ISSN: 2182-2069 / E-ISSN: 2182-2077

A Novel Hybrid CNN-PCA Model to Improve Security in Chaotic IoT Environments

Marwan Kadhim Mohammed AL-Shammari[1*]

[1*]Computer Center, University of Baghdad, Baghdad, Iraq.
marwan.kazem@cc.uobaghdad.edu.iq, alkaseralshamary@gmail.com
https://orcid.org/0000-0002-4433-5086

Received: August 14, 2025; Revised: September 22, 2025; Accepted: October 30, 2025; Published: November 28, 2025

Abstract

Chaotic Internet of Things (IoT) has grown quickly in the digital world. With the emergence of IoT, many security obstacles have been appearing. The study suggests an efficient intrusion detection and protection strategy utilizing hybrid artificial intelligence (AI) methods to protect IoT networks from botnet/DDoS and IP/DNS spoofing attacks. In this study, the convolutional neural network (CNN) has been proposed to detect and prevent large-scale attacks as a first shield to protect network traffic from Distributed Denial of Services (DDoS) attacks, while principal component analysis (PCA) has been proposed to detect and protect the network from malicious attacks that come from IP/DNS spoofing attacks. The results exposed 98.36% detection to protect against intrusion in doorbell IoT devices, 98.62% detection to protect against intrusion in thermostat IoT devices, and 98.81% detection to protect against intrusion in security camera IoT devices, concerning accuracy benchmarks. The CNN-PCA hybrid model was efficacious in detecting malicious and botnet attacks for numerous IoT devices with optimal security. The study compares accuracy, precision, recall, and F1-core metrics with state-of-the-art security models.

Keywords: Botnets/DDoS Attacks, Chaotic Internet of Things, Convolutional Neural Network, Intrusion Detection and Protection Model, IP/DNS Spoofing Attacks, Principal Component Analysis.

1 Introduction

The chaotic IoT networks are always faced with attacks from outside. Artificial intelligence AI has appeared as a promised technology to prevent network attacks (Shafi et al., 2024). According to prior studies, some security models have been used as an effective technique to increase the speed of intrusion detection in networks (Al Lail et al., 2023). Some other studies anticipated a strategy to change the network traffic data into images and process these data to find DoS and DDoS based on the ResNet method (Aswad et al., 2023). A botnet attack found using a hybrid CNN-LSTM model for IoT networks has also been suggested with a real N-BaIoT dataset (Alkahtani & Aldhyani, 2021; Prabu & Sudhakar, 2023). Regarding the studies using hybrid deep learning (DL), some studies improved feature extraction by proposing CNN-BiLSTM for bidirectional training (Alghazzawi et al., 2021; Najafimehr et al., 2023). Some other research successfully detects and mitigates botnet attacks by considering binary multi-class classification on HetIoT devices and the convolutional layer in the CNN model (Mahadik et al., 2023;

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 4 (November), pp. 515-527.
DOI: *10.58346/JISIS.2025.I4.037*

*Corresponding author: Computer Center, University of Baghdad, Baghdad, Iraq.

Lavanya & Sekhar, 2024; Rezvani et al., 2025). Other studies proposed a hybrid scheme from Efficient Net, Xception, and Decision tree models to classify among 10 DDoS main attacks (Fayyadh & Kayabaş, 2023). Some other studies have developed a deep CNN ensemble paradigm to detect botnet attacks in software-defined networks (SDNs) (Mansoor et al., 2023). Some other studies used CNN and employed SDN, but the studies used CIC-IDS2017 and CIC-IDS2019 datasets (Hnamte & Hussain, 2023). Another study focused on DDoS attack detection utilizing the hybridization of CNN and LSTM (Issa & Albayrak, 2023; Chen et al., 2025). Also, DL returned as one of the solutions to detect severe IoT attacks, especially DoS and DDoS attacks on Bot-IoT networks (Manaa et al., 2024; Alsbatin et al., 2025). The researcher at Sannio University investigated detection and protection from botnet attacks in terms of IoT and internal networks, depending on the USB-IDS detection system (Kalutharage et al., 2023; Fayyadh & Kayabaş, 2023). An optimizer-equipped CNN-MLP is used by some researchers to detect DoS and DDoS attacks. This study used the CICDDoS-2019 dataset as a reference (Mehmood et al., 2025; Soy & Nayak, 2021). Some studies have numerous convolutional and pooling layers in the CNN-LSTM model that synergistically improve feature extraction of the CNN model (Nawaz et al., 2025; Nadim et al., 2024). Detection and mitigation of DDoS attacks in SDN networks have reappeared in some studies (Setitra et al., 2023). Some researchers used CNN-LSTM to successfully detect irregular abnormal traffic in the SDN environment (Alghazzawi et al., 2021).

Some studies compared the NGBoost algorithm with four AI algorithms (CNN, SGD, Random Forest, and decision tree) with the CICDDoD2019 dataset to show the significance of the algorithm Chanu et al., 2023). Some research papers proposed a hybrid DL from CNN and gated recurrent unit (GRU) to detect threats utilizing tabular-based image data (Dahiya, 2023). Some studies proposed a multi-case CNN with a BiLSTM arbitration dense network model to detect Low-rate DDoS attacks, which are more difficult to detect (Yin et al., 2024). Some other studies proposed DL-CNN to optimize automatic detection and classification dimensionality reduction, hyperparameter tuning, and feature extraction (Deshmukh & Ravulakollu, 2024). Some studies used the CNN-LSTM model to classify flooding, blackhole, TDMA, or Grayhole attacks (Dener et al., 2023).

