Babylonian Journal of Networking
Vol.2025, **pp.** 197–206
DOI: https://doi.org/10.58496/BJN/2025/018; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Smart Hybrid Intrusion Detection for IoT Networks Using Machine Learning and Neural Networks

Klodian Dhoska [1,*], Panagiotis Kyratsis [2], Marek Dudek [3], Phani Praveen Surapaneni [4], Aaron Mogeni oirere [5]

[1] *Department of Mechanics, Polytechnic University of Tirana,Albania.*

[2] *Department of Product and Systems Design Engineering, University of Western Macedonia, Greece.*

[3] *Management Faculty, AGH University of Krakow, Poland*

[4] *Department of Computer Science & Engineering, P.V.P.Siddhartha Institute of Technology, India.*

[5] *Department of computer science, Murang'a University of Technology, Kenya.*

ARTICLE INFO

Article History

Received 30 Aug 2025
Revised 25 Sep 2025
Accepted 3 Nov 2025
Published 14 Dec 2025

Keywords
Smart Intrusion Detection,
IoT Security,
Cascade Backpropagation Neural Network (CPBNN),
Convolutional Neural Network (CNN),
Machine Learning,
KDDTest-21 Dataset,
DDoS Detection,
Network Anomaly Classification.

ABSTRACT

With the fast growth of Internet of Things (IoT), there is an increasing security impact, e.g., IoT environments has become the advanced target of complex cyber-attack like Distributed Denial of Service (DDoS) attack. Most conventional Intrusion Detection Systems (IDSs) fail to scale with the heterogeneity, scale, and dynamism of IoT networks. To overcome these challenges, in this paper, we develop a smart hybrid intrusion detection framework that can effectively utilize the power of Machine Learning (ML) and Neural Network (NN) models, namely: cascades backpropagation neural network (CPBNN) and convolutional neural network (CNN) to improving accuracy and adaptability of detection in IoT environments. The proposed system employs a two-layer detection structure where the CPBNN model is used to detect abnormal patterns in the network packet level and identify the abnormal behaviors of packet sequences, whereas the CNN model performs deep feature extraction and classification to predict the abnormality as well as the nature of the abnormality. We develop this hybrid architecture to work well under IoT level large-scale deployments without incurring software overhead. The system has been evaluated on the KDDTest-21 benchmark dataset with the usual metrics, including accuracy, precision, recall and F1-score. Experiments results prove the CNN's performance with 90% and CPBNN with 82% which valid the efficiency of the proposed method in detecting IoT related security threats. These results suggest the ability of intelligent hybrid IDS systems not only to defend in a pro-active manner using ML and neural networks in synergy, but also to use the adversary's strength against itself.

1. INTRODUCTION

Rapid proliferation of Internet of Things (IoT) is transforming several domains such as health care, industrial automation, smart cities, and so on, facilitating billions of devices to interconnect around the globe. And that's going to be great because it's all connected, but all being connected has a downside when it comes to security." The inherently constrained, heterogeneous and decentralized structure of IoT networks render them highly vulnerable to complex cyber-attacks like DDoS (Distributed Denial of Service), malware embedding, data tampering [1]. Classical security defenses e.g., when using cryptography, and authentication and access control – only keeps the attackers at bay to some extent, and do not provide a very scalable solution in the presence of a massive coordinated attacks [2,3]. Thus, the security of IoT infrastructures need more intelligent, adaptive mechanisms, especially in the field of Intrusion Detection Systems (IDSs). Recent works also exploited Machine Learning (ML) and Neural Networks (NNs) to develop real-time IDS solutions to detect abnormal behavior and unknown threats [4]. In spite of these attempts, the research and technical practices of current IDS are subject to some long-standing issues. There are several including lack of scalability, inability to handle high-dimensional traffic data, and lack of/reactivity to emerging threat environments. A number of recent works have tried to tackle these problems. For example, [5] presented an IDS that combines deep learning with XAI to enhance transparency of detection. The computational burden of the model on low-power IoT devices, however, remains challenging for deployment.

*Corresponding author. Email: pkdutta@kol.amity.edu

Similarly, [6] investigated ML based techniques in protecting the IoMT where they achieved better detection but were not resilient to complex multi-vector attacks. In another work, Moonsamy et al. [7] proposed hardware-software co-optimized IDSs with Deep Q-Network, but their approach had high computational requirements that limit its deployment in resource-constrained environment. To cope with these limitations, a smart hybrid IDS system is proposed in this paper to take advantage of the benefits of machine learning and neural network models. Specially, for anomaly detection and traffic classification the CPBNN and CNN are utilized respectively. This architecture consists of two layers, which is to improve accuracy, lower the false positives and negatives as well as to real-time speed up. The main contributions of this paper are:

a) Development of a dual-layered hybrid IDS that integrates CPBNN and CNN for enhanced IoT security.
b) Comprehensive evaluation of the proposed system using real-world benchmark datasets, including **KDDTest-21**.
c) Demonstration of the system's adaptability, scalability, and detection robustness in complex and dynamic IoT environments.

