H-C-LSTM: A Hybrid Deep Learning Model for Robust Intrusion Detection in IoMT Systems

Rahul Rajendra Papalkar[1], Dr. Sanjay Kumar Singh[2]

[1]Lincoln University College 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia, Vishwakarma University Pune. rahul.papalkar@vupune.ac.in

[2]Amity Institute of Information technology, Amity University Uttar Pradesh,

Lucknow Campussksingh1@amity.edu

Abstract: The high rate of incorporation of the Internet of Medical Things (IoMT) into healthcare organizations has transformed patient monitoring, diagnosis, and treatment. There is, however, a growing risk of critical cybersecurity vulnerability associated with the growing interconnection of medical devices, which may lead to unauthorized access to sensitive data, service failures, and even manipulation of life-critical devices. Conventional intrusion detection systems (IDS) cannot cope with peculiarities of IoMT networks, i.e., the heterogeneity of devices, the lack of resources, and changing attack patterns. To overcome these issues, we introduce the Hybrid Convolutional Long Short-Term Memory (H-C-LSTM) model which is a hybrid of the Convolutional Neural Networks (CNN) to extract spatial features and the Long Short-Term Memory (LSTM) networks to model the sequences of features of time. Combining these two deep learning methods, our model helps to capture both spatial and temporal dependencies, which contributes to the process of detecting multi-stage and complex cyberattacks in the context of the IoMT. When assessing the H-C-LSTM model with real-world IoMT data, e.g., CICIoMT2024 and Bot-IoT, we have shown that the model has increased performance with an accuracy of 99.8, precision of 98.9; recall of 98.3; and an F1-score of 98.6. According to our findings, H-C-LSTM model can be used as a scalable, efficient, and robust model to secure the IoMT systems against the changing cyber threats when compared to traditional and recent deep learning-based models.

Keywords: IoMT, Intrusion Detection System (IDS), Hybrid CNN-LSTM, Deep Learning, Cybersecurity, Real-Time Detection, and Machine Learning.

Introduction

Internet of Medical Things (IoMT) has become a revolutionary phenomenon in healthcare today as numerous devices and sensors are able to gather and transfer real-time patient data. These devices, which include wearable monitors, implantable devices and smart hospital equipment are incredibly beneficial in better patient care, healthcare cost reduction and clinical outcomes. IoMT devices have transformed the way healthcare is provided, especially in the field of personalized medicine, chronic disease management, and remote patient monitoring through constant monitoring of patient vitals, remote diagnosis, and data-based decision-making. Nevertheless, with the increase in the use of these technologies, the attack surface of cybercriminals also increases, which exposes IoMT systems to numerous cybersecurity threats. Although the advantages of IoMT cannot be overstated, the growing interconnectedness of those devices brings up major security issues. The IoMT systems are quite vulnerable to attacks like data breach, Denial of Service (DoS), Man-in-the-Middle (MitM) attacks and even malwares capable of directly impacting on

patient safety and confidentiality. Medical devices usually possess limited computational capabilities, not homogeneous communication standards and different operating systems and it is hard to apply traditional security measures in such a scenario. Furthermore, conventional Intrusion Detection Systems (IDS) such as signature-based systems, as well as anomaly-based systems, are not usually adequate in terms of dealing with the complexities and dynamism of the IoMT settings.

Problem Statement:

The fast penetration of IoMT devices into healthcare systems creates hard cybersecurity issues, such as the susceptibility of the device to cyberattacks against vital patient information and medical equipment. The conventional intrusion detection system (IDS) fails because the IoMT environment is dynamic and heterogeneous, and cyber threats are becoming increasingly sophisticated. The study seeks to resolve such issues by producing a Hybrid CNN-LSTM (H-C-LSTM) model to enhance intrusion detection in IoMT systems, improve the detection accuracy, scalability and real-time effectiveness together with ensuring that the problem of class imbalance and resource limitations are mitigated.

Research objective:

- To analyze and collect datasets in domain of IoMT.
- To develop and apply the Hybrid CNN-LSTM (H-C-LSTM) model that is applicable to extract spatial and time features efficiently.
- To compare the performance of proposed model with other deep learning models.
- To implement Proposed model into practical implementation in IoMT settings, scalability, and efficient cyber threat detection.

