learning-based intrusion detection, various limitations still exist in the current research landscape. Firstly, a considerable number of prior studies have concentrated on general IoT traffic, overlooking the specific network characteristics associated with the IoMT that reflect the communication patterns prevalent in healthcare. Secondly, while hybrid CNN–LSTM architectures have demonstrated notable detection performance, there is a lack of research that evaluates these models using up-to-date healthcare-focused datasets such as CICIoMT2024. Thirdly, operational aspects—including the consequences of false positives in healthcare-critical environments—are often inadequately analyzed. Furthermore, challenges related to dataset representativeness, scalability, and deployment feasibility are seldom discussed in depth.

As a result, there is a pressing need for a hybrid spatial–temporal intrusion detection framework that is specifically tailored to IoMT environments and assessed using realistic healthcare traffic scenarios. This study seeks to address these deficiencies by designing and evaluating a CNN–LSTM-based DDoS detection model with the CICIoMT2024 dataset, while also critically examining its detection performance within healthcare-oriented contexts.

3. Methodology

3.1 Dataset Description and Sampling strategy

This research employs the publicly accessible CICIoMT2024 dataset [9], which encompasses authentic Internet of Medical Things (IoMT) network traffic obtained from medical and IoT communication settings. The dataset comprises both benign traffic and various Distributed Denial of Service (DDoS) attack scenarios created using prevalent IoMT communication protocols. The initial dataset contains over two million traffic records stored in packet capture (PCAP) format, which were subsequently transformed into structured CSV files for machine learning analysis.

Despite the complete dataset containing more than two million instances, a stratified subset of 100,000 samples was chosen for controlled experimentation and computational efficiency. Stratified sampling was utilized to maintain the original class distribution before any balancing procedures were applied. To guarantee equitable training, the dataset was balanced by ensuring equal proportions of benign and malicious samples.

The dataset was partitioned into training and testing sets through an 80:20 stratified random split. A fixed random seed was used to ensure the reproducibility of the experimental outcomes.

3.2 Data Preprocessing

Before the model training commenced, all features underwent conversion into a numerical format. Categorical attributes were encoded correctly, and non-numeric values were altered to ensure they were compatible with deep learning models. Missing and infinite values were replaced with zero to mitigate numerical instability during the training phase.

Feature scaling was carried out using standard normalization to guarantee a consistent distribution of features and stable convergence of the neural network. Extremely large values were clipped to prevent gradient explosion during the optimization process. The preprocessed feature vectors were reshaped to satisfy the input requirements of the convolutional neural network layers.

3.3 Hybrid CNN-LSTM Architecture

The proposed framework merges CNN with LSTM networks to effectively capture both spatial and temporal features of IoMT network traffic.

The CNN part consists of one-dimensional convolutional layers, followed by Rectified Linear Unit (ReLU) activation functions and max-pooling operations. These layers are tasked with extracting high-level spatial features from network flow data, which include traffic intensity patterns and protocol-related characteristics.

The feature maps that are extracted are subsequently input into a bidirectional LSTM layer to model the temporal dependencies that are inherent in sequential traffic data. The LSTM component is capable of capturing long-term correlations and evolving patterns associated with DDoS attacks, which may not be evident through spatial feature extraction alone.

After the sequential modeling, a global max pooling operation is performed to reduce dimensionality while retaining the most informative temporal features. The resulting feature representation is then passed to fully connected (dense) layers for classification. A sigmoid activation function is utilized in the output layer to execute binary classification between benign and malicious traffic.

The overall workflow of the proposed framework, which encompasses preprocessing, feature extraction, temporal modeling, and classification stages, is illustrated in Fig. 1.