The rest of the paper is organized as follows: we conduct a review of related work in IoT network and their limitations in detection in Section 2. The proposed approach and system model architecture is explained in Section 3, including integration of cascade backpropagation neural network (CPBNN) and CNN models for the hybrid IDS. Section 4 presents experimental results and performance analysis, considering evaluation measures including accuracy, precision, recall, F1-score on benchmark datasets. 5 concludes the study and proposed possible future research towards using advanced machine learning for securing IoT.

2. LITERATURE REVIEW

Security in Internet of Things (IoT) networks has been the subject of research in recent years where several approaches have been proposed to improve the efficiency and dependability of Intrusion Detection Systems (IDS). Because of the complexity of the IoT, IDS models have been introduced with machine learning (ML) and deep learning (DL) to help them to detect and deter cyber-attacks. The following subsection summarizes some recent relevant studies with emphasis in the methodology used, main findings, strengths, and weaknesses. In [8], provided a survey of IDS in IoT network by combining deep learning and Explainable Artificial Intelligence (XAI). This fusion was more interpretable to security experts, resulting in an accuracy of 93.05%. Nonetheless, the sophisticated structure of the model and the high computational complexity of the inference algorithm made it difficult to directly apply to resource-limited IoT settings. In [9] used ML for enhancing the efficiency of IDS in IoMT networks with the detection accuracy of 90.76%. Though effective, the approach faced challenges posed by the necessity of real-time data processing in healthcare applications (where time can play a crucial role). As well as, [10] presented an IDS technique called a fusion hybrid algorithm built upon blockchain technology and federated learning in edge-based industrial IoT networks. Their proposal solved the problem of security and latency and eventually they faced scalability issues when used on large scale industrial use case. In [11] proposed a hybrid intrusion detection method adopting deep Q-networks in an optimization approach and demonstrated the effectiveness in decreasing false positives and enhancing the detection ratio. However, the method was computationally expensive and will not be applicable to low-power IoT devices. Also, [12] investigated the potential of generative AI and large language models to improve IoT security by facilitating self-organized response systems. While interesting, their method left some questions as to whether we were going to be too dependent on automation in dynamic cyber threat environments. Study [13] explored CNNs and RNNs for IoT IDSs, and achieved high detection rates. But the requirement to have a substantial amount of training data and the lack of a transparent model made it difficult to apply in practice. Nanjappan [14] developed DeepLG SecNet that combined together LSTM and GRU for enhanced intrusion detection in IoT. Although the model demonstrated improved accuracy and faster detection, further optimization was required for scale and computational efficiency and [15] used deep residual CNNs for anomaly detection in IDS with greater than 92% accuracy. Their technique was successful, but the method involved extensive data pre-processing and computing resources, making it less suitable for resource constrained IoT devices. [16] proposed a VGG19 and 2D-CNN model-based hybrid IDS for FOG-cloud environment. Although the system in [7] achieved strong detection performance, it had challenges in real-time processing since it was computationally heavy. In [17] introduced the transformer-based IDS architecture, Flow Transformer, which can achieve better accuracy and scalability for IoT networks. The authors however conceded the requirement to validate in different IoT ecosystems for generalizability. At [18] improved the performance of IDS by employing a hybrid ML model and obtained 95.12% accuracy. Although effective, their technique was computationally expensive, which was not very suitable to resource-constrained distributed IoT networks. Perumal et al. [19] proposed VBQ-Net, i.e., vectorization-based boosted quantized network, to enhance IoT security. Although it achieved better detection than the previous system, improvement could not keep pace with the known threats. Study [20] present ROAST-IoT, an attention based convolutional network to perform real-time intrusion detection for IoT. Although the accuracy and speed of the system was better, but further validation was required on heterogeneous large-scale environments. In a survey by [21], which emphasized the increasing prevalence of CNN and RNN architectures for IoT IDS. These models, however, suffered from interpretability and dependency to big labeled datasets. At [22] introduced a three-layer CNN-based IDS, which obtained a detection accuracy of 94.65%. Despite its good performance, this model was sensitive to false positives in dynamic scenes. Study [23] utilized ML algorithms for DDoS detection in IoT infrastructure, and outperformed traditional approach in terms of the overall accuracy at a particular large-scale attack. However, scalability became a significant issue in the case of larger IoT systems. Study by [24] described an IDS framework based on reinforcement learning that achieved 92.8% accuracy and remained robust against new cybermen aces. However, this framework must be optimized to be computationally feasible for large applications. At [25] performed a statistical examination and an ML analysis on the KDDS-001 dataset to evaluate IDS performance and obtained 91.2% accuracy. Zero-day attack identification was still a problem for the system though, which is important for the security of today's IoT networks. Study [26] also aimed to enhance industrial IoT security via the use of AI-driven IDS and reached an accuracy of 93.4%. However, the system had high computational requirements as well as latency may limit its scalability. As well as [27] proposed an SVM-PSO classifier model using telemetry data for IDS in IoT network. As a result, the SVM also reached increased performance (89.7% accuracy) for detecting pneumonia. But this still needed fine-tuning to enable real-time processing, and high-velocity data firehoses. These studies are summarized in Table I, with the methods, findings, strengths, and weaknesses reviewed. Taken together, the literature presents clear advancements in terms of accuracy, computational cost, and scalability. Yet, there are still critical challenges left, in particular on real-time detection, on the ability to adapt to new threats and to be deployable on resource constrained IoT devices.