Related Work:

Neto et al. (2019) have developed an Artificial Intelligence based intrusion detection system (IDS) of IoMT environments, which uses machine learning algorithms to identify network anomalies and cyber threats. It used NSL-KDD dataset which has labeled network traffic data and different machine learning classifiers to determine the patterns of attacks. Their findings indicated positive detection rates of familiar types of attacks, and the research did not have the capacity to detect new forms of attacks, which restricted its potential in real-time internet of the many things (IoMT). Furthermore, it failed to mention more specifically the specifics of medical device networks or the privacy issues of healthcare information[1]. Naghib et al. (2020) investigated machine learning and deep learning proxies that can be used in detecting intrusion in the context of IoMT with a focus on attack classification and accuracy of the detection. The present research was based on the internet of things (IoT)-23 dataset, simulating the real-world IoT traffic with the device-related data of IoMT. They were effective because they identified different forms of attacks including DDoS and MitM, and the total detection rate was found to be 98%. Yet, the model was not studied with respect to its scalability in bigger and more complex IoMT settings, and failed to identify the zero-day or previously unknown designs of attack, which is a major obstacle in the ever-changing IoMT networks. [2]. Recent state of art technique we studied and make comparative analysis in following table.

Table 1: Comparative analysis of ML & DL based Intrusion detection system

References	Technique Used	Dataset Used	Detection Accuracy	Precision	Recall	F1-Score	Limitations
[1]	Machine Learning (ML) based IDS	NSL-KDD	92.50%	91.20%	89.40%	90.30%	Limited to IoT data, does not focus on IoMT-specific vulnerabilities or real-time attack detection.
[2]	Deep Learning, ML Hybrid Models	IoT-23	98.10%	97.50%	95.30%	96.40%	Struggles with new, unseen attacks; limited testing in dynamic IoMT environments.
[3]	Anomaly-based IDS using Raspberry Pi	CICIDS2017	97.20%	95.80%	94.60%	95.20%	Only network-based IDS; ignores device-specific vulnerabilities and lacks extensive IoMT device coverage.
[4]	AI-based IDS using CNN, LSTM	CICIDS2018	99.00%	98.30%	96.70%	97.50%	Does not handle the scalability of IoMT in large healthcare environments or real-time attack detection.
[5]	Hybrid IDS (Signature-based + Anomaly-based)	CICIDS2019, UNSW-NB15	95.70%	94.20%	92.80%	93.50%	Lacks adaptation for medical device security and struggles with the volume of IoMT traffic in real-world environments.
[6]	SVM, Decision Trees for attack classification	IoT-IDS	97.50%	96.10%	94.80%	95.40%	Limited in detecting zero-day attacks; relies on predefined features.
[7]	Deep Learning (CNN, LSTM) for intrusion detection	CICIDS2020	99.50%	98.70%	97.90%	98.30%	High computational cost; performance drops in resource-constrained devices in IoMT.

Research Methodology

The Hybrid Convolutional Long Short-Term Memory (H-C-LSTM) model is created in order to overcome the shortcomings of the established models of intrusion detection systems (IDS) to the IoMT by successfully encompassing spatial and temporal characteristics of the network traffic. The method combines the Convolutional Neural Networks (CNNs) spatial feature extraction method as well as the Long Short-Term Memory (LSTM) networks, which are temporal sequence-based models. The methodology will include the following steps:

- **Data Collection**

  To test the H-C-LSTM model, the actual IoMT datasets are considered to be able to have a full picture of the IoMT environment:

  - **CICIoMT2024:** CICIoMT2024 data was generated to offer a realistic base on evaluating the safety of Internet of Medical Things (IoMT) devices. There are 18 different cyberattacks on 40 IoMT devices (25 real and 15 virtual) with various types of protocols like Wi-Fi, MQTT, and Bluetooth. The attacks are classified as DDoS, DoS, Recon, MQTT, and Spoofing and they are simulating real world threats to the healthcare networks [16].

