International Journal of Advanced Technology and Engineering Exploration, Vol 11(120)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2024.111100172

Research Article

Hybrid IDS architecture for IoT security enhancing threat detection with CPBNN and CNN models

Taha S. Alashkar*
Medical Instrumentation Engineering Department, Al-Esraa University, Baghdad, Iraq

Received: 16-February-2024; Revised: 15-November-2024; Accepted: 19-November-2024

Abstract
The rising frequency of cyberattacks, especially those targeting critical infrastructure, highlights the urgent need for robust network intrusion detection systems (IDS) specifically designed for the internet of things (IoT). Security issues in IoT networks are particularly complex due to the large number of connected devices and the emergence of new, sophisticated threats. To address these challenges, this research proposes a hybrid IDS architecture that combines machine learning (ML) and neural network (NN) approaches, leveraging cascade backpropagation neural networks (CPBNN) and convolutional neural networks (CNN) to enhance IoT security. The proposed system is designed to identify vulnerabilities in IoT systems, including distributed denial of service (DDoS) attacks, while addressing specific challenges related to scalability and the inherent complexity of IoT networks. The methodology employs a dual-layered approach: CPBNN is used to detect anomalous traffic, focusing on identifying abnormal behaviors, while CNN distinguishes between different types of traffic to determine the nature of the identified anomalies. The proposed hybrid IDS is evaluated using the KDDTest-21 dataset and assessed based on performance metrics including accuracy, precision, recall, and F1-score. Experimental results demonstrate that the hybrid IDS achieves an accuracy of 90% with the CNN model and 82% with the CPBNN model, confirming its effectiveness in detecting and mitigating IoT-specific security threats. These findings highlight the importance of integrating advanced ML techniques to safeguard IoT networks against evolving threats.

Keywords
Cascade backpropagation neural network (CPBNN), Convolutional neural network (CNN), KDDTest- 21, Distributed denial of service (DDoS) attacks, Intrusion detection system (IDS), IoT security.

1.Introduction
The Internet of things (IoT) has rapidly expanded, transforming healthcare, industrial processes, smart cities, and numerous other sectors by connecting billions of devices worldwide. While these systems have revolutionized the internet, their extensive connectivity has introduced significant security challenges, making IoT networks vulnerable to cyber threats. IoT networks are particularly insecure due to factors such as resource constraints, heterogeneity, and distributed architectures, which make them susceptible to sophisticated attacks like distributed denial of service (DDoS) and malware [1]. The evolving complexity and intensity of these threats further complicate the implementation of effective security mechanisms for IoT systems [2].

The traditional security paradigm for IoT, which includes encryption, authentication, and access control, has proven inadequate when applied in isolation, particularly against large-scale coordinated attacks [3]. Consequently, safeguarding IoT networks has increasingly focused on intrusion detection systems (IDS). Specifically, machine learning (ML) and neural network (NN) techniques have been widely adopted to develop IDS capable of identifying anomalous behaviors and detecting attacks [4]. However, existing IDS methods face several challenges, including scalability issues, handling high-dimensional data, and adapting to emerging threats effectively [3–5].

Several works have been made to address these difficulties through different artificial intelligence (AI) techniques. For instance, integrated deep learning (DL) with explainable AI (XAI) to enhance IDS for IoT networks; however, this approach introduced significant challenges, including high

*Author for correspondence

computational complexity [5]. Similarly, employed ML techniques to improve security in the internet of medical things (IoMT), demonstrating improved detection rates but failing to provide the stability required for real-time threat detection against more sophisticated attacks [6]. Another study [7] proposed a hardware-software optimization combined with deep Q-networks for intrusion detection. However, these models demanded substantial computational resources, rendering them less suitable for resource-constrained IoT devices.

This study seeks to develop a dual-layered hybrid IDS framework to address the increasing number of IoT devices and their associated security challenges. The framework utilizing cascade backpropagation neural networks (CPBNN) for anomaly detection and convolutional neural networks (CNN) for traffic classification. The primary objective is to enhance the detection rates of IoT network intrusions while minimizing false positives and false negatives (FN). The research presents an innovative framework that integrates the strengths of CPBNN and CNN, with their performance evaluated using the KDDTest-21 dataset. Key contributions include the development of the dual-layered hybrid IDS framework, a comprehensive assessment of its performance against traditional IDS approaches, and valuable insights into the system's scalability and adaptability to evolving cyber threats.

The remainder of this paper is structured as follows: Section 2 provides a review of related literature. Section 3 details the proposed detection methodology, including the IDS architecture and the roles of CPBNN and CNN. Section 4 presents the experimental results and performance analysis. Discussion of results and comparative analysis have been elaborated in Section 5. Finally, Section 6 concludes the paper with a summary and suggestions for future research directions.

2.Literature review

The security of IoT networks has been a center of significant research, and many techniques have been proposed to enhance the performance and reliability of the IDS. Since the IoT networks are complex, the IDS have generally integrated ML and DL techniques for identifying and counteracting cyber threats. This section presents important findings that recent literature provides, especially highlighting the used methods, obtained results, strengths, and weaknesses.

In [8], a critical evaluation of IDS for IoT networks was conducted by integrating a DL methodology with XAI. This approach improved decision-making by allowing security specialists to analyze the model's behavior. While the methodology achieved an accuracy of 93.05%, the high complexity and resource requirements made the model impractical for resource-constrained IoT devices.

In [9], ML techniques were employed to enhance IDS in the IoMT. The proposed approach achieved a detection accuracy of 90.76%, demonstrating the effectiveness of ML in securing medical IoT networks. However, the approach faced challenges in delivering real-time processing capabilities, which are critical in healthcare environments where prompt responses are essential.

In [10], a security framework for wireless sensor networks (WSN) in edge-enabled industrial IoT devices is suggested, using a hybrid architecture that incorporates blockchain and federated learning-based IDS. Their solution has shown considerable efficacy in augmenting security while also reducing delay. Nonetheless, the primary drawback of scalability was revealed, suggesting that managing an increased number of devices is only feasible on a large scale for industrial IoT applications.

The research on IDS [11] proposed a hybrid optimization approach that integrates deep Q-networks. Consequently, their strategy continues to provide fewer false positives while enhancing the accuracy of true result detection. Nevertheless, the computing resources required by the model hindered the development of extensive IoT systems, since such resources may be limited in these contexts.