TABLE I: SUMMARY OF RECENT STUDIES ON IDS FOR IOT SECURITY (2022–2024)

Study	Method	Accuracy / Results	Strengths	Limitations
[8]	Deep Learning + XAI	93.05%	High accuracy, transparency	High complexity
[9]	ML for IoMT	90.76%	Effective detection	Real-time delays
[10]	Blockchain + Federated Learning	Improved security	Low latency	Scalability limits
[11]	Deep Q Networks	Fewer false positives	Precise detection	High computation
[12]	Generative AI + LLMs	Future outlook	Solves complex issues	Over-automation risk
[13]	CNNs and RNNs	High accuracy	Deep model efficiency	Data dependency
[14]	LSTM + GRU	Faster detection	Improved performance	Deployment scale issues
[15]	Residual CNN	>92%	Anomaly detection	Resource-heavy
[16]	VGG19 + 2D-CNN	Robust rates	Effective detection	Overhead load
[17]	Transformer (Flow)	Improved accuracy	Scalable	Needs real-world tests
[18]	Hybrid ML	95.12%	High precision	High training cost
[19]	VBQ-Net	Effective detection	IoT-focused	Adaptability gap
[20]	ROAST-IoT	High speed/accuracy	Real-time detection	Needs large validation
[21]	CNN & RNN	High detection	Strong accuracy	Low explainability
[22]	3-layer CNN	94.65%	Accurate	High FPR in dynamics
[23]	ML for DDoS	Improved detection	Scalable for DDoS	Complex deployment
[24]	Reinforcement Learning	92.8%	Robust to new threats	Resource intensive
[25]	Statistical + ML	91.2%	Strong baseline	Poor zero-day detection
[26]	AI for IIoT	93.4%	Robustness	Scalability challenge
[27]	SVM-PSO	89.7%	Improved SVM efficiency	Real-time tuning required

3. METHODOLOGY

The proposed methodology implies the use of a two-tier intrusion detection system consisting of two machine learning ML models : Cascade Backpropagation Neural Network CBPNN and Convolutional Neural Network CNN. The objective of such ML models is to improve IDS performance through the analysis of raw data from the KDDTest-21 dataset. All the models were developed and trained on the basis of MATLAB. The configurations of all the models for the training mode are presented in Table II. Before training, the preprocessing of data was performed according to Figure 1.

TABLE II: CONFIGURATION OF ML MODELS

Parameter	Value
Training Method	Supervised Learning (SL & ANN)
Number of Epochs	100
Maximum Gradient	1×10^{-30}
Mean Squared Error	1×10^{-30}
Types of ML Models	CBPNN, CNN
Number of Test Sets	10

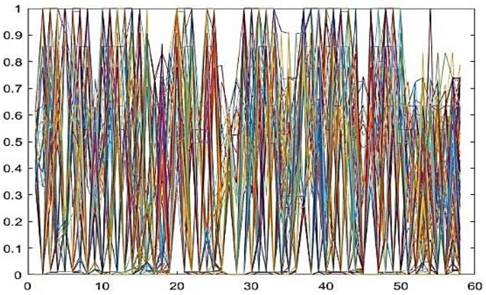


Fig 1. Dataset Preprocessing Workflow

3.1 Implementation of CBPNN and CNN Algorithms

CBPNN and CNN, two ML models for data processing and classification, were used to train IDS. These two models were selected because they are strong in detecting complicated patterns as signs of possible network intrusions.

3.1.1. CBPNN Design

The CBPNN architecture is designed to improve anomaly detection and classification in IoT systems. It is a multilayer system with the following layers:

a) **Input Layer**: Comprising 500 neurons to capture the high-dimensional features extracted during preprocessing. This layer enables the model to efficiently detect anomalous traffic patterns in IoT data.
b) **Hidden Layers**: Ten sets of neurons are designed to learn complex interrelations that help differentiate between normal and malicious traffic.
c) **Output Layer**: Produces the final classification indicating whether the traffic is normal or an attack.
d) **Random Node Distribution**: This setup mimics the dynamic structure of IoT networks, particularly simulating "DDoS nodes" to analyze vulnerability points effectively.

The cascading property of the CBPNN model enables it to learn across time and gradually grow the number of neurons and layers. This flexibility allows the model to dynamically learn various shifts in the traffic patterns, which reduces the overfitting that can occur when using a static model and results in better detection performance. The illustration of the construction and application of the CBPNN, as well as the design interface are depicted in Figure 2, and a flowchart of implementation of the algorithm is showed in Figure 3.

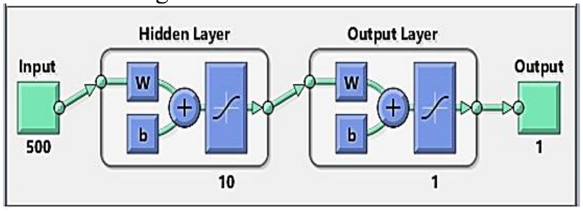


Fig 2. Architecture of the CBPNN Algorithm

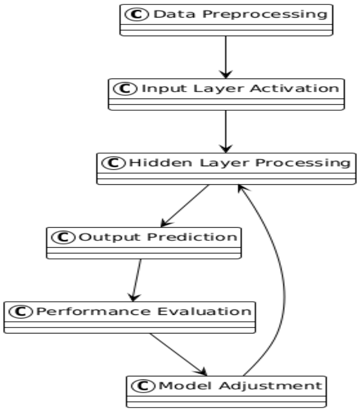


Fig 3. Flowchart of the CBPNN Algorithm.