Some studies identify abnormality in online and offline modes using the CNN model (Yaseen, 2023). Some research focused on detecting and mitigating the Mirai and DDoS attacks in IoT environments utilizing hybrid strawberry and African buffalo optimization (HSBABO) (Karthik & Krishnan, 2021). The contribution of this study is to provide an intelligent intrusion detection and protection model for a Chaotic IoT environment utilizing a CNN-PCA hybrid model. The proposed model is a hybrid model that synthesizes the CCN, which can detect the intrusion and protect the network from large-scale (botnet/DDoS) attacks as a first shield, with PCA, which can analyze the still traffic as a secondary filter for IP/DNS spoofing attacks. The remaining content of the study is prepared as follows (Nadim et al., 2024). Section 2 shows the preliminaries and related important information. Section 3 illustrates the results. Section 4 discusses the results and compares the proposed model with the state-of-the-art models. Finally, the conclusion section shows the summary of the study.

2 Preliminaries

PCA is a commonly used method to protect IoT networks from malicious attacks embedded in IP spoofing and DNS spoofing. Simultaneously, CCN is used to protect IoT networks from botnet/DDoS attacks that come from large volume traffic attacks in general, when attackers use a bot army to attack. The section presents the mathematical complexity and benchmark metrics of the suggested hybrid method.

2.1 Proposed Intrusion Detection Model

Figure 1 illustrates the model designed to protect devices in the Chaotic IoT network. The attacker represents the external intrusion in general. The attacks are classified into botnet attacks, which include but are not limited to TCP/UDP flood, DDoS, and Mirai ACK attacks, and malicious attacks like IP/DNS spoofing, which redirects traffic to malicious websites. Chaotic IoT devices represent all the Chaotic devices, for instance, doorbells, thermostats, and camera devices that are being protected by the proposed model. Update traffic represents the database that has been collected from the previous network traffic data. This traffic is periodically updated per network store session. The main target of the up-to-date traffic is to detect anomaly traffic and add to IoTID20 and TON_IoT datasets that are used in the proposed model to train CNN and CPA models, respectively. The CNN-CPA model receives data from the Internet and starts with an intrusion detection and protection procedure. The procedure starts with a check of the type of attack compared with the available previous traffic from the IoTID20 dataset and historical traffic from detecting anomalies. Depending on the study procedure, there are two main attacks. The first attack is represented by a botnet, or a bot attack; this type of attack acts as a denial of the services of servers, or what is called DDoS. Compared with the normal traffic, the model decides if the traffic is normal or anomalous. The second type of attack is represented by spoofing attacks, which are also detected by comparing the trusted resources in previous traffic and the TON_IoT dataset. Finally, the suggested model depicts a secure platform to protect the Chaotic IoT devices from various cyberattacks. In general, the CNN-PCA model acts as a twin defensive layer. This model processes incoming traffic, extracts the main network features, and detects cyberattack activities compared with available information in the two interactive datasets.