In [12], researchers investigated the application of generative AI and large language models to improve IoT security. The study showcased how AI could address intricate security challenges, especially by incorporating self-organizing response systems. However, a notable concern was the risk posed by excessive automation, which could exacerbate vulnerabilities in the face of evolving cyberattack dynamics.

DL techniques, such as CNNs and recurrent neural network (RNN), were evaluated and analyzed by [13] to enhance IoT intrusion detection. The analyzed models demonstrated elevated detection rates but exhibited various limitations, mostly regarding the substantial training data requirements and the

restricted interpretability, which may impede the practical deployment of the associated systems.

In [14], introduced DeepLG SecNet, a model that integrates long short-term memory (LSTM) and gated recurrent units (GRU) within the IoT context to enhance the accuracy of IDS. The proposed framework demonstrated improvements in both detection performance and speed. However, further advancements were needed to optimize the model's speed for large-scale applications and to reduce the computational burden in subsequent stages.

Deep residual CNN were examined for IDS by [15]. Overall, their models exhibited an efficiency of 92% and focused on anomaly detection; however, the need for extensive data preparation and resources rendered the models unfeasible for low-powered IoT devices.

In [16], a study focused on IDS within fog-cloud environments proposed a hybrid architecture combining VGG19 and 2D-CNN, showcasing an advanced approach to enhancing intrusion detection capabilities in such settings. The hybrid model's efficacy was confirmed to maintain stability in addressing detection rates. Nonetheless, several challenges associated with the use of the method for real-time processing and the resultant computing burden were noted, particularly within the IoT environment.

In [17], a flow transformer—a transformer-based IDS design—was introduced, demonstrating improved detection accuracy and scalability in IoT networks. Despite its promising results, further testing across diverse IoT scenarios was required to evaluate its robustness.

In [18], researchers proposed a mixed ML approach to enhance the effectiveness of IDS in IoT networks. Their model achieved a high accuracy rate of 95.12%, significantly improving the detection of malicious activities compared to existing systems. However, the approach faced challenges, particularly the substantial computational costs associated with training large datasets, which can be problematic in distributed IoT networks with limited processing capabilities.

In [19], vectorization-based boosted quantized network (VBQ-Net), a VBQ-Net model, was proposed to strengthen the security of IoT devices. The method demonstrated its effectiveness by improving detection capabilities. Nevertheless, it faced challenges in adapting to rapidly evolving threats, highlighting the need for a more flexible and adaptable model.

In [20], an attention-based CNN model called the range-optimized attention convolutional scattered technique -IoT (ROAST-IoT) was proposed to enhance IoT security. The model demonstrated significant improvements in detection accuracy and time efficiency, particularly in real-time detection scenarios. However, additional validation was required to establish its effectiveness in large-scale, generic IoT systems operating within complex and heterogeneous environments.

In the study on DL methods for IoT intrusion detection [21], it was observed that CNN and RNN models play an increasingly critical role in achieving high detection accuracy. However, the research highlighted key limitations, including explainability issues and the requirement for extensive labeled training data, which hinder practical deployment in dynamic IoT environments.

In [22], a three-layer CNN-based IDS was introduced for IoT networks, achieving a detection accuracy of 94.65%. While the approach significantly improved detection capabilities, it exhibited high false positive rates in dynamic environments, limiting its suitability for real-time applications.

In [23], ML techniques were applied to detect DDoS attacks on IoT networks. The approach demonstrated notable precision improvements, particularly in handling large-scale DDoS attacks. However, scalability remained a significant challenge, especially in complex IoT ecosystems with diverse network conditions.

In [24], an AI-driven detection framework for IoT security based on reinforcement learning was developed. The system achieved a detection accuracy of 92.8%, demonstrating robustness against both known and emerging attacks. However, optimization was necessary to reduce computational complexity for large-scale IoT deployments.

In [25], statistical analysis was used to evaluate IDS performance with ML techniques on the KDDS-001 dataset. The approach achieved an accuracy of 91.2% but struggled with identifying zero-day threats, a critical feature for modern IoT security frameworks.

In [26], an AI-enhanced IDS for industrial IoT security was proposed, attaining an accuracy of 93.4%. While resilient against various cyber threats, the system was insufficiently fast for large-scale networks, with significant computational demands, making scalability a primary concern.

In [27], an IDS for IoT networks was designed using a support vector machine-particle swarm optimization (SVM-PSO) classification model that leveraged telemetry data. The method achieved a detection rate of 89.7%, improving the performance of SVM for IDS. However, the system required further refinement to support real-time processing, as high-velocity data streams in IoT networks necessitate continuous optimization.

Table 1 provides a concise overview of recent research in IDS advancements for IoT security, summarizing the techniques, outcomes, strengths, and weaknesses of each approach. The findings indicate progress in detection accuracy, scalability, and computational efficiency. However, challenges persist in real-time detection and resource utilization, emphasizing the need for continued innovation.

Table 1 Summary of recent studies on IDS for IoT security

Study	Method	Results	Advantages	Limitations
[8]	DL + XAI	Accuracy: 93.05%	Improved transparency and high accuracy	Complexity and high computational demand
[9]	ML for IoMT	Accuracy: 90.76%	Enhanced detection rates	Real-time processing issues
[10]	Blockchain + Federated Learning IDS	Improved security	Reduced latency	Scalability issues
[11]	Hybrid optimization + deep Q-network	Reduced false positives and high accuracy	Reduced false positives and enhanced detection	High computational resource requirements
[12]	Generative AI + Large language models	Highlighted future AI trends	Future trends	Over-reliance on automation
[13]	CNNs and RNNs for IoT IDS	High detection rates	Effective for DL models	Extensive training data required and interpretability
[14]	Deep LSTM + GRU	Improved detection speed	Enhanced accuracy	Large-scale deployment challenges
[15]	Deep Residual CNN	High efficiency	Anomaly detection success	High computational and preprocessing needs
[16]	VGG19 + 2D-CNN Hybrid	Improved robustness	Robust detection rates	High computational overhead
[17]	Transformer-based IDS (flow transformer)	Enhanced accuracy scalability	Improved scalability	Requires further testing
[18]	Hybrid ML	95.12% Accuracy	Enhanced performance in IDS	High computational cost
[19]	VBQ-Net for IoT Security	Notable detection improvements	Improved security	Adaptation to evolving threats
[20]	ROAST-IoT	Improved accuracy and speed	Enhanced IoT security	Needs further validation
[21]	Three-layer CNN for IoT	Accuracy: 94.65%	Effective for IoT security	High false positive rates
[22]	ML for DDoS Detection	Improved accuracy	Suitable for DDoS detection	Scalability issues in complex environments