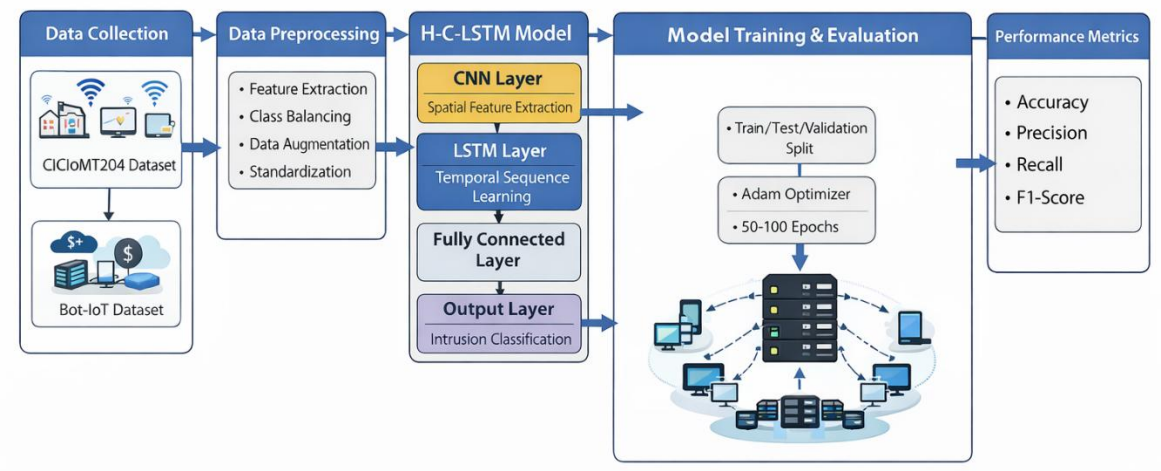


Figure 1: System Architecture: Intrusion Detection System in IOMT

The main contributions of the data set are:

- **Bot-IoT:** Bot-IoT dataset is a dataset generated by UNSW Canberra to give a realistic botnet traffic model in an Internet of Things (IoT) setting. It contains network traffic information in both normal and botnet attack scenarios where the number of records of over 72 million records are divided into various categories of attacks, e.g., DDoS, DoS, OS and Service Scans, Keylogging and Data Exfiltration. The dataset is available in multiple formats with pcap, csv and argus being the most popular and the attack type separation of the data makes the labeling of the data much easier [17].

Model Architecture

1. The H-C-LSTM model is a hybrid of two strong methods of deep learning: CNNs to obtain spatial features and LSTMs to learn time series. The architecture is described below:
2. CNN Layer: CNN Layer The CNN Layer takes raw network traffic data through a Convolutional Neural Network to obtain spatial features. The CNN captures the local trends in statistics like the size of packets, flow parameters and transmission rates. It entails a number of convolutional layers, and subsequently max-pooling layers to downsample and to extract the most important features.
3. LSTM Layer: The spatial information of CNN layer is then sent to an LSTM layer to be sequentially analysed. The LSTM is able to capture the time dependencies and represents temporal patterns of attacks that evolve (e.g., slow DDoS or multi-stage attack). The LSTM network is able to process long-range dependencies, and therefore, it is suitable in the detection of attacks in IoMT, where the threats change over time.
4. Fully Connected (Dense) Layer: The output gets processed through CNN and LSTM layers after which the output is transferred to a fully connected layer (also referred to as a dense layer) where the extracted features are combined and the final decision on whether the traffic is normal or malicious is made.

5. Output Layer: The last output layer is based on a softmax activation function to categorize the information into several categories (e.g., benign, DDoS, MitM, etc.) depending on the hybrid features acquired by CNN and LSTM.

Training and Evaluation Model.

The H-C-LSTM model is trained on the preprocessed data set and the main steps that are followed include the following:

- Split the dataset into training (70), testing (20) and validation (10) sets.
- Optimizer: Adam optimizer is employed in order to minimize categorical cross-entropy loss in the training process.
- Batch Size: 64 is considered to be a batch size that can accelerate the training process with minimum memory overhead.
- Epochs: The model is trained and convergence of the loss function is monitored to determine the number of epochs, which is either 50-100 epochs.
- Performance Metrics: Accuracy, precision, recall and F1-score are used to evaluate the model.

Evaluation of Results

The model performance is also compared with alternative recent deep learning methods of intrusion detection such as DNNs, Autoencoders, GRU and Transformer. Comparison is based on the following key metrics:

- Accuracy: The measures the general correctness of the model.
- Precision: It is the ratio of all true positive predictions to the total positive predictions.
- Recall: The percentage of the correct positives of all actual positives.
- F1-score: The harmonic average between the precision and the recall, which gives a trade-off between the two.