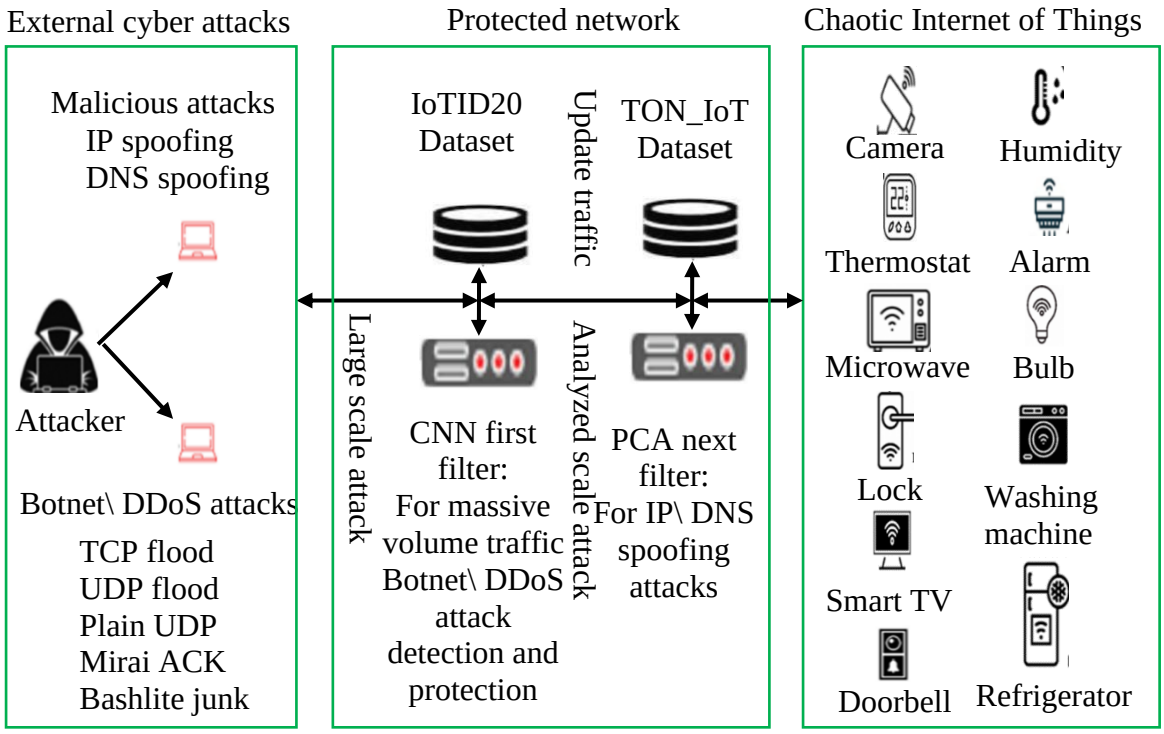


Figure 1: Proposed model to protect the Chaotic IoT system from cyberattacks

2.2 CNN-PCA Twin-Protected Shield

The model represents a hybrid model of CNN and PCA to protect Chaotic IoT networks from cyberattacks. The security mechanism starts with training a CNN as a deep learning model on the massive IoTID20 dataset, which contains both BENIGN and Bot\DDoS matrices network traffic. Through this partition of protection procedure, the CNN model learned how to extract the features and patterns of malicious attacks and classify and prevent the Botnet/DDoS attacks in live network traffic. In the next stage, the real-time live network traffic is loaded to the dataset after separating and numerating the target variables (labels) from the feature columns to detect if the traffic is BENIGN or DDOS. This procedure is accomplished utilizing the label encoding as shown in Equation (1). Numerical encoding is essential to ensure the fitness of inputs with the suggested model. The next stage is the normalization stage. In Equation (2), (x') represents the normalized value for (x), which is the original value with maximum and minimum values of features (x_{max}, x_{min}). Equation (2) is provided throughout the learning process. The attack detection procedure includes preparing and updating the database and loading data, and labels for necessary deep-learning training. The data is separated into 80% for training and 20% for testing. CNN is pre-trained on the network and extracts the network update features in the convolutional layer. The flattening layer is added at the end to flatten the extracted feature to a one-dimensional TensorFlow vector. The SoftMax activation function in Equation (3) is utilized to predict the probabilities where (z_i) embodies the output of the (i^{th}) neurons, and (k) is the number of classes. The loss is defined as the preparation classification task calculated by Equation (4) (Ashawa et al., 2024). The next filter in the security mechanism is the profiling of the PCA security model. The procedure starts training the model on the TON_IoT dataset, which contains sets of paradigms to identify anomaly traffic. After this portion of the protection procedure, the PCA model can filter the packets that are far from normal behavior. About the mathematical complexity of the PCA model, the output can be calculated by Equation (5). The data normalization for the APC method adopts min-max normalization to perform a linear transformation on the data within the [0,1] interval. The conversion function utilized is shown in Equation (6), where (x) is the (i^{th}) item before normalization (Jose & Jose, 2023; Al-Kahtani et al., 2023).

$$y_{encoded}=\text{LabelEncoder}(y_{categorical}) \quad (1)$$

$$\acute{x}=\frac{x-x_{min}}{x_{max}-x_{min}} \quad (2)$$

$$\text{oftmax}(z_i)=\frac{e^{z_i}}{y\sum_{i=1}^{k}e^{z_i}} \quad (3)$$

$$\text{oss}(y,\hat{y})=-\frac{1}{N}\sum_{i=1}^{N}y_i\log(\hat{y}_i) \quad (4)$$

$$\text{softmax}(z_i)=\frac{e^{z_i}}{y\sum_{i=1}^{k}e^{z_i}} \quad (5)$$

$$\text{loss}(y,\hat{y})=-\frac{1}{N}\sum_{i=1}^{N}y_i\log(\hat{y}_i) \quad (6)$$

2.3 Data Acquisition

There are two datasets used in this study. The first is the IoTID20 dataset that was used to train the CNN security model. The dataset contains both BENIGN network traffic and different attack types, for instance, Botnet, DDoS, TCP\ UDP flood, plain UDP, Mirai ACK, and Bashlite junk, which work on Chaotic IoT environments (Thereza & Harahap, 2024). The second dataset (TON_IoT) is used to train

the PCA security model. This dataset includes patterns of both BENIGN and IP\ DNS spoofing traffic (Tareq et al., 2022). These two datasets are up-to-date simultaneously from live network traffic.

2.4 Metrics

The performance of the suggested hybrid method is evaluated depending on Precision in Equation (7), recall in Equation (8), Accuracy in Equation (9), and F1-score in Equation (10). The ratio of truly detected attacks, namely, Precision, is represented mathematically in Equation (7), where TP represents the number of real input data, and FP represents intrusion data. The effectiveness of the recommended model to detect intrusion correctly is shown in Equation (8), where FN is the prediction results of intrusion in the Recall function (Sajid et al., 2024). Accuracy, which is represented mathematically in Equation (9), represents the correctly classified attack packet and normal packet, where the TN parameter represents the number of intrusion packets. Finally, the harmonic means of Precision and Recall values, namely F1-score, is mathematically represented in Equation (10). More metrics to show the significance of pair compared methods are the mean accuracy difference (MAD) to show the difference in mean accuracy (MA) between two models, as in Equation (11), and the P-value as shown in Equation (12), where α is a common value of 0.05 or 0.01 (Al-Yaseen & Idrees, 2023).

$$\text{Precision}=\frac{TP}{TP+FP}\times 100 \tag{7}$$

$$\text{Recall}=\frac{TP}{TP+FN}\times 100 \tag{8}$$

$$\text{Accuracy}=\frac{TP+TN}{TP+FN+TN+FP}\times 100 \tag{9}$$

$$\text{F1-Score}=2\times\frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{10}$$

$$\text{MAD}=|MA_{\text{Model A}}-MA_{\text{Model B}}| \tag{11}$$

$$\text{Significance}=\begin{cases}\text{Yes } (\rho<\alpha)\\ \text{No } (\rho\geq\alpha)\end{cases} \tag{12}$$