3.Methodology

The proposed methodology involves the installation and deployment of a two-tier IDS comprising a CBPNN model and a CNN model. These models aim to enhance the detection of intrusions by utilizing ML algorithms on raw data from the KDDTest-21 dataset. All models were trained in MATLAB, with the training configuration settings detailed in *Table 2*. Prior to applying the ML algorithms, data preprocessing was performed on the dataset, as illustrated in *Figure 1*. The data represents activity from a network exposed to potential intrusions, with the axes depicting time and the probability of abnormal behavior. Significant fluctuations may indicate potential network scanning, denial-of-service

attacks, or exploitation attempts. Cyclical peaks suggest periodic attack patterns, while lower values typically reflect normal network behavior.

Table 2 Configurations of ML models

Particle	Details
Training Method	Supervised learning
Number of Epochs	100
Maximum Gradient	1×10^{-30}
Mean squared error (MSE)	1×10^{-30}
Kinds of ML Models	CBPNN, CNN
Number of Test Sets	10

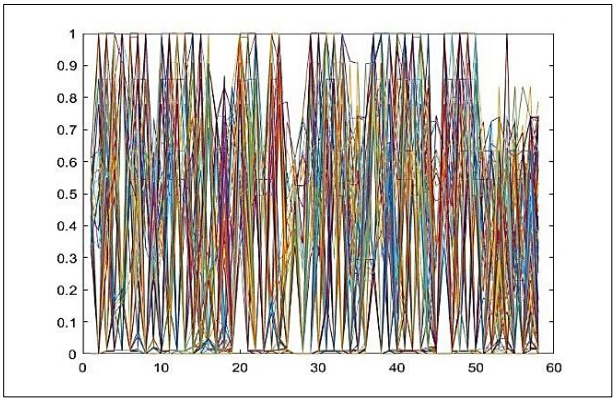


Figure 1 Dataset after processing for training

3.1Implement of CBPNN & CNN algorithms

Subsequently, data processing for the IDS training is achieved by using two ML models: CBPNN and CNN. In order to improve the overall detection accuracy of the CBPNN algorithm, it uses a multilayer architecture that is optimised for the identification of patterns characteristic of network invasions.

3.1.1Cascade backpropagation neural network (CBPNN) design

The CBPNN is designed to improve the detection and classification of network anomalies, specifically tailored for IoT environments. The architecture consists of multiple layers, each serving a specific purpose:

1. The input layer consists of 500 neurons, recollecting the input features formed from the processed data. This layer enables the network to handle high-dimensional features to identify anomalous traffic in IoT.
2. The proposed network consists of 10 sets of neurons. These layers are designed to learn complex patterns and relationships that are essential for distinguishing between normal and malicious traffic.
3. The output layer provides the final prediction, indicating whether the network traffic is normal or an attack.
4. The network structure incorporates a random distribution of nodes to emulate the dynamics of IoT nodes, particularly focusing on "DDoS" nodes, which represent points of DDoS attacks. This design enables a detailed analysis of specific vulnerabilities within the network.

The proposed CBPNN framework distinguishes itself through its innovative design, which combines the strengths of traditional backpropagation techniques with the flexibility of a cascade structure. This design is implemented and visualized using MATLAB-GUI, with the model configuration illustrated in *Figure 2*. The framework allows for the progressive addition of nodes and layers during the learning process, enabling the model to dynamically adapt to the complexities of IoT network traffic. Unlike previous approaches that rely on fixed architectures, the adaptable structure of the CBPNN enhances detection capabilities and minimizes the risk of overfitting by supporting incremental learning.

Additionally, *Figure 3* presents a flowchart of the CBPNN algorithm. By leveraging this CBPNN framework, the proposed model significantly improves the effectiveness of intrusion detection in IoT networks. It addresses critical challenges such as high-dimensional data processing and the need for adaptability to evolving cyber threats.

3.1.2Convolutional neural network (CNN) design

CNN is specifically designed to improve the classification of network traffic by leveraging learned patterns. The architecture of the CNN model shares similarities with that of the CBPNN but is tailored to optimize traffic classification in IoT environments. The CNN architecture consists of the following layers:

1. Input Layer: Comprises 500 neurons designed to receive the input features.
2. Hidden Layers: The model includes fully connected layers, each with 10 units, to capture and learn subtle features of the network traffic data.
3. Output Layer: Generates classification outputs, indicating the presence or absence of an attack.

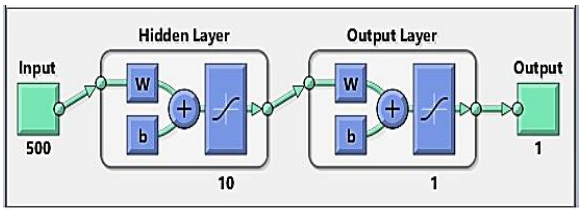


Figure 2 Design of the CBPNN algorithm

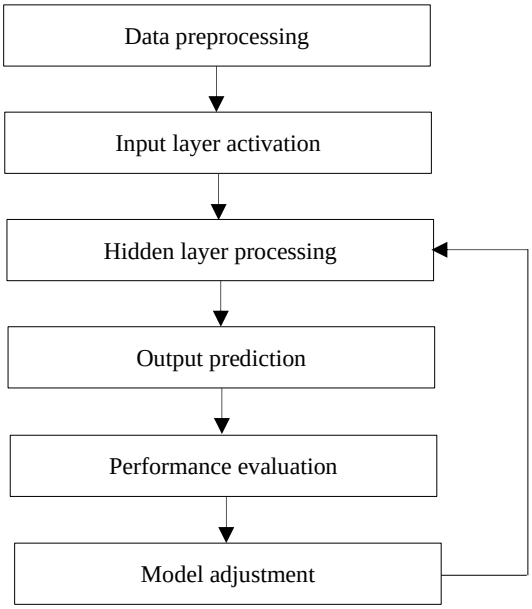


Figure 3 Flowchart of the CBPNN algorithm

The nodes in the CNN architecture are randomly set, with four nodes allocated for DDoS conditions, as shown in *Figure 4*. This configuration enables the CNN model to effectively identify various forms of cyberattacks commonly occurring in IoT networks.

