Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

A novel Capsule Dual-Channel Convolutional Block Attention Neural Network with Carpet Weaver Optimization-based intrusion detection system in IOT networks

A Roshini[1*], Ajaypradeep Natarajsivam[2]

[1*]Computer Science and Engineering, Kumaraguru College of Technology Coimbatore, Tamil Nadu, India.

[2]Computer Science and Engineering, Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India

[1*]roshini.a.cse@kct.ac.in, [2]ajaypradeepn@mits.ac.in

Corresponding author E-mail ID: roshini.a.cse@kct.ac.in

Abstract:

The development of Internet of Things (IoT) networks has made them susceptible to cyber-attacks, and thus, proper Intrusion Detection (ID) is the key to safe communication. Current detection systems are usually characterized by low accuracy, high false alarms, and low capability to learn complex feature relations in heterogeneous IoT traffic, which shows the necessity of a more powerful solution. To tackle these issues, this paper proposed the Capsule Dual-Channel Convolutional Block Attention Neural Network with Carpet Weaver Optimization (CD-CCBANNet-CWO) in terms of detecting intrusions. The information gathered on the TON-IoT dataset is preprocessed with Pearson Correlation Coefficient and MinMax Normalization (PCC-MMN). The processed data is then input into the CD-CCBANNet model, and network weights are optimized using Carpet Weaver Optimization (CWO) to provide better convergence and accuracy. Experimental outcomes prove that the model has a 99.45% accuracy, high recall, precision, and F1-score, and a low error rate of 0.55, which is much better compared to the current methods. To sum up, CD-CCBANNet-CWO is a trustworthy and high-performance ID network.

Keywords: *Dual-Channel Convolution, Internet of Things, Intrusion Detection, Carpet Weaver Optimization, Preprocessing.*

1. INTRODUCTION

The high rate at which interconnected devices spread into various spheres of human life, including healthcare, transportation, and smart cities, has highly diversified the IoT ecosystem, with the risk of cyber-attacks Ullah, S. et al, (2023). Real-time monitoring and anomaly detection prove to be a challenging task since IoT networks frequently contain heterogeneous devices that generate massive

DoI: https://doi.org/10.63949/crinfo.v1i2.001

amounts of data in various formats. IDS provides an incredibly significant means of protection of IoT networks, identifying unauthorized log-in and protecting secret information Awajan, A. . et al, (2023). Conventional Machine Learning (ML) methods are not suitable for large-scale IoT data. This has led to the development of Deep Learning (DL) algorithms, which are useful as they accomplish the goal of learning complex patterns and enhancing the scalability and resiliency of IDS to the IoT environment Ullah, S. . et al, (2022).

IoT networks are challenged by a wide range of issues, even though there are improvement steps in the development of the IDS and its implementation in ML and DL. The heterogeneous property of IoT devices generates high-dimensional, intricate, and large-volume data, and thus, the traditional IDS techniques are less efficient in retrieving complex patterns Han, H . et al, (2022). IoT devices have resource limitations that hinder the use of computationally specific security schemes and, in most cases, lead to delayed or inaccurate detection of intrusion Chen, Y . et al, (2022). Among the traditional DL models, though able to learn complex relationships, they demand large training data and computation resources Yadav, N . et al, (2022). And most of the IDS systems are not able to identify advanced attacks, including zero-day exploits, ransomware, and multi-vector attacks. These shortcomings demonstrate the suitability of robust, efficient, and adaptive IDS frameworks that can monitor and detect with high accuracy in the context of the IoT networks Saba, T. . et al, (2022).

The growing number of cyberattacks on IoT devices encourages the development of improved ID models that combine high performance with resource efficiency. It is of urgent necessity to have models that can learn intricate relationships on massive heterogeneous IoT data and retain quick and dependable detection. Adaptive feature extraction and optimization techniques may be used to enhance the IDS and guarantee a higher level of security and reduction of false alarms, and also help to identify threats in real-time. This drives the development of powerful, scalable, and intelligent IDS in the contemporary IoT networks.