3 Results

The result in Table 1 shows the efficiency of the proposed model. The ideal measurements go for botnet\ DDoS attacks, where it is easy to predict the large-scale attacks. Balanced performance has been shown in micro and weighted averages across the IoTID20 and TON_IoT datasets. About the IP\ DNS spoofing prediction of intrusion, the values are varied but less than expected. For normal traffic in benign cases, the system is stable, as shown in the table results. Four iterations of training and one iteration for testing are shown in the experimental results records in Table 2. The Table shows accuracy through training, and in the end, the balanced testing value equals 98.88 % with a standard deviation equal to 0.06% which shows great stability. The accuracy behavior for the proposed model over Gaussian noise was carried out in Table 3 to show the durability of the model against possible adversarial perturbations and noisy surroundings. The noise is defined by zero mean and a standard deviation (σ = 0.1, 0.05, and 0.01).

Table 1: Classification performance metrics for botnet, DDoS, and BENIGN

Intrusion class	Precisión	Recall	F1-Score
Botnet\ DDoS attack	0.9973	0.9962	0.9965
IP\ DNS Spoofing	0.9954	0.984	0.9883
BENIGN	1.00	1.00	1.00
Weighted Avg.	0.9997	0.9994	0.9993
Macro Avg.	0.9991	0.9992	0.9996

Table 2: Period cross-validation accuracy results

Periods	Accuracy (%)
Training 1	98.64
Training 2	98.75
Training 3	98.82
Training 4	98.85
Testing 1	98.88
Mean	98.86 ± 0.06

Table 3: Model accuracy under gaussian noise perturbation

Noise Level (σ)	Accuracy (%)
0 (Original)	98.87
0.01	98.65
0.05	97.91
0.10	96.32

3.1 Accuracy and Loss Performance of CNN-PCA Models

The noise procedure simulates the packet loss obfuscation effect, or sensor abnormalities in real-time input. Figure 2 illustrates the performance of the proposed model to detect intrusion classified by the type of IoT devices. The figure shows that the botnet\ DDoS and IP\ DNS spoofing attacks are detected with an accuracy near 98.36% for doorbells, 98.62% for thermostat devices, and 98.81% for camera sensor devices, in most cases. Figure 3 shows the performance of the proposed CNN-PCA hybrid model, with each model's performance individually. The calculations show the training and validation accuracy of intrusion detection for each model and the loss of packets for each model. The results illustrate how the suggested CNN-PCA hybrid model demonstrates a significant improvement in intrusion detection and protection for a Chaotic IoT environment. Figure 3 (c) shows the positive accuracy and loss for the CNN-PCA hybrid model. The training and validation accuracy both reach a high accuracy, reaching 98.6%. That is a good indicator of the efficiency of the model learning and fast prediction. In terms of loss, the validation and training loss are nearly similar and decrease to reach 0.05. Compared with the CNN model and PCA model individually in Figure 3 (a), (b), the models also reach a high level of accuracy and low loss, but the result is volatile and still less than that of the proposed model.

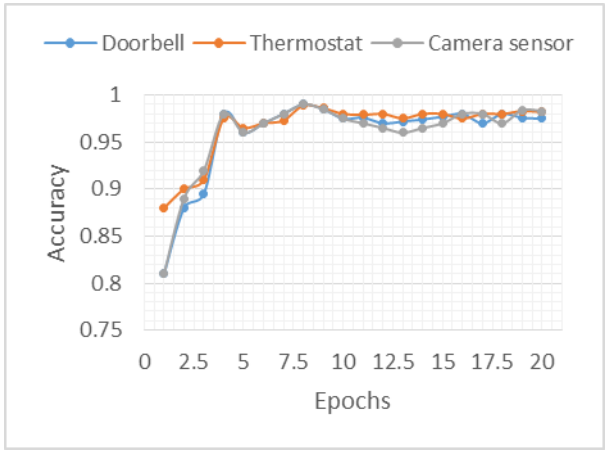
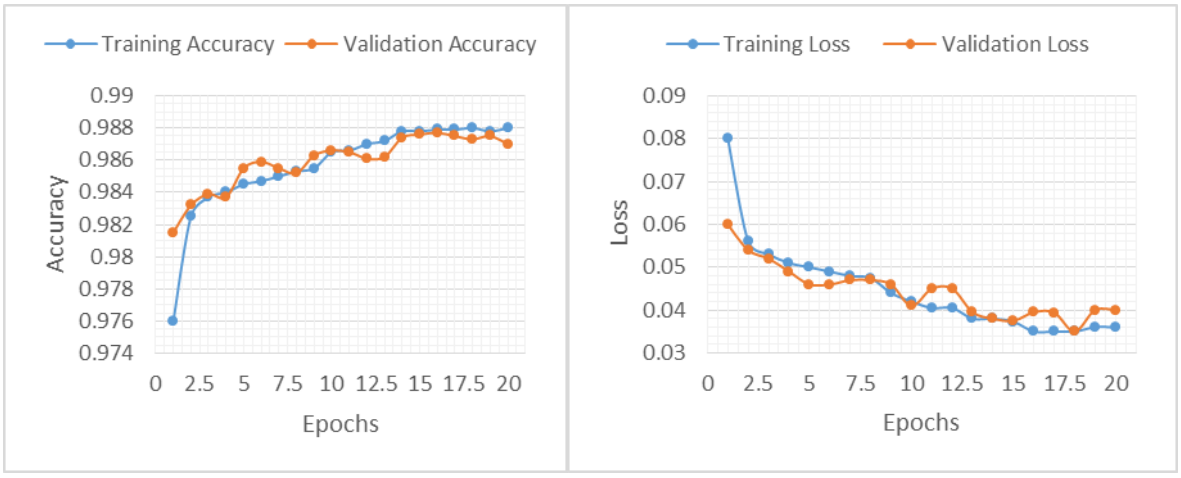
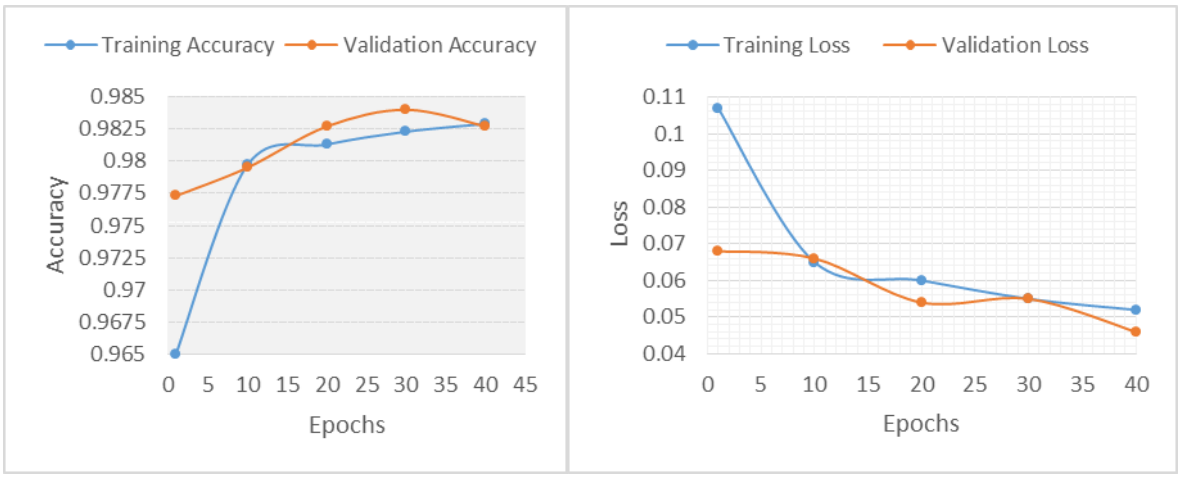