3.1.2. Convolutional Neural Network (CNN) Design

The CNN model is tailored to classify IoT network traffic by identifying spatial features through convolutional layers. Its architecture consists of:

a) **Input Layer**: Contains 500 neurons for feature intake.
b) **Hidden Layers**: A fully connected layer with 10 units captures nuanced patterns in the network traffic.
c) **Output Layer**: Outputs the final classification, indicating whether the instance is an attack.

The CNN models include the allocation of nodes with DDoS-like behavior being simulated using dynamically allocated nodes, with four nodes specifically allocated to this, as shown in Figure 4. This flexible model improves the model's capability to recognize a wide range of cyber threats targeting IoT systems. The CNN model is engineered to accommodate traffic patterns in IoT, thus, achieving higher classification accuracy. It is a flexible system that can adjust to new data to counter emerging attack vectors. The CNN algorithm flow is shown in Figure 5.

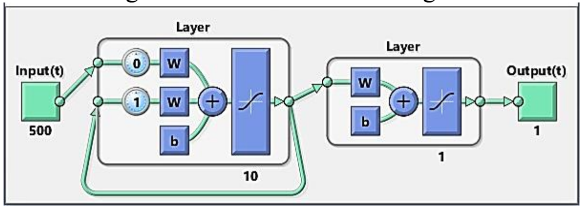


Fig 4. Architecture of the CNN Algorithm.

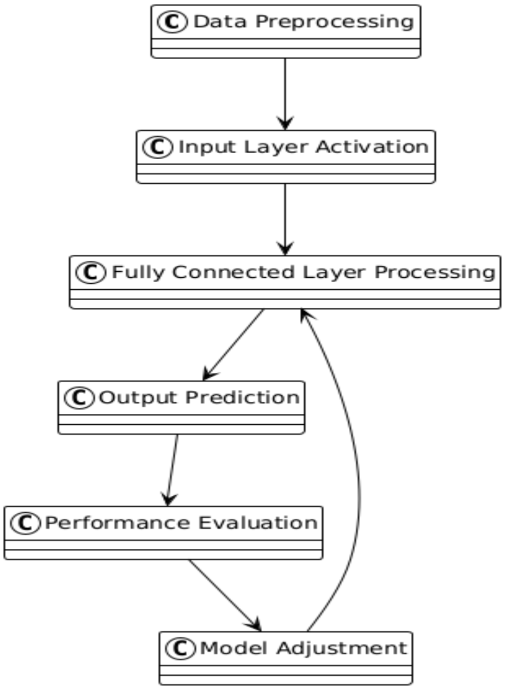


Fig 5. Flowchart of the CNN Algorithm

3.2 Training and Evaluation

The training and testing subsystem of the proposed hybrid IDS contains two machine learning models: CBPNN and CNN. These models are trained and tested with the preprocessed KDDTest-21 dataset. The preprocessing phase consists of cleaning and transforming raw packet-capture data, and selecting interesting elements such as protocol type, service and flag fields to build up a high dimensional data set that can be used for classifying packets with machine learning algorithms. The performance of both the models is measured by the commonly used criteria: Accuracy (ACC), Detection Rate (DR) and False Positive Rate (FPR). The choices of CBPNN and CNN algorithms is driven by their capabilities to work with complex and high-dimensional datasets, which is crucial for anomaly detection in IoT networks. In order to provide a sound and generalizable evaluation, the dataset is divided into training, validation and testing sets. Training data is used to develop model parameters, validation data is used for hyperparameter tuning and model selection, and the testing data provides an unbiased estimate of performance of the final model. BOS methods such as cross-validation and early stopping are used to avoid overfitting and improve generalization ability of the model to new data. The simulation results of CBPNN approach and MATLAB simulation of CNNs are shown in Fig. 6.

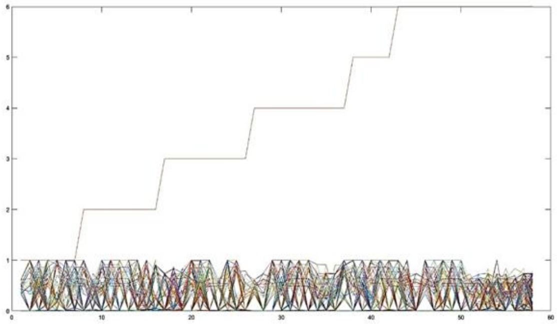


Fig 6. experimental results of the CBPNN and CNN models obtained from MATLAB simulations.

3.2.1. Performance Metrics

To evaluate the effectiveness of the IDS, the following classification outcomes are considered:

a) **True Positive (TP):** Number of correctly identified abnormal records.
b) **False Positive (FP):** Number of normal records incorrectly classified as abnormal.
c) **True Negative (TN):** Number of correctly identified normal records.
d) **False Negative (FN):** Number of abnormal records misclassified as normal.