Novelty and Contributions

- The proposed model CD-CCBANNet-CWO combines Dual-Channel Convolution, Block Attention, and Capsule Neural Networks to discover both global and local patterns in IoT network traffic while preserving hierarchical relationships between features.
- The PCC-MMN preprocessing is used to eliminate redundant features, make the features more relevant, and normalize the data to achieve better model performance.
- CWO is utilized to weight tune to ensure quicker convergence, optimum learning, and solid detection of the various types of IoT attacks.
- The framework outperforms the state-of-the-art methods because it detects incursions more accurately and reliably.
- Section 2 critically assesses the relevant literature. In Section 3, the methods of this research are explained in detail. The findings are discussed in section 4. Section 5 contains personal thoughts and suggestions on further research.

DoI: https://doi.org/10.63949/crinfo.v1i2.001

2. Literature Survey

In 2024, Momand et al. Momand, A . et al, (2024) suggested an Attention-Based Convolutional Neural Network (ABCNN) for ID in IoT settings. The ABCNN complemented with a CNN on the attention mechanism to target informative traffic patterns and boost learning of low instance attack classes. The preprocessing phase, which consists of a mutual information (MI)-based step, was used to determine the significant features and eliminate redundancy before the classification. The ABCNN outperformed the other traditional methods of ML and DL in terms of detection. The primary strength of the model was that it addressed the problem of imbalance in classes and the discriminative feature learning. However, an increased number of computations and reliance on feature selection hindered the scalability of the resource-constrained IoT systems.

In 2025, Fares et al. Fares, I.A. et al, (2025) introduced a hybrid ID approach to IoT security based on transfer learning. This method used the Swin Transformers and Long Short-Term Memory (LSTM) networks to use hierarchical feature representation and sequential dependency learning. The hybrid architecture was trained with initially pre-trained weights, and then the weights were transferred to another model instance to be trainable on the new data, minimizing the amount of training data and computational resources. The approach was better in detection, scale, and flexibility than traditional DL methods. The benefits of good feature reuse and quicker convergence were important. But it also made the models more complex, and they needed fine-tuning of the parameters to be successfully deployed in a limited IoT system.

In 2025, Afraji et al. Afraji, D.M.A.A. . et al, (2025) suggested a deeper hybrid DL architecture, CNN-LSTM-GRU, which combines Convolutional Neural Network (CNN), LSTM, and Gated Recurrent Unit (GRU) in a multi-branch setup to detect intrusions in the IoT and the Industrial Internet of Things (IIoT). The parallel-sequential fusion model was used to capture spatial and temporal information and eliminate unnecessary calculations. The CNN-LSTM-GRU model enhanced the granularity of detection, learning, and generalization. The complexity of the architecture and calculations was also a constraint that restricted the usage in the resource-restricted IoT setups.

In 2025, Iliyasu et al. Iliyasu, A.S. et al, (2025) introduced a lightweight CNN-based Network ID System, PNet-IDS, to protect IoT security. The approach minimized floating point operations (FLOPs) and optimized how much resources on-device are used to do real-time ID. Distillation of knowledge increased the resistance to changes in network traffic distributions. PNet-IDs were more scalable and efficient, as they were highly accurate and precise with less model size and computation requirements. The lightweight framework, however, did not allow deep feature representation as much as the bigger and more complex DL models.

2.1 Problem Statement

Security IoT networks are characterized by a high level of security risks because of the heterogeneous and resource-limited nature of devices that connect to the network. The large amount of high-dimensional

DoI: https://doi.org/10.63949/crinfo.v1i2.001

data produced by these devices renders the conventional ID techniques less effective in detecting complicated attacks. The traditional approaches to ML do not always identify complex associations between features, and deep neural networks require a lot of computing power and lots of training samples. Consequently, the IoT networks are susceptible to advanced attacks, ransomware, zero-day exploits, and multi-vector attacks, which demonstrate the necessity of a powerful, effective, and flexible ID system.