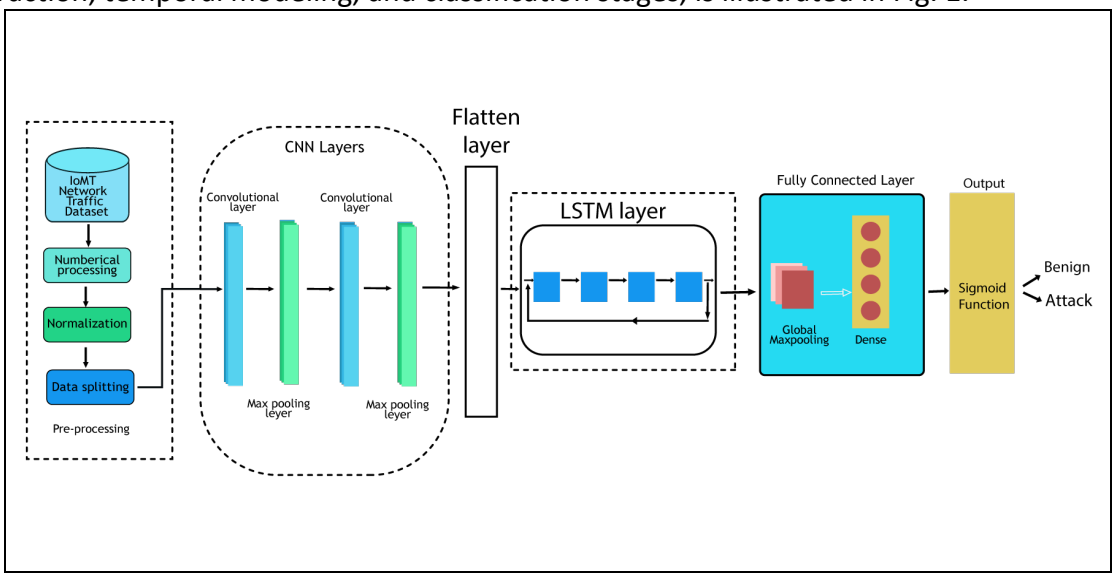

Fig. 1 Proposed hybrid CNN–LSTM architecture for DDoS detection in IoMT networks.

3.4 Model Training and Hyperparameter Configuration

The proposed CNN–LSTM architecture was executed using the PyTorch deep learning framework. The model underwent optimization through the Adam optimizer, which was configured with a learning rate of 0.01, and cross-entropy loss was utilized as the objective function for binary classification.

The training process spanned 10 epochs with a batch size of 32. To address overfitting and enhance generalization capabilities, dropout regularization was incorporated. Model parameters were initialized randomly, and a fixed random seed was applied to maintain experimental reproducibility.

All experiments were carried out on a workstation that included an Intel Core i5-10500H processor (2.50 GHz, 6 cores, 12 threads), 16 GB of RAM, and an NVIDIA GeForce RTX 3050 GPU

running Windows 11 Pro. This computational configuration facilitates reproducibility and provides ample resources for the training and assessment of the proposed deep learning framework.

3.5 Evaluation Metrics

Model performance was assessed using conventional classification metrics, such as accuracy, precision, recall, F1-score, and confusion matrix analysis. Additionally, the False Positive Rate (FPR) and False Negative Rate (FNR) were calculated to evaluate operational reliability in healthcare-oriented IoMT settings.

In healthcare scenarios, it is vital to reduce false positives to prevent unnecessary alerts that could disrupt clinical workflows, while also minimizing false negatives to ensure that harmful traffic is not misidentified as benign. Thus, both FPR and FNR were analyzed comprehensively to assess the practical applicability of the proposed detection framework.

4. Results and Discussion

4.1 Training Performance Analysis

The training performance assessment of the proposed hybrid CNN–LSTM model was carried out over ten epochs. Fig. 2 illustrates the changes in training accuracy and F1-score throughout these epochs. The results indicate a steady and consistent improvement in both metrics during the training process, reflecting effective learning and stable convergence.

By the end of the final epochs, the model attained a detection accuracy of 99.60% and an F1-score of 99.61%, highlighting the effectiveness of the hybrid spatial–temporal learning strategy. The smooth learning curves shown in Figure 3 indicate that the model avoids both underfitting and overfitting, thereby confirming the robustness of the training process when applied to IoMT network traffic.