From these values, the following evaluation metrics are computed:

- **Accuracy (ACC):** Proportion of correctly classified records among all records.

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \times 100\% \quad (1)$$

- **Detection Rate (DR):** Also known as True Positive Rate or Recall, this measures the ratio of correctly detected abnormal instances.

$$DR = \frac{TP}{TP + FN} \times 100\% \quad (2)$$

- **False Positive Rate (FPR):** Measures the proportion of normal records misclassified as abnormal.

$$\boldsymbol{FPR = \frac{FP}{FP + TN} \times 100\%} \quad (3)$$

Anomaly detection thresholds were empirically derived and tuned to maximize performance. The effect of different thresholds on ACC, DR and FPR was tested to fructify the detection performance in different network models and attack behaviors. The main goal of the IDS assessment should be to optimize detection (the highest Detection Rate and Accuracy) with the lowest number of false positive. The hybrid IDS system proposed shows great prospect in improving the security of IoT networks by efficiently identifying and mitigating new cyber threats.

4. EXPERIMENTAL RESULT

Performance of the proposed hybrid IDS in terms of the CBPNN and CNN models were implemented and tested. Models were evaluated with K-fold cross validation that improves the confidence level by breaking up the dataset into K complementary parts, where use of every observation in training and validation phases is guaranteed. The statistical efficacy results for the models are given in Tables III and IV.

TABLE III: PERFORMANCE METRICS OF THE CBPNN MODEL

Metric	Result
Validation Method	K-fold
Number of Observations	58
Number of Test Sets	10
Accuracy (Acc)	82%
Mean Squared Error (MSE)	1.4138
Mean Absolute Error (MAE)	0.512
Root Mean Squared Error	1.189
Runtime	27 seconds

TABLE IV: PERFORMANCE METRICS OF THE CNN MODEL

Metric	Result
Validation Method	K-fold
Number of Observations	50
Number of Test Sets	10
Accuracy (Acc)	90%
Mean Squared Error (MSE)	0.988
Mean Absolute Error (MAE)	0.327
Root Mean Squared Error	0.991
Runtime	17 seconds

These results indicated that the CNN model far surpassed the CBPNN model in detection accuracy and computational efficiency. The optimal CNN presented a classification accuracy of 90% with a processing time of about 17 seconds, proving the efficiency to learn and detect complex attack patterns in IoT traffic.

4.1 Analysis of Detection Capabilities

Detection capability the analysis shows that the CNN model is quite good at identifying DDoS attacks. As shown in Figure 7, the CNN model obtained a validation gradient of 1.1567 and performed well at 8 validation positions with no significant DE degradation at epoch 10. But the preliminary tests didn´t go well in positions 0 and 2, which means that the model can be refined in some way.

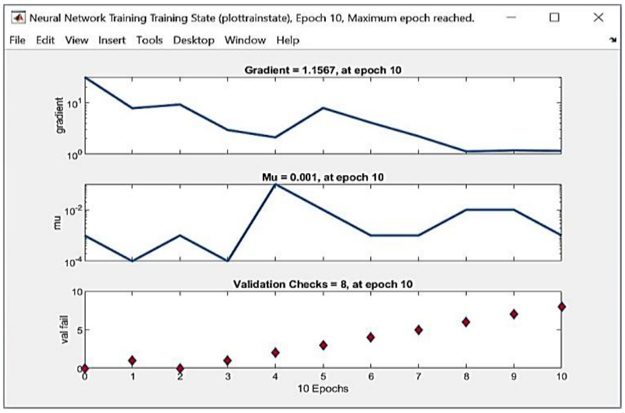

Neural Network Training Training State (plottrainstate), Epoch 10, Maximum epoch reached.
File Edit View Insert Tools Desktop Window Help
Gradient = 1.1567, at epoch 10
gradient
10^1
10^0
Mu = 0.001, at epoch 10
mu
10^{-2}
10^{-4}
Validation Checks = 8, at epoch 10
val fail
10
5
0
0 1 2 3 4 5 6 7 8 9 10
10 Epochs

Fig 7. Results for the Best Algorithm (CNN)

Furthermore, the validation accuracy was assessed using the mean squared error (MSE) criterion. As described in Figure 8, the minimum value of validation loss appeared in epoch 2 and the higher value of validation accuracy was 2.8118. It also shows the training and validation curves which confirms that CNN has a nearly balanced learning behavior.