3. Proposed Methodology

In the section, the proposed Capsule Dual-Channel Convolutional Block Attention Neural Networks with Carpet Weaver Optimization (CD-CCBANNet-CWO) is used to detect intrusion in the IoT networks. The first step involves collecting data by using the TON-IoT dataset, which is a realistic dataset of the IoT network traffic of normal and malicious activities. The data obtained is then preprocessed by Pearson Correlation Coefficient and Min-Max Normalization (PCC-MMN) to remove irrelevant features, increase feature relevance, and normalize values in a standard range. Following preprocessing, the refined data is input into the CD-CCBANNet model, in which the capsule networks retain hierarchical relationships of features, the dual-channel convolution captures local and global traffic patterns, and the block attention highlights key intrusion features. Finally, the model is optimised with the help of Carpet Weaver Optimization (CWO) instead of the model weights, which further optimises the model and results in improved detection and resistance to different IoT attacks. Figure 1 describes the proposed workflow architecture.

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

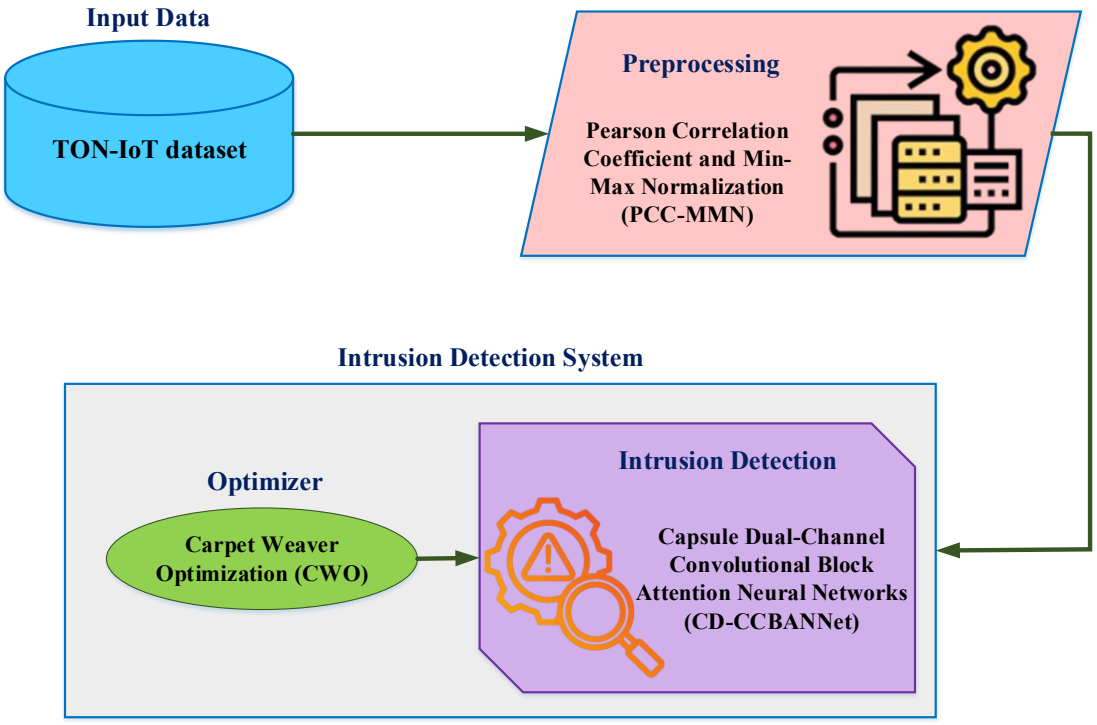


Figure 1 Workflow of the Proposed CD-CCBANNet-CWO Architecture

3.1 Data collection

First, the collection of data is performed through the TON-IoT dataset. Some of the data collected includes network traffic, telemetry, and log data of various IoT devices, which are both normal and malicious (DoS, scanning, and malware activity). The data requires preprocessing in order to encode categorical categories, missing values, and normalize numerical features.