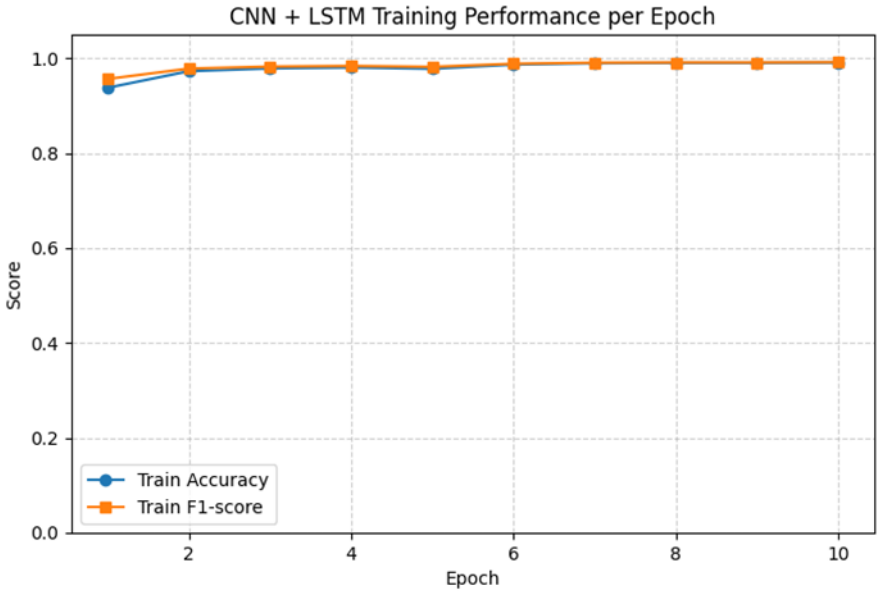

Fig. 2 Training accuracy and F1-score of the proposed CNN–LSTM model across epochs

4.2 Test Performance Evaluation

The trained model was subjected to evaluation utilizing a balanced dataset that included 100,000 samples of IoMT network traffic, encompassing both benign and DDoS traffic. The evaluation results indicate a significant ability to generalize when the model is applied to data it has not encountered before.

The model achieved a detection accuracy of 99.60% and an F1-score of 99.61%, underscoring its capability to effectively differentiate between normal and malicious traffic in IoMT contexts. These results demonstrate that the proposed CNN–LSTM model retains high detection performance even in the face of diverse DDoS attack scenarios.

4.3 Per-Class Performance and Confusion Matrix Analysis

Fig. 3 displays the confusion matrix associated with the proposed model. The majority of benign and malicious samples were accurately classified, with only a few misclassifications detected.

The model achieved a false positive rate (FPR) of 2.06% and a false negative rate (FNR) of 0.38%. The low FNR reflects a strong proficiency in identifying DDoS attacks without misclassifying harmful traffic as benign. However, despite the FPR being relatively minor, in large healthcare environments, a 2.06% false alarm rate could still result in a significant number of alerts. Therefore, it may be necessary to consider threshold tuning or filtering mechanisms at the deployment level to further alleviate operational challenges.

The weighted F1-score of 0.9959 reinforces the notion of balanced classification performance across both classes. These results indicate that the hybrid spatial–temporal architecture effectively captures the complex traffic patterns associated with DDoS attacks.

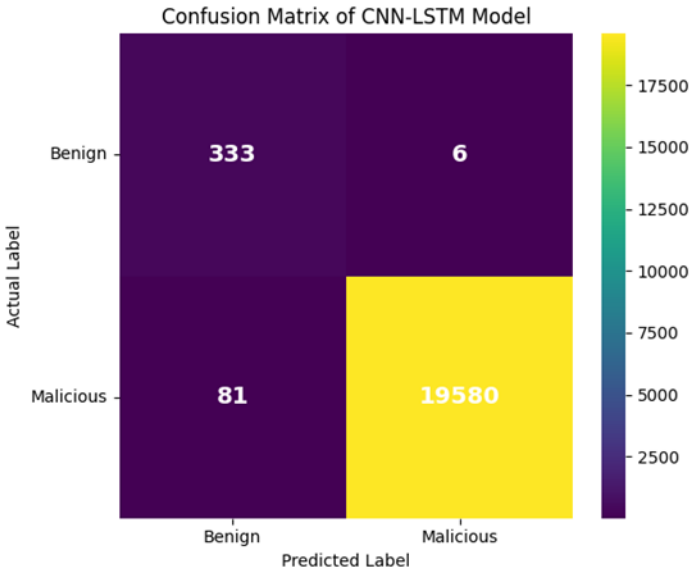

Fig. 3 Confusion matrix of the proposed CNN–LSTM model for DDoS detection in IoMT networks

4.4 Comparative Discussion

In comparison to independent CNN and LSTM models assessed under the same preprocessing and training conditions, the hybrid CNN–LSTM framework exhibits enhanced detection stability and

a decrease in false negatives. The CNN segment captures spatial correlations among network features, whereas the LSTM segment addresses the temporal dependencies present in the changing attack traffic. This synergistic learning approach facilitates a more resilient detection capability than that of single-architecture models.