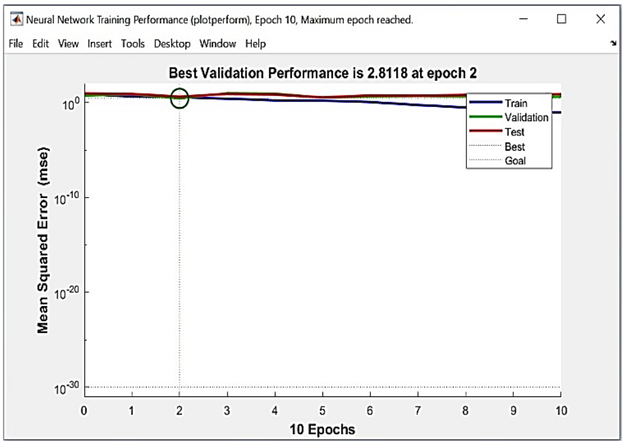
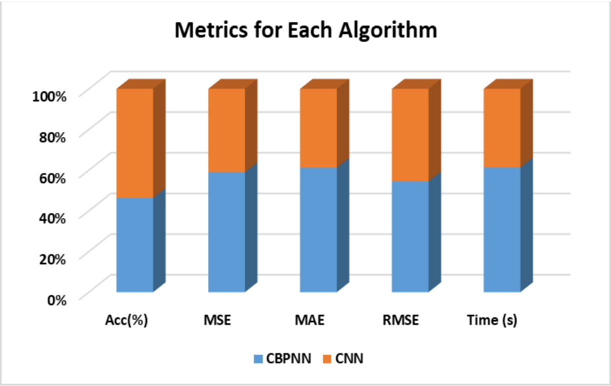

Neural Network Training Performance (plotperform), Epoch 10, Maximum epoch reached.
File Edit View Insert Tools Desktop Window Help
Best Validation Performance is 2.8118 at epoch 2
Mean Squared Error (mse)
10^0
10^-10
10^-20
10^-30
0
1
2
3
4
5
6
7
8
9
10
10 Epochs
Train
Validation
Test
Best
Goal

Fig 8. Optimal Validation Goal for CNN Model Performance.

4.2 Comparative Performance Metrics

The baseline performance of both models is presented in Figure 9 where accuracy, MSE, MAE and RMSE are used to perform comparative evaluation. The CNN model achieved better results than the CBPNN under all conditions demonstrating the robustness and reliability of its use for intrusion detection problems.



4.3 Computational Efficiency

The hybrid IDS in the paper demonstrated significant computational efficiency. The CNN model trained in 17 s, and the training time of the CBPNN model was 27 s. This performance improvement is due to optimizations of the architecture and the utilization of thinner but powerful configurations of neural networks. This efficiency is especially important for real-time application in IoT applications in which fast response and low delay are required.

4.4 Adaptive Mechanisms

For improved detection accuracy and to minimize false alarms, the IDS incorporates adaptive thresholding schemes. These thresholds adaptively change based on traffic levels and attack densities. For instance, in case that the network is busy, the system can automatically reduce the detection threshold to increase the response time while still controlling the rate of false alarms. This flexibility leads to a more responsive architecture that acts contextually and adaptively, enhancing the system to the rise of new cyber threats.

5. DISCUSSION

The hybrid IDS, proposed in this paper, which combines CBPNN and CNN, has shown significant advantages on detecting and alleviating the cyber-attacks of IoT. The CNN model performed significantly better with 90% accuracy and a detection rate (DR) 99% through an exhaustive analysis compared to the CBPNN model, which obtained only an accuracy of 82%. These findings demonstrate the effectiveness of using DNN techniques that are designed to adapt to complex and volatile IoT network traffic. The results are compatible with previous studies that underscores the importance to have scalable, efficient and adaptive IDS in IoT environments. Offering inclusion of strong machine learning models, the proposed system improves the security of the IoT networks and can be contributing to the ongoing efforts to secure the ecosystems from the wide gamut of cyber threats.

5.1 Comparison Between the Proposed Model and Existing Studies

To show the efficiency of the hybrid IDS, especially the CNN model, we performed comparison experiments on KDDTest-21 [28][32-34]. In this comparison, the performance of proposed CNN architecture was compared with a number of traditional machine learning techniques with special interest on detection of DDoS attacks. Before training, we transformed input features, protocol type, service, and flags from nominals to numericals by pre-processing, to fit better to the flow of machine learning processes. 92% and a detection rate of 99% after 10 training epochs, which greatly outperforms hand-crafted methods. The comparative results are presented in Table V.

TABLE V: COMPARISON OF THE CNN ALGORITHM WITH OTHER STUDIES USING THE KDDTEST-21 DATASET

Ref.	Algorithm	Attack Type	Accuracy (%)	FPR (%)	DR (%)
[29]	RNN	DDoS	68%	2.0%	83%
[30]	BLSTM / DBN	DDoS	75% / 66%	19% / 22%	67% / 54%
[31]	CNN	DDoS	77%	16%	80%
*	Proposed CNN	DDoS	**90%**	**2.0%**	**99%**

The comparison results indicate that the proposed CNN-based IDS outperforms other models in the accuracy of detection and false positive rate. The proposed scheme demonstrates significant improvement when compared to the CNN model in [31], which achieved an accuracy of 77% and DR of 80%.
Several primary enhancements are added for this improvement:

a) Super Learning Methodology: The CNN model used a super training method with programmed for conducting rigorous pre-processing on the images, which thereby significantly improved the feature extraction and filter out noise, leading to an improved accuracy.
b) Adaptive Threshold Mechanisms: Our approach has real-time adaptive mechanisms for threshold tuning based on the observed traffic behavior which enhances the reactivity and reduces false positives.
c) Hyperparameter Optimization - The fine-tuning of learning rates, batch sizes, and epochs allowed for a faster convergence, reduced over fitting and increased robustness of the model.
d) Comprehensive evaluation measure: Beyond accuracy and detection rate, the proposed study gave high importance to minimizing the False Positive Rate (FPR), a critical concern for practical applications.