3.2 Data preprocessing using Pearson Correlation Coefficient and Min-Max Normalization (PCC-MMN)

Preprocessing is a part and parcel of this study to enhance the quality of data and the performance of the model. This research employed Pearson Correlation Coefficient and Min-Max Normalization (PCC-MMN) Iliyasu, A.S. et al, (2025), which are responsible for identifying the relevant features and appropriate normalization of the values for those features. Finding the correlation between the goal variable and the feature is the responsibility of PCC. This is followed by MMN for the normalization of values for all the features considered in this research. The PCC is explained by equation (1).

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

$$s = \frac{\sum_{j=1}^{n}\left(q_j - \bar{q}\right)\left(g_j - \bar{g}\right)}{\sqrt{\sum_{j=1}^{n}\left(q_j - \bar{q}\right)^2}\sum_{j=1}^{n}\left(g_j - \bar{g}\right)^2} \quad (1).$$

where, q_j and g_j are individual values of feature and target, respectively, and $\bar{q}$ and $\bar{g}$ indicate the mean of the feature and target. n refers to the total number of samples. The correlation coefficient s helps determine the relationship between the feature and the target, resulting in the model paying attention to the relevant points. The MMN is written in equation (2).

$$q'_{j,m} = \frac{q_{j,m} - \min\left(q_j\right)}{\max\left(q_j\right) - \min\left(q_j\right)} \bullet \left(new\max - new\min\right) + new\min \quad (2).$$

In this context, $q_{j,m}$ is the original value of the j^{th} variable of the m^{th} sample, and $\min\left(q_j\right)$ and $\max\left(q_j\right)$ are the minimum and maximum values of that variable. The value of $new\min$ and $new\max$ is 0 and 1, respectively, and is taken as the new minimum and maximum value of the value obtained after scaling. Also, the normalized value of the j^{th} variable $q'_{j,m}$ prevents a variable with a large value from dominating the model. The preprocessed data is then put through the intrusion detection phase.

3.3 Intrusion Detection using Capsule Dual-Channel Convolutional Block Attention Neural Networks (CD-CCBANNet)

In order to efficiently perform intrusion detection within IoT networks, the proposed CD-CCBANNet Shantal, M. . et al, (2023), Zhou, J. et al, (2024) model combines the characteristics of both Convolutional Block Attention Capsule Networks (CBACN) and Dual-Channel Convolutional Neural Networks (D-CCNN). These models utilize attention mechanisms to focus on the most critical pieces of information, capsules to maintain the relationships between features, and learn both local and global information.

CBACN addresses the weakness of CNN, where important features might not be captured by the pooling processes of CNN. It combines the ideas of CAPS and the attention mechanism to improve the detection of attacks by enhancing feature extraction capability. CAPS are made up of convolutional layers, primary capsules, and digital capsules with dynamic routing algorithms among capsules to maintain hierarchical patterns.

The parent capsule vectors are created by first weighting and adding the input vectors, as indicated by equation (3).

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

$$\hat{v}_{k|j} = X_{jk} v_j$$
$$t_k = \sum_j d_{jk} \hat{v}_{k|j} \quad (3).$$

where, v_j represents the output of the j^{th} sub-capsule corresponding to the feature in the input, X_{jk} shows the transformation matrix that was used to project the parent capsule onto the sub-capsule, $\hat{v}_{k|j}$ shows the parent capsule's anticipated vector k given the input from the capsule j, d_{jk} represents the coupling coefficient used to control the strength of the connection, and t_k represents the combined input to the k^{th} parent capsule. The formula helps the network to learn the relationship between the lower and higher level attack feature. Additionally, the values of the coupling coefficients are updated online according to agreement of the features is shown as equation (4).

$$d_{jk} = \frac{\exp(c_{jk})}{\sum_l \exp(c_{jl})}, \quad c_{jk} \leftarrow c_{jk} + \hat{v}_{k|j} \bullet w_k \quad (4).$$

Here, c_{jk} is the log prior probability that capsule j in the lower layer connects to parent capsule k, w_k is the output vector of the parent capsule after squashing, and the inner product $\hat{v}_{k|j} \bullet w_k$ updates c_{jl} based on the agreement between predicted and actual vectors. This dynamic routing enhances feature extraction, enabling accurate identification of attack patterns.