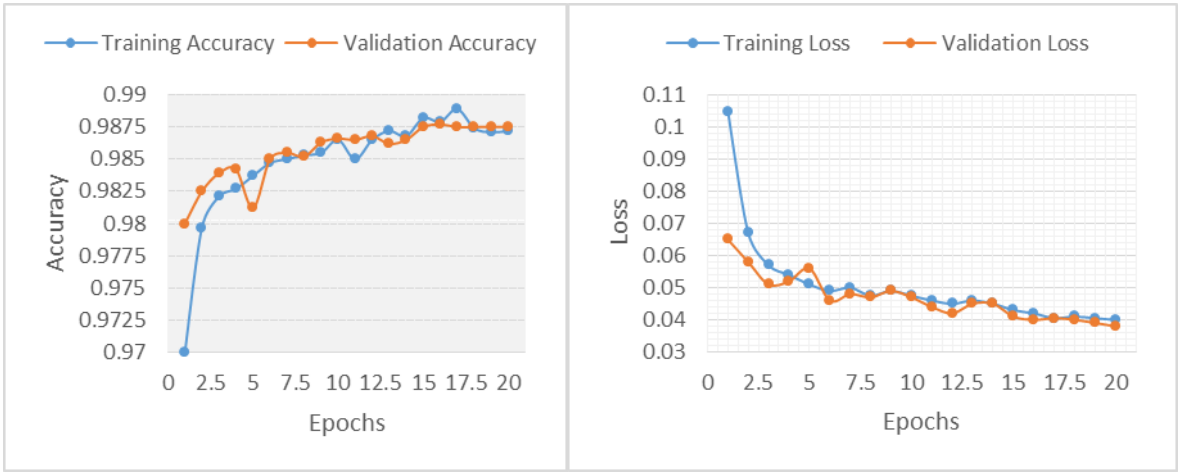
Figure 2: The performance of CNN-PCA to detect the botnet\ DDoS and IP\DND spoofing attacks from Chaotic IoT devices (doorbell devices, thermostat devices, and camera sensor devices)



(a)



(b)



(c)

Figure 3: The accuracy of prediction and loss packets performance of the proposed models: (a) CNN model, (b) PCA model, and (c) CNN-PCA hybrid model