The proposed CNN framework offers several novel features compared to previous methods. It uses dynamic node configurations to simulate the dynamic nature of IoT networks, enhancing its versatility in detecting a wider range of attacks. The architecture is specifically designed to address the unique characteristics of IoT traffic, learning and adapting to the data types typically encountered in IoT environments, thereby improving classification accuracy. The flowchart of the CNN algorithm is depicted in *Figure 5*.

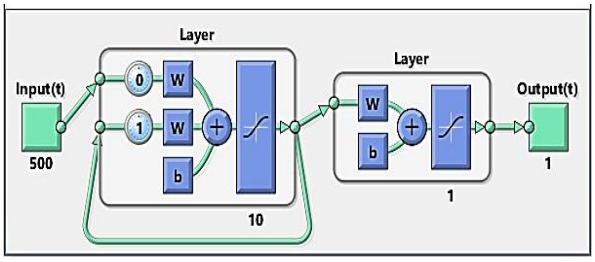


Figure 4 Design of the CNN algorithm

3.2Training and evaluation

During the training and evaluation of the proposed hybrid IDS, the CBPNN and CNN models are applied to the processed dataset. The preprocessing phase involves cleaning and transforming raw data obtained from packet captures. This process includes selecting relevant features, such as protocol type, service, and flags, and extracting them to create a high-dimensional dataset suitable for ML applications.

The performance of each model is evaluated using key metrics, including accuracy, detection rate, and false positive rate. The selection of the CBPNN and CNN algorithms is based on their demonstrated effectiveness in processing complex, high-dimensional data, making them particularly well-suited for detecting anomalies in IoT environments.

The dataset is partitioned into training, validation, and test sets to ensure a thorough evaluation and to mitigate overfitting. The training set is used to train the model, the validation set is employed to fine-tune hyperparameters and select the optimal model, and the test set is reserved for an unbiased assessment of the model's performance. Techniques such as cross-validation and early stopping are employed to mitigate overfitting and enhance the model's generalizability to unseen data. *Figure 6* shows the results of CBPNN and CNN algorithms

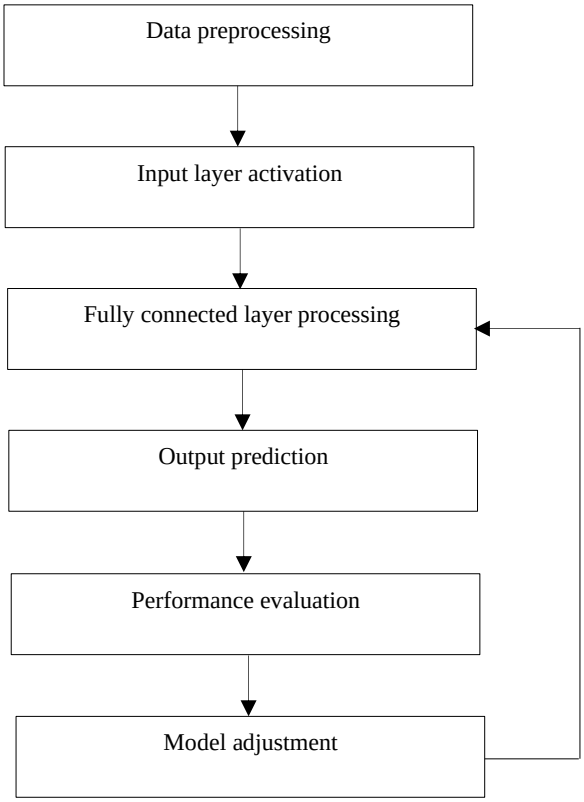


Figure 5 Flowchart of the CNN algorithm

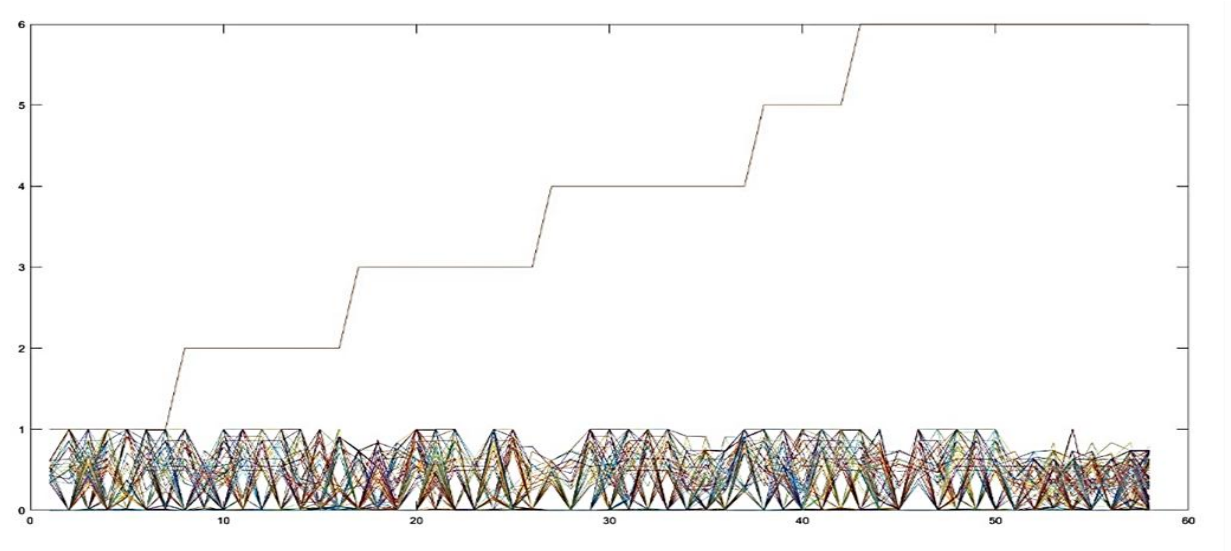


Figure 6 Results of CBPNN and CNN algorithms

Figure 6 is composed of two distinct components: a lower section with dense lines illustrating detailed network activity data, and an upper section featuring a stepped line that represents a cumulative metric. The lower portion highlights areas of intensive data activity, while the upper stepped line provides a higher-level overview, potentially indicating threat levels, system updates, or significant events. This dual representation—combining granular data with a summarized view—can be instrumental in identifying real-time trends, such as emerging threats and patterns in network activity.