When these features are integrated, a complete and scalable solution for IoT intrusion detection emerges. They exhibit not only higher accuracy, but also adaptability and efficiency — which are crucial for use in real-time, resource-bounded IoT applications. The experimental results demonstrate that the proposed CNN model outperforms state-of-the art techniques and provides a significant contribution to intrusion detection in the new IoT systems.

6. CONCLUSION

This paper provides a detailed analysis of the consolidated Intrusion Detection System (IDS) which is an improved security mechanism implemented in the IoT network to enhance their resistance against the increasing sophistication of cyber threats. The proposed methodology combines the CBPNN and CNN models to holistically detect and respond to intrusions within the dynamic IoT networks. The performance comparison shows that the CNN model is superior to the CBPNN, the accuracy of detection is as high as 90% and the detection rate is 99%, especially for the ability to detect Distributed Denial of Service (DDoS) attacks. The findings verify the efficiency of the deep learning methods in the case of intrusion detection problem, as well as the importance of preprocessing and model fine-tuning. Comparison with current approaches emphasizes the high-performance potential of the proposed CNN-based IDS in in accuracy, false positive mitigation and complexity. This work additionally highlights the demand from scalable and flexible IDS schemes which offer the potential to adapt to the evolution of the real-time network surroundings. Further work could consider using ensemble and reinforcement learning techniques, adaptive thresholding dynamics, and more general use-cases in different IoT settings, including healthcare, industrial systems, and smart cities. In general, the hybrid IDS proposed in this work is a clear step toward resilient and intelligent IoT security systems.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment

Non.

References

[1] A. A. Megantara and T. Ahmad, “A hybrid machine learning method for increasing the performance of network intrusion detection systems,” Journal of Big Data, vol. 8, no. 1, pp. 1–19, 2023.

[2] J. F. Yonan and N. A. A. Zahra, “Node intrusion tendency recognition using network level features based deep learning approach,” Babylonian Journal of Networking, vol. 2023, pp. 1–10, Jan. 2023, doi: 10.58496/bjn/2023/001.

[3] Z. Abboud and J. F. Yonan, “Driver drowsy and yawn system alert using deep cascade convolution neural network (DCCNN),” Iraqi Journal for Computer Science and Mathematics, pp. 111–120, Oct. 2023, doi: 10.52866/ijcsm.2023.04.04.010.

[4] H. Liao, M. Z. Murah, M. K. Hasan, A. H. M. Aman, J. Fang, X. Hu, and A. U. R. Khan, “A survey of deep learning technologies for intrusion detection in Internet of Things,” IEEE Access, 2024.

[5] K. DeMedeiros, A. Hendawi, and M. Alvarez, “A survey of AI-based anomaly detection in IoT and sensor networks,” Sensors, vol. 23, no. 3, p. 1352, 2023.

[6] M. Markevych and M. Dawson, “A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (AI),” in Proc. Int. Conf. Knowledge-Based Organization, vol. 29, no. 3, pp. 30–37, 2023.

[7] S. S. Qasim and S. M. Nsaif, “Advancements in time series-based detection systems for distributed denial-of-service (DDoS) attacks: A comprehensive review,” Babylonian Journal of Networking, vol. 2024, pp. 9–17, Jan. 2024, doi: 10.58496/bjn/2024/002.

[8] B. Sharma et al., “A critical analysis of IDS for IoT networks by incorporating deep learning approach with explainable AI (XAI),” Journal of Network and Computer Applications, vol. 210, p. 102999, 2023, doi: 10.1016/j.jnca.2022.102999.

[9] Z. Sun et al., “Improving IDS in the Internet of Medical Things (IoMT) using machine learning algorithms,” Journal of Medical Systems, 2023, doi: 10.1007/s10916-023-02101-3.

[10] S. Ali et al., “Wireless sensor network security in edge-enabled industrial IoT devices using a blockchain, federated learning-based IDS hybrid architecture,” Computers & Security, vol. 121, p. 102817, 2023, doi: 10.1016/j.cose.2023.102817.

[11] E. Selvan et al., “A hybrid optimization method including deep Q networks for network intrusion detection,” Future Generation Computer Systems, vol. 136, pp. 204–216, 2023, doi: 10.1016/j.future.2022.09.032.

[12] F. Alwahedi et al., “Generative AI and large language models in IoT security,” Journal of Information Security and Applications, vol. 70, p. 103289, 2023, doi: 10.1016/j.jisa.2023.103289.

[13] H. Liao et al., “Deep learning methods for IoT intrusion detection,” IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3456–3467, 2023, doi: 10.1109/JIOT.2022.3148254.

[14] M. Nanjappan, “DeepLG SecNet: LSTM and GRU for IoT intrusion detection,” IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2458–2468, 2023, doi: 10.1109/TNSM.2023.3285448.

[15] G. S. C. Kumar and A. Binbusayyis, “Deep residual convolutional neural networks for intrusion detection systems,” Information Sciences, vol. 658, pp. 175–186, 2023, doi: 10.1016/j.ins.2023.04.052.