4 Discussion

Botnets\ DDoS and IP\ DNS spoofing attacks are the most frequent attacks that intrude on Chaotic IoT devices. Our daily life is based on IoT devices, which are all under the chaotic IoT network. The vulnerability of these types of networks opens the door for attackers to develop tools to prevent security systems from achieving zero-day protection and devices to protect IoT devices. Therefore, utilizing hybrid artificial intelligence (AI) models to detect these types of attacks becomes more efficient. These models use a prevalent strategy to detect intrusion by gathering packets from the network and filtering to detect the expected attack. The prior attack traffic has been stored in the IoTID20 and TON_IoT datasets previously. After comparing with the extracted features of the network and previous scenarios from the datasets, the detection will be more effective. This study investigates the capability of using the CNN-PCA hybrid model to achieve efficient intrusion detection. The model is supported with two datasets and a daily traffic scenario. The efficiency of accurate intrusion detection comparison for the proposed model with the state-of-the-art AI models is shown in Table 4. The results in the table declared the accuracy of intrusion detection for the suggested model, with a value of 98% and the prediction of intrusion with a value reaching 99%. The compared models are PCA-DNN, DL, decision tree models (DTEXNet), ResNet50, and our proposed model. The comparison emphasizes the efficiency of the suggested model. In Figure 4, the metrics comparison becomes clearer. From the figure, the nearest significant results for all metrics are CNN-SLTM and ResNet50 methods. The CNN-PCA proposed model versus the CNN-LSTM and ResNet50 pair comparison has been illustrated in Table 5. The table displays the main accuracy difference and p-values to declare the significance of the proposed method. The p-value is obtained statistically through a testing period. Typically, the P-value depends on how the value is near the stable center of the alpha value, which is commonly between (0, 0.1). That means the best threshold value is 0.05. The smaller the p-value becomes, the smaller it is than the 0.05 threshold value, that indicates stronger the evidence for luckily received a good and stable occurrence accuracy. On the other hand, if the p-value became larger than 0.-05 threshold value, it is evidence that there is a chance to occur more random and unexpected accuracy. From the results, the CNN and ResNet series could work harmoniously with the PCA model as a hybrid. Since the significance results go to the 0.05

threshold value. That means the possibility of getting unexpected ranges of accuracy is an unlikely occurrence.

Table 4: Comparative Behavior of Different Models on DoS/DDoS Detection.

Model	Accuracy (%)	Precision	Recall	F1-Score	Inference Time (ms/sample)
PCA-DNN (Shafi et al., 2024)	88.642	0.832	0.872	0.714	10.233
DL	92.843	0.921	0.933	0.925	7.221
DTEXNet (Mahadik et al., 2023)	90.561	0.913	0.901	0.905	12.443
CNN-LSTM (Aswad et al., 2023)	96.128	0.966	0.963	0.961	6.162
ResNet50 (Al Lail et al., 2023)	97.353	0.972	0.971	0.973	9.843
CNN-PCA (Proposed)	98.642	0.991	0.996	0.995	5.678

Table 5. Comparing the nearest metrics methods versus the proposed method

Nearest models compare	CNN-LSTM	RestNet50
Main accuracy difference (%)	6.23	1.56
P-value	0.00032	0.0042
Significance	Yes (p< 0.02)	Yes (p< 0.05)

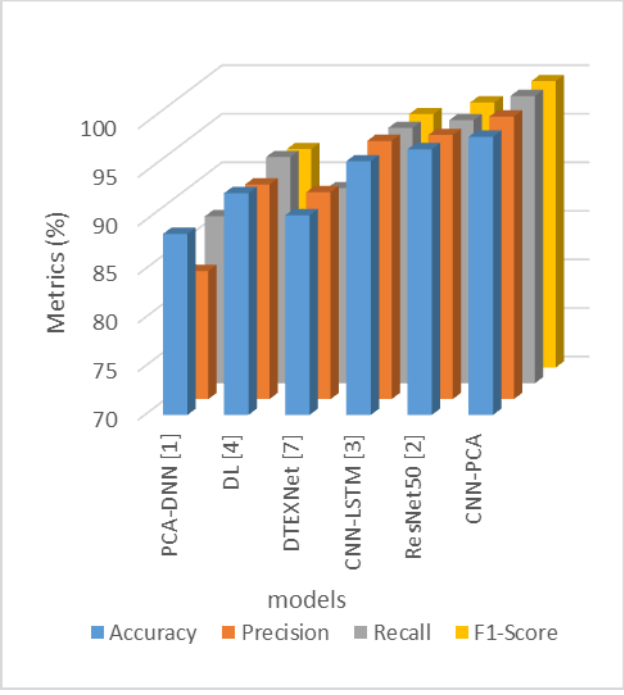


Figure 4: The metrics of state-of-the-art methods compared with the proposed method

5 Conclusions

The hybrid CNN-PCA intrusion detection model utilized in the research significantly enhances both training and detection speed while maintaining high detection accuracy. The model employed CNN to process the primary screening of botnet\ DDoS attacks, meanwhile and the PCA dealt with IP\ DNS spoofing vulnerability. The suggested model reads the packet traffic and simultaneously checks the result with the previous database to predict the intrusion. The accuracy of detection through training iterations varies, but the steady-state interval becomes more stable. Furthermore, the proposed model extracts feature of the packet in convolutional layers and reduces the prediction period. The proposed model shows 98.64% general Accuracy with a Precision equal to 0.991, a recall equal to 0.996, and an F1-score equal to 0.973, while the iteration time is 9.843 ms. The accuracy per device type shows that doorbell devices are equal to 98.36%, thermostat devices are equal to 98.62%, and camera sensor devices are equal to 98.81%. The efficiency and complexity of the proposed model are compared with state-of-the-art AI models, considering the individual detection accuracy per time for each attack. There is a limitation in encoding for the chaotic IoT, which leads to a search in reinforcement learning models for real-time detection of attacks in HetIoT devices.

Conflict of Interest

There is no type of conflict of interest related to the subject of the work.