The proposed model assesses the effectiveness of the IDS using performance metrics for intrusion detection, including:

1. True positive (TP): The number of records accurately identified as abnormal.
2. False positive (FP): The normal sample records that will be incorrectly classified as abnormal samples.
3. True negative (TN): This is the number of normal records an IDS correctly assigned in a given database.
4. FN: The number of abnormal records wrongly classified as normal.

The metrics used for the evaluation of the proposed work are as under:

1.Accuracy: Express as the proportion of the classification success rate to the total record strength (Equation 1).

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

2.Detection rate: It is commonly referred to as the precision rate, which represents the ratio of records correctly identified as abnormal to the total number of predicted abnormal records (Equation 2).

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

3.False positive rate: It indicates the percentage of incorrectly rejected normal records relative to the total number of normal records (Equation 3).

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

The threshold values for detection were determined based on empirical results and adjusted to optimize performance metrics. The impact of different threshold settings on the accuracy, detection rate, and false positive rate is analyzed to ensure optimal performance across varying network conditions and attack types.

Evaluating the efficiency of an IDS is centered on achieving key objectives: maximizing the detection rate and accuracy while minimizing the false positive rate. The proposed hybrid IDS system provides a robust solution for enhancing the security of IoT networks against emerging cyber threats.

4.Experimental result

The dataset used, KDDTest-21 [28], includes features such as protocol type, service flags, and connection duration. It encompasses a diverse set of attributes designed for IoT networks, with values reflecting various network behaviors, including both normal

and malicious activities. The range of feature values facilitates comprehensive analysis, improving model training and validation. The NSL-KDD dataset [28] is an updated version of the original KDD dataset, containing 41 features that describe each connection in the dataset. These features provide detailed information about each connection, while the labeling feature indicates whether the connection is normal or under threat by identifying the specific type of attack.

To assess the proposed hybrid IDS, the CBPNN and CNN models were utilized in this study. The capabilities of these algorithms were evaluated based on K-fold cross-validation; a robust technique that helps ensure the reliability of the results by partitioning the dataset into K subsets. *Tables 3* and *4* summarizes the evaluation metrics and results for the proposed hybrid IDS model. It details the validation process, performance metrics, and runtime of the system.

Table 3 Performance metrics and results of the CBPNN model

Metrics	Results
Validation	K-fold
Observations number	58 observations
Test sets	10 test sets
Accuracy	82%
MSE	1.4138
Mean absolute error (MAE)	0.512
Root mean squared error (RMSE)	1.189
Runtime	27s

Table 4 Performance metrics and results of the CNN model

Metrics	Results
Validation	K-fold
Observations number	50 observations
Test sets	10 test sets
Accuracy	90%
MSE	0.988
MAE	0.327
RMSE	0.991
Runtime	17s

The results indicate that the CNN algorithm outperformed the CBPNN in terms of detection accuracy and processing time. Specifically, the CNN achieved a detection accuracy of 90% within a runtime of 17 seconds, making it the most effective algorithm among the models tested. This improvement in performance highlights CNN ability to learn complex patterns in network traffic, which is essential for identifying malicious activities.

4.1Analysis of detection capabilities

The analysis of detection capabilities revealed that the CNN model excelled in identifying DDoS attacks, as evidenced by its accuracy of 90% and efficient detection time. *Figure 7* illustrates the performance metrics of the CNN model, including a gradient weight of 1.1567 and a validation score measured across 8 positions at an epoch value of 10. Notably, the validation checks at positions 0 and 2 failed to validate the CNN algorithm, highlighting areas that require further optimization for potential improvement.

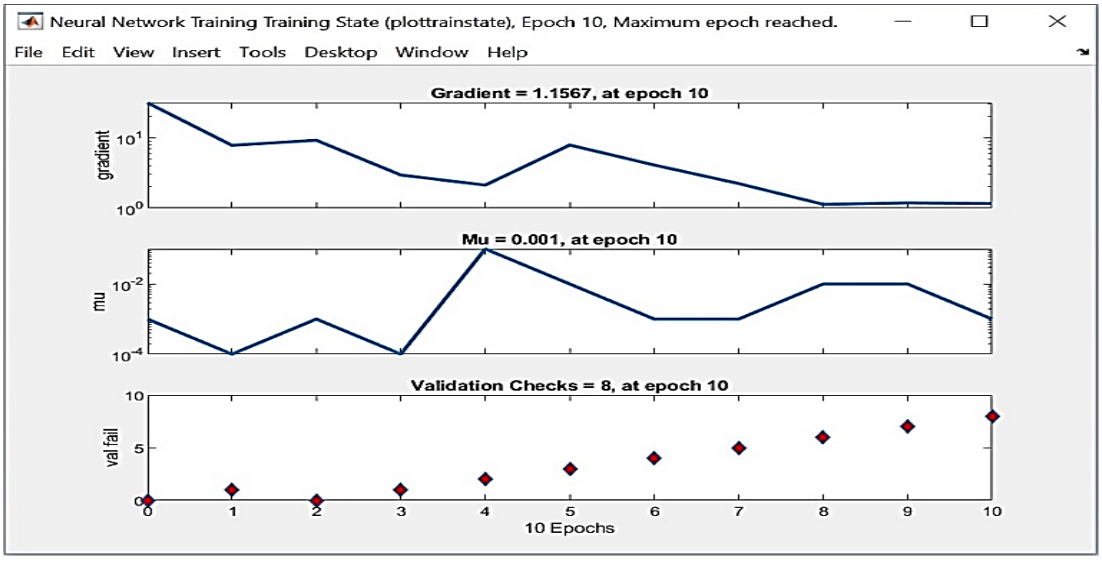


Figure 7 Training state of the CNN model

Furthermore, the MSE was utilized to measure the validation accuracy of the algorithms. As shown in *Figure 8*, the CNN model achieves its lowest validation loss and the highest validation accuracy of 2.8118 at epoch 2, indicating a well-balanced trade-off between detection speed and validation accuracy. The figure also highlights the training and validation lines, which represent the model's learning curve, providing insight into the progression and convergence of the training process.