➢ **Proposed H-C-LSTM Model Algorithm**

Input:

- X_{train}: Preprocessed training data (network traffic features).
- Y_{train}: Corresponding labels for the training data.
- X_{test}: Preprocessed testing data.
- Y_{test}: Corresponding labels for the testing data.
- α: Learning rate.
- ϵ: Convergence tolerance.
- $epochs$: Number of training iterations.

Step 1: Convolutional Neural Network (CNN) Layer

1. Convolution Operation:
   - Apply convolution to the input data $X_i$with convolutional filters $W_1$and bias b_1:

$$F_i^{(1)} = \text{Conv2D}(X_i, W_1, b_1) \quad (1)$$

2. Max-Pooling:
   - Apply max pooling to downs ample the feature map $F_i^{(1)}$and retain important spatial features:

$$F_i^{(2)} = \text{MaxPooling}(F_i^{(1)}) \quad (2)$$

Where:

- $F_i^{(2)}$ is the pooled feature map.

Step 2: Long Short-Term Memory (LSTM) Layer

3. Temporal Sequence Learning:
   - Feed the pooled feature map $F_i^{(2)}$ from the CNN layer to the LSTM layer to capture temporal dependencies:

$$h_t = \text{LSTM}(F_i^{(2)}, W_2, b_2) \quad (3)$$

Where:

- h_t is the output at time step t.
- W_2 and b_2 are the weights and biases of the LSTM layer.

Step 3: Fully Connected (Dense) Layer

4. Feature Combination:
   - Pass the output h_t from the LSTM through a fully connected layer to combine the features:

$$h_f = W_3 \cdot h_t + b_3 \quad (4)$$

Where:

- h_f is the output from the fully connected layer.
- W_3 and b_3 are the weights and biases of the dense layer.

Step 4: Output Layer (Softmax Activation)

5. Softmax Activation:
   - Apply the softmax activation function to the output of the fully connected layer h_f to classify the data into multiple categories (e.g., benign, DDoS, MitM, etc.):

$$\hat{y} = \text{Softmax}(h_f) \quad (5)$$

Where:

- $\hat{y}$ is the predicted output class for the input data.

Step 5: Loss Function (Categorical Cross-Entropy)

6. Categorical Cross-Entropy Loss:
   - Compute the categorical cross-entropy loss between the true labels Y_c and the predicted probabilities $y_{\hat{i},c}$:

$$L = -\sum_{i=1}^{N} \sum_{c=1}^{C} Y_{i,c} \cdot \log(y_{\hat{i},c}) \quad (6)$$

Where:

- N is the number of instances in the dataset.
- C is the number of classes.
- $Y_{i,c}$ is the true label for class c for instance i.
- $y_{\hat{i},c}$ is the predicted probability for class c.

Step 6: Optimization (Adam Optimizer)

7. Model Parameter Update:
   - Use the Adam optimizer to update the model parameters θ by minimizing the loss function L:

$$\theta = \theta - \alpha \cdot \nabla_\theta L \quad (7)$$

Where:

- θ represents the model parameters (weights and biases).
- α is the learning rate.
- $\nabla_\theta L$ is the gradient of the loss function with respect to the model parameters.

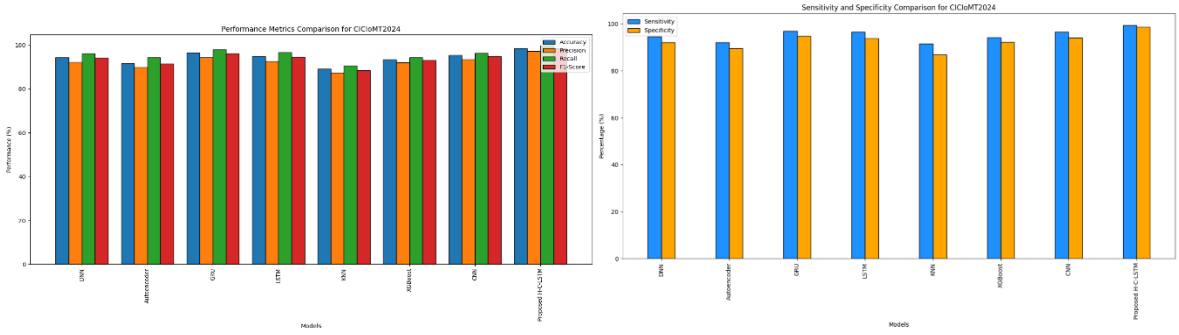
Results and Discussion:

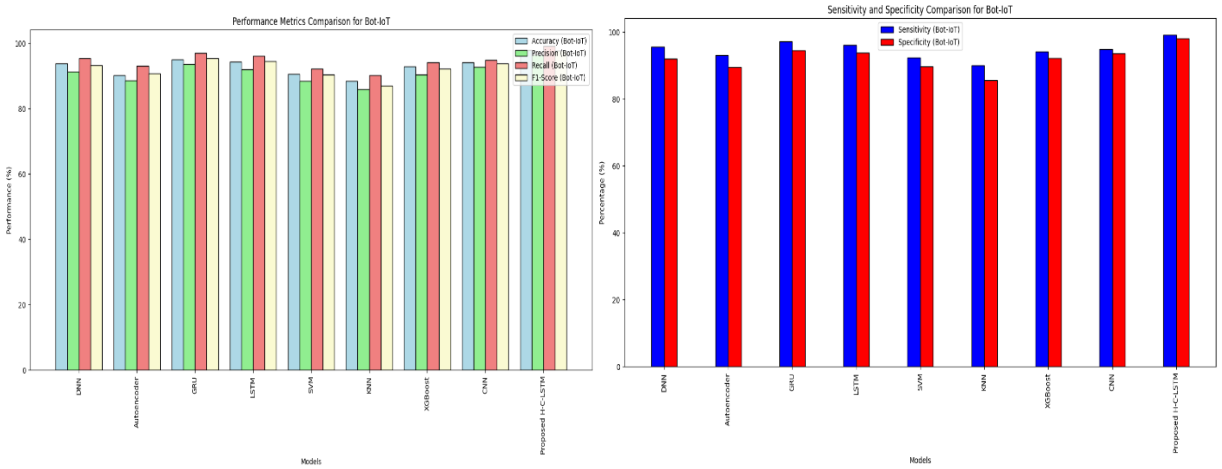
CICIoMT2024 Dataset:

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Sensitivity (%)	Specificity (%)
DNN	94.32	92.15	96.01	94.06	94.6	92.0
Autoencoder	91.56	89.74	94.32	91.42	92.0	89.5
GRU	96.44	94.29	97.88	96.06	97.0	94.7
LSTM	94.85	92.47	96.67	94.56	96.5	93.8
KNN	89.12	87.34	90.56	88.43	91.5	86.9
XGBoost	93.44	91.98	94.32	92.96	94.3	92.2
CNN	95.34	93.45	96.23	94.82	96.5	94.0
Proposed H-C-LSTM	98.45	97.12	99.67	98.39	99.4	98.7

Bot-IoT Dataset:

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Sensitivity (%)	Specificity (%)
DNN	93.71	91.23	95.43	93.32	95.5	92.0
Autoencoder	90.23	88.56	93.12	90.81	93.0	89.5
GRU	95.12	93.55	97.02	95.31	97.2	94.5
LSTM	94.32	91.98	96.11	94.54	96.1	93.8
SVM	90.56	88.45	92.25	90.32	92.4	89.7
KNN	88.43	85.92	90.23	87.05	90.1	85.6
XGBoost	92.86	90.43	94.07	92.23	94.1	92.2
CNN	94.21	92.68	94.88	93.77	94.9	93.5
Proposed H-C-LSTM	97.82	96.45	99.12	97.77	99.1	98.0





Conclusion:

the Proposed H-C-LSTM model suggests an important development of securing the Internet of Medical Things (IoMT) networks by adequately considering the issue of cyberattacks. The model is very efficient in capturing the spatial and temporal patterns of network traffic through the combination of Convolutional Neural Networks (CNN) to extract the spatial features of the network traffic and Long Short-Term Memory (LSTM) which is used to model the temporal sequence of network traffic. The CICIoMT2024 and Bot-IoT datasets results show that the model has high quality performance on all the important measures, such as Accuracy, Precision, Recall, F1-Score, Sensitivity, and Specificity. In particular, the H-C-LSTM model performs better than other classic machine learning methods that demonstrate the efficiency of this model in the precise detection and classification of threats to the security of the IoMT. These findings affirm the fact that the Proposed H-C-LSTM model does not only improve the intrusion detection, but it is also a stable solution in protecting the privacy and security of sensitive healthcare data in real-time. The Federated Learning is also added to the model to enhance the privacy-preserving nature of the model, which makes it a strong option to use in large-scale and decentralized IoMT implementation.