Authorship Contribution

Conceptualization: Marwan Kadhim Mohammed AL-shammari, Data curation: Marwan Kadhim Mohammed AL-shammari, Formal analysis: Marwan Kadhim Mohammed AL-shammari, Acquisition of funds: Marwan Kadhim Mohammed AL-shammari, Research: Marwan Kadhim Mohammed AL-shammari, Methodology: Marwan Kadhim Mohammed AL-shammari, Project administration: Marwan Kadhim Mohammed AL-shammari, Resources: Marwan Kadhim Mohammed AL-shammari, Software: Marwan Kadhim Mohammed AL-shammari, Supervision: Marwan Kadhim Mohammed AL-shammari, Validation: Marwan Kadhim Mohammed AL-shammari, Visualization: Marwan Kadhim Mohammed AL-shammari, Writing - original draft: Marwan Kadhim Mohammed AL-shammari, Writing - review and editing: Marwan Kadhim Mohammed AL-shammari.

References

[1] Al Lail, M., Garcia, A., & Olivo, S. (2023). Machine learning for network intrusion detection—a comparative study. *Future Internet*, *15*(7), 243. https://doi.org/10.3390/fi15070243

[2] Alghazzawi, D., Bamasag, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. *Applied Sciences*, *11*(24), 11634. https://doi.org/10.3390/app112411634

[3] Alkahtani, H., & Aldhyani, T. H. (2021). Botnet attack detection by using CNN-LSTM model for Internet of Things applications. *Security and Communication Networks*, *2021*(1), 3806459. https://doi.org/10.1155/2021/3806459

[4] Al-Kahtani, M. S., Mehmood, Z., Sadad, T., Zada, I., Ali, G., & ElAffendi, M. (2023). Intrusion detection in the Internet of Things using fusion of GRU-LSTM deep learning model. *Intelligent Automation & Soft Computing*, *37*(2), 2279-2290. https://doi.org/10.32604/iasc.2023.037673

[5] Alsbatin, L., Alrifai, B. M., Zawaideh, F., & Alawneh, T. A. (2025). Advancing IoMT security: Machine learning-based detection and classification of multi-protocol cyberattacks. *Journal of*

Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, *16*(2), 228–247. https://doi.org/10.58346/JOWUA.2025.I2.015

[6] Al-Yaseen, W. L., & Idrees, A. K. (2023). MuDeLA: multi-level deep learning approach for intrusion detection systems. *International Journal of Computers and Applications*, *45*(12), 755-763. https://doi.org/10.1080/1206212X.2023.2275084

[7] Ashawa, M., Owoh, N., Hosseinzadeh, S., & Osamor, J. (2024). Enhanced Image-Based Malware Classification Using Transformer-Based Convolutional Neural Networks (CNNs). *Electronics*, *13*(20), 4081. https://doi.org/10.3390/electronics13204081

[8] Aswad, F. M., Ahmed, A. M. S., Alhammadi, N. A. M., Khalaf, B. A., & Mostafa, S. A. (2023). Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. *Journal of Intelligent Systems*, *32*(1), 20220155. https://doi.org/10.1515/jisys-2022-0155

[9] Chanu, U. S., Singh, K. J., & Chanu, Y. J. (2023). A dynamic feature selection technique to detect DDoS attack. *Journal of Information Security and Applications*, *74*, 103445. https://doi.org/10.1016/j.jisa.2023.103445

[10] Chen, E., Zhang, N., Tu, X., & Bao, X. (2025). Optimized DDoS Detection in Software-Defined IIoT Using a Hybrid Deep Neural Network Model. *Internet Technology Letters*, *8*(3), e70012. https://doi.org/10.1002/itl2.70012

[11] Dahiya, D. (2023). DDoS attacks detection in 5G networks: hybrid model with statistical and higher-order statistical features. *Cybernetics and Systems*, *54*(6), 888-913. https://doi.org/10.1080/01969722.2022.2122002

[12] Dener, M., Okur, C., Al, S., & Orman, A. (2023). Wsn-bfsf: a new data set for attacks detection in wireless sensor networks. *IEEE Internet of Things Journal*, *11*(2), 2109-2125. https://doi.org/10.1109/JIOT.2023.3292209

[13] Deshmukh, A., & Ravulakollu, K. (2024). An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity. *Technologies*, *12*(10), 203. https://doi.org/10.3390/technologies12100203

[14] Fayyadh, S. A. F., & Kayabaş, A. (2023). Semi-Supervised Learning for Intrusion Detection in IoT Networks with UNSW_NB15 Dataset. *International Journal of Advances in Engineering and Emerging Technology*, *14*(1), 229-243.

[15] Hnamte, V., & Hussain, J. (2023). An efficient DDoS attack detection mechanism in SDN environment. *International Journal of Information Technology*, *15*(5), 2623-2636. https://doi.org/10.1007/s41870-023-01332-5

[16] Issa, A. A., & Albayrak, Z. (2023). DDoS attack intrusion detection system based on hybridization of CNN and LSTM. *Acta Polytechnica Hungarica*, *20*(2), 1-19.

[17] Jose, J., & Jose, D. V. (2023). Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(1), 1134-1141. https://doi.org/10.11591/ijece.v13i1.pp1134-1141

[18] Kalutharage, C. S., Liu, X., Chrysoulas, C., Pitropakis, N., & Papadopoulos, P. (2023). Explainable AI-based DDOS attack identification method for IoT networks. *Computers*, *12*(2), 32. https://doi.org/10.3390/computers12020032

[19] Karthik, M. G., & Krishnan, M. M. (2021). Securing an internet of things from distributed denial of service and Mirai botnet attacks using a novel hybrid detection and mitigation mechanism. *Int. J. Intell. Eng. Syst*, *14*(1), 113-123. https://doi.org/10.3390/electronics13204081