Then, to identify any attack behavior in network traffic, D-CCNN utilizes the Max-pooling and Attention-pooling layers, which learn both global and local characteristics. The preliminary feature maps from the input data are extracted by the convolutional layer described in equation (5).

$$p_j = X \bullet T_{j:j+i-1} + c \quad (5).$$

Here, T represents the feature matrix input, X is the convolution kernel weight matrix, and $T_{j:j+i-1}$ denotes the sub-matrix corresponding to the j^{th} to the $j+i-1$ rows of T, c is the bias term and p_j is the convolution output. This is given in equation (6), where the layer selects the most active features within a local region.

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

$$w = \max_{0 \le j \le t-i} \{p_j\} \tag{6}$$

In this instance, the convolution layer's feature map is represented as p_j, the input sequence's length is represented by t, the size of the kernel is denoted by i, and w denotes the strongest local feature. The Scaled Dot-product Attention (SDA) function, shown in equation (7), is used by the Attention-pooling layer to find long-range relationships.

$$SDA(Qu, Ke, Ve) = soft\max\left(\frac{QuKe^{\top}}{\sqrt{e_l}}\right)Ve \tag{7}$$

In this context, Qu, Ke, and Ve represent the query, key, and value matrices that are obtained from the feature maps, and e_l is the dimension of the keys. The softmax function is used to obtain the attention weights, and when these are multiplied by Ve, global feature vectors are obtained that identify the distant parts of the input, meaning attack patterns.

3.4 CD-CCBANNet weight optimizer using Carpet Weaver Optimization (CWO)

To achieve the optimal weights of the proposed CD-CCBANNet intrusion detection model, Carpet Weaver Optimization (CWO) Alomari, S . et al, (2024) is used to optimally tune the weights. CWO is inspired by the old-fashioned carpet weaving method with global exploration and local exploitation practices: imitating pattern-driven weaving and creative enhancements. A candidate set of weights of the CD-CCBANNet is represented by each carpet, and its quality is measured by the loss function of the model. In the optimization process, the algorithm initially examines the search space by tracing the weaving patterns that are generated randomly in order to prevent premature convergence. After that, minor innovative changes are made to polish effective solutions as well as enhance convergence stability. This dual-stage progressive approach allows the efficient adaptation of weights, minimizes classification error, and facilitates the accuracy of intrusion detection as it directs CD-CCBANNet to the optimal parameter space.

Algorithm 1: Process of CWO

Input: Population size M, maximum iterations T, lower bound lob, upper bound upb

Output: Optimized CD-CCBANNet weights

Initialize population C using:

$$c_{j,e} = lob_e + s \bullet (upb_e - lob_e)$$

Evaluate the fitness of each solution:

DoI: https://doi.org/10.63949/crinfo.v1i2.001

$f_j = f(C_j)$

for $t = 1$ t = 1 to T do

Randomly generate a weaving pattern C_Q

for each solution C_j do

// Phase 1: Exploration

Update position using:

$c_{j,k}^{Q1} = c_{j,k} + (1-2s)(c_{Q,k}) - J \cdot c_{j,k}$

if $f(C_j^{Q1}) \le f(C_j)$ then

$C_j = C_j^{Q1}$

end if

// Phase 2: Exploitation

Update position using:

$c_{j,k}^{Q2} = (1+(1-2s)/t)c_{jk}$

if $f(C_j^{Q2}) \le f(C_j)$ then

$C_j = C_j^{Q2}$

end if

end for

Store the best solution of iteration.

end for

Return the best optimized CD-CCBANNet weight vector.