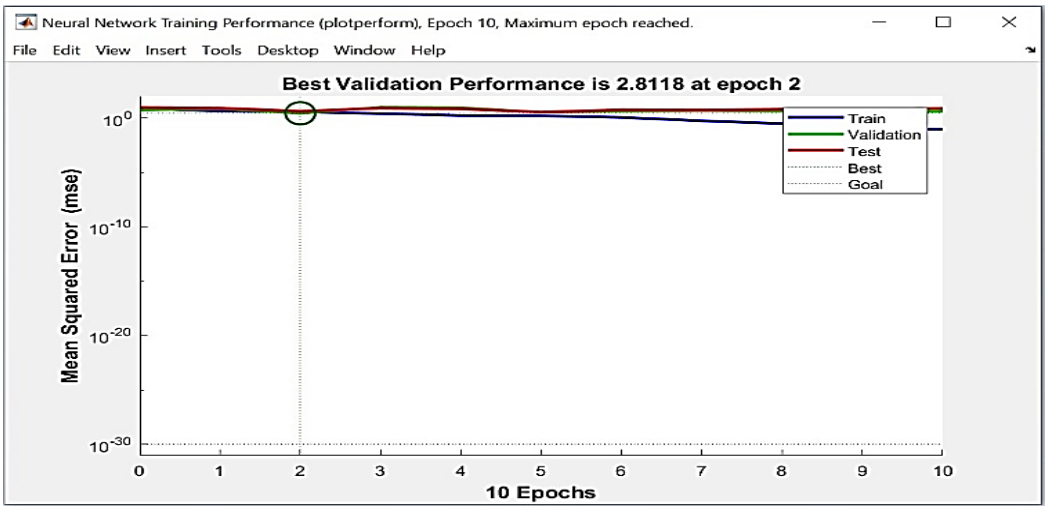


Figure 8 Validation performance of the CNN model, measured using MSE

4.2Comparative performance

Table 3 and *Table 4* compare the performance metrics of the CBPNN and CNN models. Based on accuracy, MSE, MAE, and RMSE, the CNN model outperforms the CBPNN model with a higher accuracy of 90% (compared to 82%), lower MSE (0.988 vs. 1.4138), lower MAE (0.327 vs. 0.512), and lower RMSE (0.991 vs. 1.189), indicating better prediction quality and efficiency in error minimization.

These experimental results demonstrate that the CNN algorithm significantly outperforms the CBPNN in both accuracy and efficiency. The overall findings indicate the effectiveness of employing these techniques in enhancing the security of IoT networks, particularly in detecting and mitigating threats.

4.3Computational efficiency

The proposed hybrid IDS demonstrated notable computational efficiency, with the CNN model completing training in 17 seconds and the CBPNN model in 27 seconds. This efficiency is attributed to optimizations in the model architecture and the implementation of advanced algorithms that minimize resource consumption, making it feasible for deployment in real-time IoT environments. The reduction in runtime is particularly significant given the growing need for instantaneous threat detection in today's connected landscape.

4.4Adaptive mechanisms

To enhance detection capabilities, the IDS incorporates adaptive mechanisms for dynamically adjusting threshold values based on observed traffic patterns and attack density. This adaptability allows the system to respond effectively to fluctuations in network behavior, improving detection accuracy and reducing false positive rates. For instance, during periods of heightened network activity, the system may lower the threshold for detecting anomalies, allowing for quicker responses to potential threats without significantly increasing false alarms.

5.Discussion

The proposed hybrid IDS, integrating both the CBPNN and CNN models, exhibits notable advancements in detecting and mitigating cyber threats within IoT networks. A thorough evaluation of the model's performance indicates that the CNN, with an accuracy of 90% and a detection rate of 99%, surpasses the CBPNN, which achieved an accuracy of 82%. This highlights the effectiveness of utilizing these advanced techniques, specifically designed to address the complex and dynamic challenges of IoT environments.

The results align with existing literature, highlighting the necessity for adaptive and efficient detection mechanisms to safeguard IoT infrastructures against

an array of cyber threats. The findings from this study emphasize the critical importance of integrating robust ML algorithms to enhance the security posture of IoT networks, thereby contributing valuable insights to the ongoing research in this field.

5.1Comparison between proposed model and other studies

To evaluate the performance of the proposed hybrid IDS utilizing the CNN algorithm, a comparative analysis was conducted considering previous related work. This analysis aimed to assess the effectiveness of the CNN model against established ML algorithms, with a specific focus on its performance metrics in detecting DDoS attacks. To facilitate this comparison, input parameters were preprocessed from the KDDTest-21 dataset, converting nominal features into numerical values. Key features transformed included protocol type, services, and flags, ensuring the dataset was appropriate.

The comparative results are summarized in *Table 5*. The CNN model achieved an accuracy of 90% and a detection rate of 99% after 10 epochs of training. This performance surpasses that of the RNN model, which recorded an accuracy of 68% and a detection rate of 83% [29]. Similarly, the bidirectional long short-term memory (BLSTM) and deep belief network (DBN) algorithms yielded accuracies of 75% and 66%, respectively, with detection rates of 67% and 54% [30]. Another study employing a CNN framework reported an accuracy of 77% and a detection rate of 80% [31].