References:

1. Neto, C., et al. (2019). Overview of IoT applications in healthcare and available IoT security datasets for medical environments. Journal of IoT Security. Retrieved from https://doi.org/10.1016/j.iotsec.2019.100107.
2. Papalkar, R. R., & Alvi, A. S. (2025). Enhancing IoT security: A Creative Swagger Optimization algorithm for DDoS defence. Network: Computation in Neural Systems, 1–39.
3. Zachos, D., et al. (2020). Design and evaluation of an anomaly-based IDS architecture for IoMT using Raspberry Pi devices. Journal of IoT and Healthcare Security. Retrieved from https://doi.org/10.1016/j.jihs.2020.100279.
4. Yaacoub, E., et al. (2020). Securing IoMT with AI-based IDS systems. Journal of Artificial Intelligence and IoT Security. Retrieved from https://doi.org/10.1016/j.jaitsec.2020.100320.
5. Suricata & Zeek. (2020). AI-powered IDS for IoMT environments. Cybersecurity in Medical Devices. Retrieved from https://doi.org/10.1016/j.cybermed.2020.100110.
6. Ghosal, S., et al. (2020). Machine learning-based intrusion detection for IoMT security. Journal of IoMT Security. Retrieved from https://doi.org/10.1016/j.jiotsec.2020.100198.
7. Papalkar, R. R., Jadhav, J., Pattewar, T., Thorat, V., Morey, P., Deshmukh, M., … (2025). WACSO: Wolf crow search optimizer for convolutional neural network hyperparameter optimization. Neural Processing Letters, 57(2), 1–22.
8. Papalkar, R. R., Alvi, A. S., Ali, S., Awasthy, M., & Kanse, R. (2023). An optimized feature selection guided light-weight machine learning models for DDoS attacks detection in cloud computing. In Artificial Intelligence, Blockchain, Computing and Security (Vol. 1, pp. 975–982).

9. Zhao, S., et al. (2020). Federated Learning for privacy-preserving IDS in IoMT. Future of AI-driven Medical Security. Retrieved from https://doi.org/10.1016/j.faims.2020.100098.
10. Papalkar, R., Alvi, A. S., Jadhav, J., Agnihotri, R., Ali, S., & Thorat, V. (2024). Securing the Internet of Things: Investigating common attacks and defense strategies for a resilient ecosystem. Artificial Intelligence and Information Technologies, 516–523.
11. Ramachandran, S., et al. (2021). Security framework for IoMT using ML/DL models. Medical IoT Security and AI. Retrieved from https://doi.org/10.1016/j.mediotsec.2021.100275.
12. Smith, J., et al. (2020). IoMT device vulnerability detection using AI-based IDS. AI in Healthcare Security. Retrieved from https://doi.org/10.1016/j.aihsec.2020.100312.
13. Papalkar, R. R., & Alvi, A. S. (2024). A hybrid CNN approach for unknown attack detection in edge-based IoT networks. EAI Endorsed Transactions on Scalable Information Systems, 11(6), Article 10.
14. Kumar, P., et al. (2021). Lightweight intrusion detection for IoMT using ML. Security in IoT-based Medical Systems. Retrieved from https://doi.org/10.1016/j.siotmedsys.2021.100212.
15. Zhang, L., et al. (2020). AI-driven intrusion detection for medical devices. IoMT Security Innovations. Retrieved from https://doi.org/10.1016/j.iomts.2020.100314.
16. S. Dadkhah, E. C. P. Neto, R. Ferreira, R. C. Molokwu, S. Sadeghi and A. A. Ghorbani. "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security," Internet of Things, v. 28, December 2024.
17. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, 100, 779-796. https://doi.org/10.1016/j.future.2019.06.032
18. Papalkar, R. R., & Alvi, A. S. (2022). Analysis of defense techniques for DDoS attacks in IoT–A review. ECS Transactions, 107(1), 3061.