4. Results

The results of the experiment on intrusion detection in the Internet of Things networks with the suggested CD-CCBANNet-CWO model are presented here. The model is able to detect network anomalies and correctly categorize the different types of attacks using the TON-IoT dataset. To build the architecture, Python 3.9 is used based on Keras and TensorFlow with the support of NumPy, Pandas, and Scikit-learn to process and analyze data. The experiments are performed using a Windows 64-bit platform with an AMD processor (Intel Core i7 2.8 GHz), 16 GB of RAM, and a 4 GB graphics card by NVIDIA. Table 1 provides the main simulation parameters.

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

Table 1. Simulation Parameters

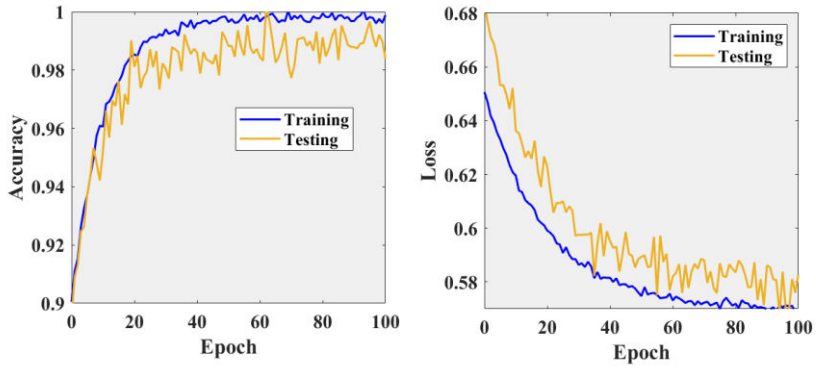
Parameters	Description
Operating System	Windows 64-bit
Dataset	TON-IoT
Proposed Neural Network	CD-CCBANNet
Learning Rate	0.001
Optimizer	CWO
Dropout Rate	0.01
Weight Decay	0.0001
Number of Epochs	100

4.1 Dataset Description

TON-IoT dataset https://www.kaggle.com/datasets/arnobbhowmik/ton-iot-network-dataset is a realistic collection of IoT network traffic that includes both benign and malevolent activities. Among the various types of attack, there exist Backdoor (35,000), DDoS (16,030), Denial of Service (DoS, 20,000), Injection (35,000), Man-in-the-Middle (MITM, 1,043), Password assaults (35,000), Scanning (3,973), Cross-site scripting XSS (6,116), and Regular traffic (245,000). The trained model will be tested on the remaining 20 per cent of the dataset, which will be used for experimental purposes. The distribution renders the learning effective and the evaluation of intrusion detection models robust.

4.2 Performance Evaluation

The suggested CD-CCBANNet-CWO is tested using the TON-IoT dataset and compared to such methods as ABCNN Momand, A . et al, (2024), LSTM Fares, I.A. et al, (2025), CNN-LSTM-GRU Afraji, D.M.A.A. . et al, (2025), and CNN Iliyasu, A.S. et al, (2025). The metrics used to measure performance are accuracy, recall, precision, F1-score, and error rate. The results show that the CD-CCBANNet-CWO has superior accuracy, robust attack detection, and reduced error rate, which implies it can be applied to discern intrusion detection in IoT networks.



(a) **(b)**

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

Figure 2. (a) Accuracy (b) Loss on TON-IoT dataset

Figure 2(a) and Figure 2(b) together depict training and testing accuracy and loss of the proposed CD-CCBANNet-CWO on the TON-IoT dataset with respect to the epochs. The accuracy curves depict that the accuracy improves quickly in the first training phase, and this convergence remains constant, which points to the successful learning and a good generalization capacity. At the same time, the loss values in training and testing converge uniformly with more and more epochs, indicating convergent convergence and optimized weight of the model in the Carpet Weaver Optimization that increases the strength of the model in intrusion detection.