Table 5 Comparison of the CNN algorithm with other studies using the KDDTest-21 dataset

Source	Algorithm	Type of attack	Accuracy (%)	False positive rate (%)	Detection rate (%)
[29]	RNN	DDoS	68%	2.0%	83%
[30]	BLSTM/ DBN	DDoS	75% / 66%	19% / 22%	67% / 54%
[31]	CNN	DDoS	77%	16%	80%
Proposed IDS model	CNN	DDoS	90%	2.0%	99%

The findings of this study demonstrate that the proposed CNN-based IDS significantly outperforms existing approaches in terms of detection accuracy and overall effectiveness. The CNN-IDS model showcases superior capabilities in detecting DDoS attacks when compared with other classification algorithms. Specifically, the proposed CNN model achieved an accuracy of 90% and a detection rate of 99%, illustrating a marked improvement over prior models, including the CNN from reference [31], which reported an accuracy of 77% and a detection rate of 80%. This comparative analysis highlights that the proposed CNN model not only enhances detection capabilities but also addresses the limitations identified in previous studies, reaffirming the critical role of advanced DL techniques in bolstering the security of IoT networks. The comparison shows that while both the CNN model from reference [31] and the proposed CNN model employs similar architectures, the proposed method introduces several enhancements that contribute to its superior performance. Firstly, the training methodology has been optimized, featuring a more extensive dataset preprocessing phase. This improvement facilitates better feature extraction and selection, resulting in higher accuracy and lower false positive rates. Moreover, the proposed CNN model incorporates adaptive mechanisms that dynamically adjust threshold values based on real-time traffic patterns. This adaptability leads to improved detection rates and a more effective response to various attack types. In addition, rigorous hyperparameter tuning strategies have been employed in the proposed method, enhancing model performance through a more effective learning process while mitigating the risk of overfitting.

Training the proposed CNN model for an optimal number of epochs, along with adjustments to the learning rate, has further contributed to better convergence and accuracy. This contrasts with the static training conditions that may have been utilized in the previous study, which could have limited its performance.

Finally, the proposed study emphasizes a comprehensive set of evaluation criteria, including the reduction of false positive rates. This broader focus ensures a more balanced assessment of the model's effectiveness, providing insights into its real-world applicability.

5.2Study limitations

While the proposed hybrid IDS delivers promising results, it does have certain limitations:

1. The performance of the model is heavily reliant on

the quality and diversity of the datasets used for training and evaluation. The KDDTest-21 dataset, while widely recognized, may not encompass all potential attack vectors and network conditions encountered in real-world scenarios.
2. Although the model demonstrates robust performance in controlled settings, its adaptability to dynamic and varied network environments requires further validation. Future studies should focus on testing the model against diverse datasets reflective of real-time IoT conditions.
3. While the CNN model has shown improvements in runtime efficiency, the computational demands may still pose challenges in resource-constrained IoT environments. Optimization techniques are necessary to ensure feasibility in real-time applications.
4. The performance of the IDS can be sensitive to the chosen threshold values for detection. Further investigation is needed to dynamically adjust these thresholds based on traffic patterns and attack density, ensuring optimal performance under varying conditions.

Future work should focus on expanding the model's applicability, validating its performance across diverse scenarios, and refining its computational efficiency to strengthen real-time security in IoT infrastructures. A complete list of abbreviations is listed in *Appendix I.*

6. Conclusion

This study provides a comprehensive analysis of a hybrid IDS designed to strengthen the security of IoT networks amidst an ever-evolving landscape of cyber threats. By integrating advanced ML techniques, specifically the CBPNN and CNN, the proposed model effectively addresses the challenges associated with detecting and mitigating intrusions in IoT environments. The performance evaluation demonstrated that the CNN algorithm outperforms the CBPNN, achieving a detection accuracy of 90% and a detection rate of 99%. These results indicate the effectiveness of employing DL methodologies to enhance the identification of cyberattacks, particularly DDoS attacks. Moreover, the comparative analysis with existing studies highlighted the superiority of the proposed CNN model in terms of accuracy and efficiency, affirming its potential for real-time application in securing IoT networks. The findings also emphasize the critical need for scalable and robust IDS frameworks capable of adapting to the complexities and dynamic nature of IoT environments. By preprocessing data and optimizing model architectures, this study contributes to the ongoing efforts to address the limitations associated with traditional security measures and existing IDS models. Therefore, the hybrid IDS developed in this research not only demonstrates a significant improvement in detection capabilities but also sets a foundation for future research in IoT security. Future investigations could explore the integration of additional ML techniques, such as ensemble methods and reinforcement learning, to further enhance detection accuracy and adaptability. Additionally, it is essential to develop adaptive mechanisms for dynamic threshold adjustments based on real-time network behavior and attack patterns. Expanding the model's applicability to diverse IoT applications and environments will be pivotal in building a more resilient defense against emerging cyber threats.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

Data availability

The dataset used in this study, KDDTest-21, is publicly available and can be accessed from the Kaggle repository (https://www.kaggle.com/datasets/hassan06/nslkdd).

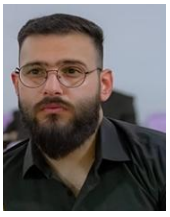
Author's contribution statement

Taha S. Alashkar: Conceptualization, investigation, data curation, writing – original draft, writing – review and editing.

References

[1] Megantara AA, Ahmad T. A hybrid machine learning method for increasing the performance of network intrusion detection systems. Journal of Big Data. 2021; 8(1):142.
[2] Yonan JF, Zahra NA. Node intrusion tendency recognition using network level features based deep learning approach. Babylonian Journal of Networking. 2023; 2023:1-10.
[3] Abbood Z, Yonan JF. Driver drowsy and yawn system alert using deep cascade convolution neural network DCCNN. Iraqi Journal for Computer Science and Mathematics. 2023; 4(4):111-20.
[4] Liao H, Murah MZ, Hasan MK, Aman AH, Fang J, Hu X, et al. A survey of deep learning technologies for intrusion detection in internet of things. IEEE Access. 2024.
[5] Demedeiros K, Hendawi A, Alvarez M. A survey of AI-based anomaly detection in IoT and sensor networks. Sensors. 2023; 23(3):1-33.
[6] Markevych M, Dawson M. A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (AI). In international conference