4.5 Discussion

The experimental results substantiate that the integration of spatial and temporal feature learning significantly bolsters the reliability of DDoS detection within IoMT environments. The hybrid architecture proficiently captures high-dimensional traffic characteristics while preserving strong generalization performance.

Nonetheless, certain limitations are evident. The evaluation was carried out on a single dataset without cross-dataset validation, and the latency associated with real-time deployment was not measured experimentally. Additionally, while the performance metrics are promising, further exploration into scalability under high-throughput healthcare traffic conditions is essential.

Overall, the results imply that the proposed CNN–LSTM framework presents a reliable and effective method for enhancing IoMT cybersecurity against DDoS attacks while maintaining satisfactory operational performance.

5. Conclusions

This research proposed a hybrid deep learning-based intrusion detection framework that integrates CNN and LSTM networks for the detection of DDoS attacks in IoMT environments. The architecture was designed to address the limitations of traditional intrusion detection systems and standalone deep learning models by jointly capturing the spatial and temporal characteristics of network traffic.

The experimental evaluation using the CICIoMT2024 dataset showed that the hybrid CNN-LSTM model achieved a high detection accuracy of 99.60% and an F1-score of 99.61%, with low rates of false positives and false negatives. These results indicate that the integration of spatial-temporal feature learning enhances the reliability of detection in IoMT traffic scenarios.

Despite these promising results, several limitations exist. The model was evaluated on a single dataset without cross-dataset validation, and the feasibility of real-time deployment was not experimentally assessed. Additionally, scalability in high-throughput healthcare environments and robustness against adversarial manipulation were not explored in this study.

Future research will focus on evaluating the framework across multiple IoMT datasets, conducting cross-validation experiments, analyzing real-time deployment latency, and exploring adaptive learning mechanisms to address evolving attack patterns. Such investigations will further enhance the practical applicability of hybrid deep learning approaches for securing healthcare-oriented IoMT networks.

Acknowledgement

This research was supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme (FRGS), grant number FRGS/1/2022/ICT07/USIM/02/1.

References

[1] Tripathi, Shivam, Vatsalkumar Makwana, Malaram Kumhar, Harshal Trivedi, Jitendra Bhatia, Sudeep Tanwar, and Hossein Shahinzadeh. "IoMT-enabled smart healthcare: state-of-the-art, security and future directions." In *2023*

14th International Conference on Information and Knowledge Technology (IKT), pp. 36-43. IEEE, 2023. https://doi.org/10.1109/IKT62039.2023.10433013

[2] "Internet of Medical Things Market | IoMT Industry Statistics, Segments Analysis | Forecast - 2027." Accessed: Jan. 08, 2026. [Online]. Available: https://www.alliedmarketresearch.com/internet-of-medical-things-market-A07917?utm_source=chatgpt.com

[3] Ahmim, Ahmed, Faiz Maazouzi, Marwa Ahmim, Sarra Namane, and Imed Ben Dhaou. "Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model." *IEEE Access* 11 (2023): 119862-119875. https://doi.org/10.1109/ACCESS.2023.3327620

[4] Rani, SV Jansi, Iacovos Ioannou, Prabagarane Nagaradjane, Christophoros Christophorou, Vasos Vassiliou, Sai Charan, Sai Prakash, Niel Parekh, and Andreas Pitsillides. "Detection of DDoS attacks in D2D communications using machine learning approach." *Computer Communications* 198 (2023): 32-51. https://doi.org/10.1016/J.COMCOM.2022.11.013