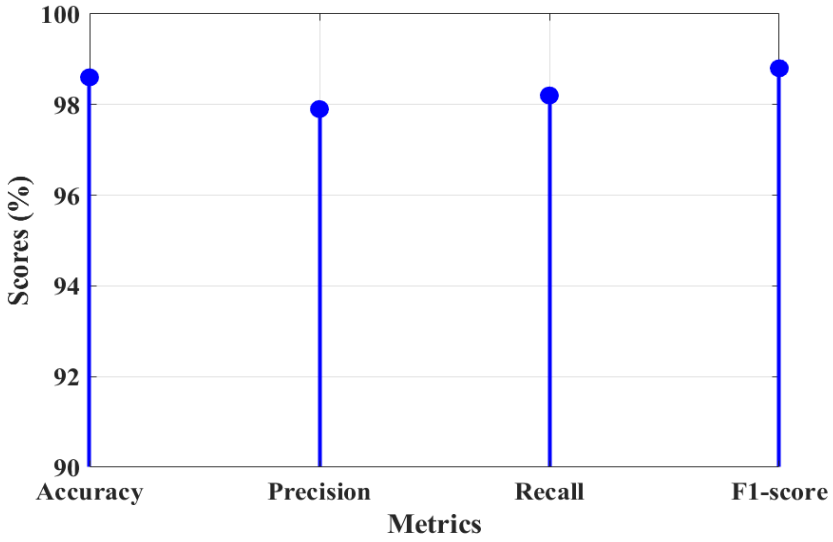


Figure 3. Performance Metrics of CD-CCBANNet-CWO on TON-IoT Dataset

The performance study of the suggested model is shown in Figure 3. All metrics were high, thus indicating the great ability of the model to effectively determine both safe and malicious traffic. The balanced score of all measures shows that there is good performance of feature extraction, attention-based learning, and optimal weight tuning in intrusion detection.

Table 2. Performance Comparison on TON-IoT Dataset

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Error Rate (%)
ABCNN Momand, A . et al, (2024)	95.62	95.10	94.85	94.97	4.38
LSTM Fares, I.A. et al, (2025)	96.48	96.02	95.76	95.89	3.52
CNN-LSTM-GRU Afraji, D.M.A.A. . et al, (2025)	97.83	97.45	97.18	97.31	2.17
CNN Iliyasu, A.S. et al, (2025)	96.95	96.50	96.20	96.35	3.05

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Proposed CD-CCBANNet-CWO	99.45	99.42	99.38	99.40	0.55

Table 2 provides comparisons of intrusion detection performance of current models and the proposed CD-CCBANNet-CWO over the TON-IoT data. Although the traditional DL models generate results that are quite competitive, they, however, show poorer performance as compared to the proposed model. CWO model CD-CCBANNet has been proven to be effective and strong in the detection of IoT intrusion, as it has the best accuracy rate of 99.45%, best recall, best precision, and F1-score. It also has the lowest error rate of 0.55.

5. Conclusion

This paper presented the CD-CCBANNet-CWO framework of intrusion detection in IoT networks, which involves using PCC–MMN preprocessing, Capsule Dual-Channel Convolutional Block Attention Neural Networks, and Carpet Weaver Optimization in terms of weight optimization. The model demonstrated 99.45% accuracy, 99.38% recall, 99.42% precision, 99.40% F1-score, and a low error rate of 0.55 when tested on the TON-IoT dataset. These results are highly comparable to those of the previously described methods, such as ABCNN, LSTM, CNN-LSTM-GRU, and CNN. The key benefits of the suggested framework are the capability to increase the hierarchical representation of features through capsule networks, the possibility of effective feature selection with the help of attention, the increased convergence and weight optimization with the help of CWO, and the capability to detect various types of attacks. The model, however, has increased computational resources in training and therefore may not be deployed on resource-limited devices. Further research will be aimed at incorporating blockchain to obtain model changes and intrusion notifications, provide transparency, log tamper-proof, and share intrusion detection among distributed IoT networks, thus providing a greater degree of trust and resilience.