knowledge-based organization 2023 (pp. 30-7). Sciendo.
[7] Salman QS, Nsaif SM. Advancements in time series-based detection systems for distributed denial-of-service (ddos) attacks: a comprehensive review. Babylonian Journal of Networking. 2024; 2024:9-17.
[8] Sharma S, Yadav M, Chandan M. Explainable AI (XAI): bridging the gap between machine learning and human understanding. Res Militaris. 2020; 10(1):156-65.
[9] Otoum Y, Wan Y, Nayak A. Federated transfer learning-based ids for the internet of medical things (IOMT). In GLOBECOM workshops 2021 (pp. 1-6). IEEE.
[10] Mabrouk A. Innovative approach for optimized IOT security based on spatial network voronoï diagrams, network centrality, and ML-enabled blockchain. In blockchain and machine learning for IoT security (pp. 31-55). Chapman and Hall/CRC.
[11] Thirumalairaj A, Jeyakarthic M. Hybrid cuckoo search optimization based tuning scheme for deep neural network for intrusion detection systems in cloud environment. Journal of Research on the Lepidoptera. 2020; 51(2):209-24.
[12] Taulli T. Large language models: how generative AI understands language. In generative AI: how chatGPT and other AI tools will revolutionize business 2023 (pp. 93-125). Berkeley, CA: Apress.
[13] Tsimenidis S, Lagkas T, Rantos K. Deep learning in IoT intrusion detection. Journal of Network and Systems Management. 2022; 30(1):8.
[14] Nanjappan M, Pradeep K, Natesan G, Samydurai A, Premalatha G. DeepLG SecNet: utilizing deep LSTM and GRU with secure network for enhanced intrusion detection in IoT environments. Cluster Computing. 2024:1-3.
[15] Kumar GSC, Kumar RK, Kumar KPV, Sai NR, Brahmaiah M. Deep residual convolutional neural network: an efficient technique for intrusion detection system. Expert Systems with Applications. 2024; 238(4):121912.
[16] Mohamed D, Ismael O. Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing. Journal of Cloud Computing. 2023; 12(1):41.
[17] Manocchio LD, Layeghy S, Lo WW, Kulatilleke GK, Sarhan M, Portmann M. Flowtransformer: a transformer framework for flow-based network intrusion detection systems. Expert Systems with Applications. 2024; 241:122564.
[18] Hikal NA, Elgayar MM. Enhancing IoT botnets attack detection using machine learning-IDS and ensemble data preprocessing technique. In proceedings of ITAF internet of things-applications and future: 2019 (pp. 89-102). Singapore: Springer Singapore.
[19] Perumal G, Subburayalu G, Abbas Q, Naqi SM, Qureshi I. VBQ-Net: a novel vectorization-based boost quantized network model for maximizing the security level of IoT system to prevent intrusions. Systems. 2023; 11(8):1-25.
[20] Mahalingam A, Perumal G, Subburayalu G, Albathan M, Altameem A, Almakki RS, et al. ROAST-IoT: a novel range-optimized attention convolutional scattered technique for intrusion detection in IoT networks. Sensors. 2023; 23(19):1-29.
[21] Gueriani A, Kheddar H, Mazari AC. Deep reinforcement learning for intrusion detection in IoT: a survey. In international conference on electronics, energy and measurement 2023 (pp. 1-7). IEEE.
[22] Mohan RKR, Katiravan J. Dynamic trusted cross-layer IDS for secured communications in wireless networks using routing algorithm and FT-CNN. Journal of Intelligent & Fuzzy Systems. 2024:1-3.
[23] Bala S, Ahsan SM. Detecting DDoS attacks in software define networking: a machine learning based approach. In international conference on next-generation computing, IoT and machine learning 2023 (pp. 1-6). IEEE.
[24] Raimundo A, Pavia JP, Sebastião P, Postolache O. YOLOX-Ray: an efficient attention-based single-staged object detector tailored for industrial inspections. Sensors. 2023; 23(10):1-26.
[25] Alnifie KM, Kim C. Appraising the manifestation of optimism bias and its impact on human perception of cyber security: a meta analysis. Journal of Information Security. 2023; 14(2):93-110.
[26] Sharghivand N, Derakhshan F. Data security and privacy in industrial IoT. AI-Enabled Threat Detection and Security Analysis for Industrial IoT. 2021:21-39.
[27] Al-rubaye SA. Intrusion detection system in IoT networks using SVM-PSO classification. Master's Thesis, Institute of Graduate Education - Altınbaş University. 2022.
[28] https://www.kaggle.com/datasets/hassan06/nslkdd. Accessed 20 October 2024.
[29] Songa AV, Karri GR. Ensemble-RNN: a robust framework for DDoS detection in cloud environment. Majlesi Journal of Electrical Engineering. 2023; 17(4):31-44.
[30] Alashhab AA, Zahid MS, Muneer A, Abdullahi M. Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks. International Journal of Advanced Computer Science and Applications. 2022; 13(11).
[31] Haider S, Akhunzada A, Mustafa I, Patel TB, Fernandez A, Choo KK, et al. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. IEEE Access. 2020; 8:53972-83.



Taha S. Alashkar earned an M.Sc. degree in Artificial Intelligence from the Department of Information Technology at Altinbaş University, Istanbul, in 2022. He is currently an Assistant Lecturer in the Department of Engineering at the Technical College, Al-Esraa University, Baghdad, Iraq. His

research interests focus on Artificial Intelligence, Machine Learning, and their applications in enhancing Cybersecurity and IoT systems.
Email: taha.ashkar97@gmail.com

Appendix I

S. No.	Abbreviation	Description
1	AI	Artificial Intelligence
2	BLSTM	Bidirectional Long Short-Term Memory
3	CNN	Convolutional Neural Network
4	CPBNN	Cascade Backpropagation Neural Network
5	DBN	Deep Belief Network
6	DDoS	Distributed Denial of Service
7	DL	Deep Learning
8	FN	False Negative
9	GRU	Gated Recurrent Units
10	IDS	Intrusion Detection Systems
11	IoT	Internet of Things
12	IoMT	Internet of Medical Things
13	LSTM	Long Short-Term Memory
14	MAE	Mean Absolute Error
15	ML	Machine Learning
16	MSE	Mean Squared Error
17	NN	Neural Network
18	RMSE	Root Mean Squared Error
19	TP	True Positive
20	TN	True Negative
21	RNN	Recurrent Neural Network
22	ROAST-IoT	Range-Optimized Attention Convolutional Scattered Technique - IoT
23	SVM-PSO	Support Vector Machine-Particle Swarm Optimization
24	VBQ-Net	Vectorization-Based Boosted Quantized Network
25	WSN	Wireless Sensor Networks
26	XAI	Explainable AI