[5] Garcia, Sebastian, Martin Grill, Jan Stiborek, and Alejandro Zunino. "An empirical comparison of botnet detection methods." *computers & security* 45 (2014): 100-123. https://doi.org/10.1016/J.COSE.2014.05.011

[6] "GrAPL 2021 Keynote 1: Sparse Adjacency Matrices at the Core of Graph Databases: GraphBLAS the Engine Behind RedisGraph Property Graph Database," pp. 240–241, Jun. 2021, https://doi.org/10.1109/IPDPSW52791.2021.00044

[7] Mnasri, Zied, Stefano Rovetta, and Francesco Masulli. "A novel pitch detection algorithm based on instantaneous frequency." In *2021 29th European Signal Processing Conference (EUSIPCO)*, pp. 16-20. IEEE, 2021. https://doi.org/10.23919/EUSIPCO54536.2021.9616047

[8] Sharafaldin, Iman, Arash Habibi Lashkari, and Ali A. Ghorbani. "Toward generating a new intrusion detection dataset and intrusion traffic characterization." *ICISSp* 1, no. 2018 (2018): 108-116. https://doi.org/10.5220/0006639801080116

[9] Canadian Institute for Cybersecurity, "CICIoMT2024: A Realistic Internet of Medical Things Dataset for Intrusion Detection."

[10] Aydın, Hakan, Zeynep Orman, and Muhammed Ali Aydın. "A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment." *Computers & Security* 118 (2022): 102725. https://doi.org/10.1016/J.COSE.2022.102725

[11] Y. Liu, C. Zhang, and X. Wang, "Deep learning-based intrusion detection for IoT networks: A survey," IEEE Access, vol. 9, pp. 118977–118999, 2021, https://doi.org/10.1109/ACCESS.2021.3107895

[12] M. H. ur Rehman, M. Yaqoob, and A. Ahmed, "Machine learning and deep learning methods for intrusion detection systems in IoT: A survey," IEEE Access, vol. 9, pp. 118987–119010, 2021, https://doi.org/10.1109/ACCESS.2021.3107901

[13] S. Latif, S. Ahmed, M. A. Awais, and J. Qadir, "A comprehensive survey of deep learning techniques for cyber security," IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1431–1470, 2022, https://doi.org/10.1109/COMST.2022.3147915

[14] F. Ullah and M. A. Mahmood, "CNN-based intrusion detection system for IoT networks," Computers & Security, vol. 112, p. 102506, Jan. 2022, https://doi.org/10.1016/j.cose.2021.102506

[15] J. Kim, H. Kim, and H. Kim, "Hybrid deep learning-based DDoS detection model using CNN and LSTM," IEEE Access, vol. 9, pp. 101699–101709, 2021, https://doi.org/10.1109/ACCESS.2021.3097775

[16] Javaid, Ahmad, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. "A deep learning approach for network intrusion detection system." *Eai Endorsed Transactions on Security and Safety* 3, no. 9 (2016): 21. https://doi.org/10.4108/eai.25-5-2021.170310

[17] Ferrag, Mohamed Amine, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." *Journal of Information Security and Applications* 50 (2020): 102419. https://doi.org/10.1016/j.jisa.2020.102642

[18] S. Verma and A. K. Singh, "An efficient deep learning-based intrusion detection system for IoT networks," Computer Communications, vol. 190, pp. 32–44, 2022, https://doi.org/10.1016/j.comcom.2022.04.012

[19] R. Alrashdi and M. Alharthi, "DDoS attack detection in IoT networks using hybrid deep learning techniques," IEEE Access, vol. 10, pp. 45012–45025, 2022, https://doi.org/10.1109/ACCESS.2022.3168200

[20] H. Hindy et al., "A taxonomy of network threats and intrusion detection systems in IoT," IEEE Access, vol. 8, pp. 19037–19052, 2020, https://doi.org/10.1109/ACCESS.2020.2968989

[21] M. T. Alshammari and A. N. Zincir-Heywood, "Machine learning-based DDoS detection for IoT networks," IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 58–72, 2022, https://doi.org/10.1109/TNSM.2021.3123456

[22] K. R. Choo, "The cyber threat landscape: Challenges and future research directions," Computers & Security, vol. 125, p. 103037, 2023, https://doi.org/10.1016/j.cose.2023.103037