[16] Gaganjot et al., “Intrusion detection in fog-cloud environments using hybrid architecture,” Journal of Systems and Software, vol. 208, p. 111171, 2023, doi: 10.1016/j.jss.2023.111171.

[17] L. D. Manocchio et al., “Flow Transformer: A transformer-based intrusion detection system architecture,” ACM Transactions on Internet Technology, vol. 23, no. 2, p. 12, 2023, doi: 10.1145/3550130.

[18] A. A. Megantara and T. Ahmad, “Enhancing the performance of IDS in IoT networks using hybrid machine learning methodology,” Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 5, pp. 2591–2605, 2023, doi: 10.1007/s12652-021-03583-0.

[19] G. Perumal et al., “VBQ-Net: A vectorization-based boosted quantized network model for enhancing IoT security,” IEEE Transactions on Industrial Informatics, vol. 19, no. 6, pp. 3951–3960, 2023, doi: 10.1109/TII.2023.3248679.

[20] A. Mahalingam et al., “ROAST-IoT: An attention-based convolutional network for IoT security,” Sensors, vol. 23, no. 19, p. 8044, 2023, doi: 10.3390/s23198044.

[21] H. Liao et al., “A survey of deep learning technologies for IoT intrusion detection,” IEEE Access, vol. 11, pp. 25742–25763, 2023, doi: 10.1109/ACCESS.2023.3234567.

[22] D. Abu Laila, “Responsive machine learning framework and lightweight utensil of prevention of evasion attacks in the IoT-based IDS,” STAP Journal of Security Risk Management, vol. 2025, no. 1, pp. 59–70, 2025, doi: 10.63180/jsrm.thestap.2025.1.3.

[23] A. Ali, “Adaptive and context-aware authentication framework using edge AI and blockchain in future vehicular networks,” STAP Journal of Security Risk Management, vol. 2024, no. 1, pp. 45–56, 2024, doi: 10.63180/jsrm.thestap.2024.1.3.

[24] Q. Al-Na’amneh, M. Aljawarneh, A. S. Alhazaimeh, R. Hazaymih, and S. M. Shah, “Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments,” STAP Journal of Security Risk Management, vol. 2025, no. 1, pp. 85–114, 2025, doi: 10.63180/jsrm.thestap.2025.1.

[25] M. Almaayah and R. B. Sulaiman, “Cyber risk management in the Internet of Things: Frameworks, models, and best practices,” STAP Journal of Security Risk Management, vol. 2024, no. 1, pp. 3–23, 2024, doi: 10.63180/jsrm.thestap.2024.1.1.

[26] S. Alsahaim and M. Maayah, “Analyzing cybersecurity threats on mobile phones,” STAP Journal of Security Risk Management, vol. 2023, no. 1, pp. 3–19, Aug. 2023, doi: 10.63180/jsrm.thestap.2023.1.2.

[27] R. Almanasir et al., “Classification of threats and countermeasures of cloud computing,” Journal of Cyber Security and Risk Auditing, vol. 2025, no. 2, pp. 27–42, 2025, doi: 10.63180/jcsra.thestap.2025.2.3.

[28] A. A. Almuqren, “Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions,” Journal of Cyber Security and Risk Auditing, vol. 1, no. 1, pp. 1–11, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.1.1.

[29] R. S. Mousa and R. Shehab, “Applying risk analysis for determining threats and countermeasures in workstation domain,” Journal of Cyber Security and Risk Auditing, vol. 2025, no. 1, pp. 12–21, Jan. 2025, doi: 10.63180/jcsra.thestap.2025.1.2.

[30] S. R. Addula and A. Ali, “A novel permissioned blockchain approach for scalable and privacy-preserving IoT authentication,” Journal of Cyber Security and Risk Auditing, vol. 2025, no. 4, pp. 222–237, 2025, doi: 10.63180/jcsra.thestap.2025.4.3.

[31] S. Sheeja and J. Joseph, “A three-layer CNN-based intrusion detection system for IoT networks,” International Journal of Computing and Digital Systems, vol. 12, no. 2, pp. 95–104, 2023, doi: 10.12785/ijcds/120201.

[32] O. Jaupi and E. Spaho, “A systematic literature review on integrating VANETs, VDTNs, 5G, and IoT for smart cities: Current approaches, challenges, and future directions,” Journal of Transactions in Systems Engineering, vol. 3, no. 3, pp. 420–448, 2025, doi: 10.15157/JTSE.2025.3.3.420-448.

[33] G. L. Sravanthi and R. Mandava, “AI-enabled distributed cloud frameworks for big data analytics with privacy preservation,” Journal of Transactions in Systems Engineering, vol. 3, no. 3, pp. 449–470, 2025, doi: 10.15157/JTSE.2025.3.3.449-470.

[34] Y. K. Aluri and S. Tamilselvan, “Machine learning-driven cross-layer IDS architecture for next-generation IoT networks,” International Journal of Innovative Technology and Interdisciplinary Sciences, vol. 8, no. 3, pp. 707–733, 2025, doi: 10.15157/IJITIS.2025.8.3.707-733.