REFERENCES

[1] Ullah, S., Ahmad, J., Khan, M. A., Alshehri, M. S., Boulila, W., Koubaa, A., Jan, S. U., & Ch, M. M. I. (2023). TNN-IDS: Transformer neural network-based intrusion detection system for MQTT-enabled IoT networks. *Computer Networks*, 237, 110072.

[2] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers*, 12(2), 34.

[3] Ullah, S., Ahmad, J., Khan, M. A., Alkhammash, E. H., Hadjouni, M., Ghadi, Y. Y., Saeed, F., & Pitropakis, N. (2022). A new intrusion detection system for the Internet of Things via deep convolutional neural network and feature engineering. *Sensors*, 22(10), 3607.

DoI: https://doi.org/10.63949/crinfo.v1i2.001

[4] Han, H., Kim, H., & Kim, Y. (2022). Correlation between deep neural network hidden layer and intrusion detection performance in IoT intrusion detection systems. *Symmetry*, 14(10), 2077.

[5] Chen, Y., Lin, Q., Wei, W., Ji, J., Wong, K. C., & Coello, C. A. C. (2022). Intrusion detection using multi-objective evolutionary convolutional neural network for Internet of Things in fog computing. *Knowledge-Based Systems*, 244, 108505.

[6] Yadav, N., Pande, S., Khamparia, A., & Gupta, D. (2022). Intrusion detection system on IoT with 5G network using deep learning. *Wireless Communications and Mobile Computing*, 2022, 9304689.

[7] Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning models. *Computers and Electrical Engineering*, 99, 107810.

[8] Momand, A., Jan, S. U., & Ramzan, N. (2024). ABCNN-IDS: Attention-based convolutional neural network for intrusion detection in IoT networks. *Wireless Personal Communications*, 136(4), 1981–2003.

[9] Fares, I. A., Abdellatif, A. G., Abd Elaziz, M., Shrahili, M., Elmahallawy, A., Sohaib, R. M., Shawky, M. A., & Shah, S. T. (2025). Deep transfer learning based on hybrid Swin transformers with LSTM for intrusion detection systems in IoT environments. *IEEE Open Journal of the Communications Society*.

[10] Afraji, D. M. A. A., Lloret, J., & Peñalver, L. (2025). An integrated hybrid deep learning framework for intrusion detection in IoT and IIoT networks using CNN–LSTM–GRU architecture. *Computation*, 13(9), 222.

[11] Iliyasu, A. S., Siddiqui, A. J., Song, H., & Abdu, F. J. (2025). PNet-IDS: A lightweight and generalizable convolutional neural network for intrusion detection in Internet of Things. *IEEE Access*.

[12] Shantal, M., Othman, Z., & Bakar, A. A. (2023). A novel approach for data feature weighting using correlation coefficients and min–max normalization. *Symmetry*, 15(12), 2185.

[13] Zhou, J., Zhang, S., & Wang, P. (2024). Fault diagnosis for power batteries based on a stacked sparse autoencoder and a convolutional block attention capsule network. *Processes*, 12(4), 816.

[14] Ma, K., Tang, C., Zhang, W., Cui, B., Ji, K., Chen, Z., & Abraham, A. (2023). DC-CNN: Dual-channel convolutional neural networks with attention pooling for fake news detection. *Applied Intelligence*, 53(7), 8354–8369.

[15] Alomari, S., Kaabneh, K., AbuFalahah, I., Gochhait, S., Leonova, I., Montazeri, Z., & Dehghani, M. (2024). Carpet weaver optimization: A novel simple and effective human-inspired metaheuristic algorithm. *International Journal of Intelligent Engineering & Systems*, 17(4).

[16] Arnob Bhawmik. (n.d.). TON-IoT network dataset. *Kaggle*. https://www.kaggle.com/datasets/arnobbhowmik/ton-iot-network-dataset

DoI: https://doi.org/10.63949/crinfo.v1i2.001

Frontiers in Engineering and Informatics
ISSN: 3049-3412 (Online)
Volume No: 01 – Issue No: 02 – June 2025

DoI: https://doi.org/10.63949/crinfo.v1i2.001