[20] Lavanya, V., & Sekhar, P. C. (2024). Efficient Cybersecurity Model Using Wavelet Deep CNN and Enhanced Rain Optimization Algorithm. *International Journal of Image and Graphics*, *24*(04), 2450048. https://doi.org/10.1007/s10922-022-09697-x

[21] Mahadik, S., Pawar, P. M., & Muthalagu, R. (2023). Efficient intelligent intrusion detection system for heterogeneous internet of things (HetIoT). *Journal of Network and Systems Management*, *31*(1), 2. https://doi.org/10.1007/s10922-022-09697-x

[22] Manaa, M. E., Hussain, S. M., Alasadi, S. A., & Al-Khamees, H. 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

[23] Mansoor, A., Anbar, M., Bahashwan, A. A., Alabsi, B. A., & Rihan, S. D. A. (2023). Deep learning-based approach for detecting DDoS attack on software-defined networking controller. *Systems*, *11*(6), 296. https://doi.org/10.3390/systems11060296

[24] Mehmood, S., Amin, R., Mustafa, J., Hussain, M., Alsubaei, F. S., & Zakaria, M. D. (2025). Distributed denial of services (DDoS) attack detection in SDN using Optimizer-equipped CNN-MLP. *PloS one*, *20*(1), e0312425. https://doi.org/10.1371/journal.pone.0312425

[25] Nadim, I., Rajalakshmi, N. R., & Hammadeh, K. (2024). A Novel Machine Learning Model for Early Detection of Advanced Persistent Threats Utilizing Semi-Synthetic Network Traffic Data. *Journal of VLSI Circuits and Systems*, *6*(2), 31-39. https://doi.org/10.31838/jvcs/06.02.04

[26] Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2023). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. *Engineering Reports*, *5*(12), e12697. https://doi.org/10.1002/eng2.12697

[27] Najar, A. A., Sugali, M. N., Lone, F. R., & Nazir, A. (2024). A novel CNN-based approach for detection and classification of DDoS attacks. *Concurrency and Computation: Practice and Experience*, *36*(19), e8157. https://doi.org/10.1002/cpe.8157

[28] Nawaz, M., Tahira, S., Shah, D., Ali, S., & Tahir, M. (2025). Lightweight machine learning framework for efficient DDoS attack detection in IoT networks. *Scientific Reports*, *15*(1), 24961. https://doi.org/10.1038/s41598-025-10092-0

[29] Prabu, K., & Sudhakar, P. (2023). An automated intrusion detection and prevention model for enhanced network security and threat assessment. *Int. J. Comput. Netw. Appl*, *10*(4), 621. https://doi.org/10.22247/ijcna/2023/223316

[30] Rezvani, A., Mirzaei, A., Mikaeilvand, N., Nouri-Moghaddam, B., & Gudakahriz, S. J. (2025). A novel framework for enhancing data collection macro-strategies in heterogeneous IoT networks using advanced mathematical modeling. *Archives for Technical Sciences*, *2*(33), 1–21. https://doi.org/10.70102/afts.2025.1833.001

[31] Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing*, *13*(1), 123. https://doi.org/10.1186/s13677-024-00685-x

[32] 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

[33] Shafi, M., Lashkari, A. H., Rodriguez, V., & Nevo, R. (2024). Toward generating a new cloud-based Distributed Denial of Service (DDoS) dataset and cloud intrusion traffic characterization. *Information*, *15*(4), 195. https://doi.org/10.3390/info15040195

[34] Soy, A., & Nayak, A. (2021). Machine Learning-enabled Intrusion Identification Model for IoT Environment. *International Academic Journal of Science and Engineering*, *8*(1), 53–57.

[35] Tareq, I., Elbagoury, B. M., El-Regaily, S., & El-Horbaty, E. S. M. (2022). Analysis of ton-iot, unw-nb15, and edge-iiot datasets using dl in cybersecurity for iot. *Applied Sciences*, *12*(19), 9572. https://doi.org/10.3390/app12199572

[36] Thereza, N., & Harahap, P. R. (2024). Enhancing the performance of IoT network intrusion detection models using NF-ToN-IoT-V2 and IoTID20 datasets with chi-square feature selection. *Sriwijaya Electrical and Computer Engineering Journal*, *1*(2), 64-76. https://doi.org/10.62420/selco.v1i2.7

[37] Yaseen, A. (2023). The role of machine learning in network anomaly detection for cybersecurity. *Sage Science Review of Applied Machine Learning*, *6*(8), 16-34. https://orcid.org/0009-0002-8950-0767

[38] Yin, X., Fang, W., Liu, Z., & Liu, D. (2024). A novel multi-scale CNN and Bi-LSTM arbitration dense network model for low-rate DDoS attack detection. *Scientific Reports*, *14*(1), 5111. https://doi.org/10.1038/s41598-024-55814-y

Author Biography

Marwan Kadhim Mohammed Al-shammari, PhD, in Northeastern University. He received the B.S. in Computer Engineering from Baghdad University, Iraq in 2000, the M.S. in Computer Engineering from UTeM University, Malaysia, in 2014, CISCO American institute instructor from 2007. He joined Baghdad University in 2006 as a lecturer at the Department of Computer Engineering. He was director for research & developing division and training & continues learning division respectively. He was a Core member in the advisory office of Baghdad University. He has been a team leader at South Korean and Canada with Coicka and ED companies respectively. He is team leader for many projects in the field of Java, Dot.net, visuals, IOS, OS, CG, Media, Networking, DB, Embedded Systems, Embedded Software, VR, EEG, Robotic surgery, Networking. He was a lecturer for postgraduate students at Northeastern University.