Received: September 27, 2023. Revised: December 8, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Cybersecurity Warning System Using Diluted Convolutional Neural Network Framework for IOT Attack Prevention

Karthick M[1]* Salomi Samsudeen[2] Likewin Thomas[3] Priya Darsini V[4]
Prabaakaran K[5]

[1]*Department of Information Technology, Nandha college of Technology, Tamilnadu, India*
[2]*Department of Computational Intelligence, SRMIST, KTR Campus, Chennai, India*
[3]*Department of Artificial Intelligence & Machine Learning, PESITM, Shivamogga 577204, India*
[4]*Panimalar Engineering College, Information Technology,*
Varadharajapuram, Poonamallee, Chennai 600123, India
[5]*Department of Electrical and Electronics Engineering, Easwari Engineering College, Chennai, India*
* Corresponding author's Email: magukarthik@gmail.com

Abstract: The internet of things (IoT) integrates plans, operations, data management, and strategies, because they continuously support businesses, they could be a new point of entry for cyberattacks. IoT security is being seriously threatened by viruses and illicit downloads. These dangers run the risk of obtaining sensitive information, damaging their reputation and their finances. The attack prevention in IoT is detected in this work using a hybrid optimisation mechanism and deep learning a frame. A cybersecurity warning system (CWS) is proposed in this paper, by first pre-processing the input, then classifying, and finally optimizing it. With the modified particle swarm optimization algorithm (MPSO), the IDS is more effective at identifying both normal and abnormal connection in the networks. The smart initialization phase combines various pre-processing strategies to ensure that the informational features incorporated in the early development phase have been enhanced. Then the dilated convolutional neural network (di-CNN) is used for classification and is optimized by using MPSO algorithm to detect the attack. The recommended method is implemented in MATLAB stimulator. The effectiveness of the proposed CWS method approach has been assessed utilising performance criteria such as accuracy, precision ratio, F1 score, specificity, and detection rate. According to experimental findings, the proposed CWS technique 99% in which is relatively high compared to existing methods of 78%, 84%, and 90% than TCN-IDS, MCNN and DSBEL.

Keywords: Internet of things, Modified particle swarm Optimization algorithm, Dilated convolutional neural network.

1. Introduction

An internet of things is a system for connecting machines to each other which is known as machine-to-machine connectivity (IoT). The internet of things will make it possible to connect everything. Also, IoT refers to the network of identifiable embedded computers that communicate data across a network without the assistance of humans or machines. IoT is expanding the number of devices linked to the Internet on a daily basis [1]. And new IoT technologies make it possible to capture and manage almost anything online. This technology is used in numerous fields such as transportation, manufacturing, telecommunications, water and energy management, government, healthcare, even entertainment, education, and finance [2].

IoT is a quickly evolving standard in computing history. In recent years, IoT has developed rapidly in various technical fields. We aggregate billions of devices from several systems, including smart grids, smart homes, smart cars, and smart healthcare [3]. IoT devices are heterogeneous (different types, different communication methods, different types of data sent), numerous (billions of dollars), and have limited computing resources, so IoT devices are typically located at the edge. Because it works, it is vulnerable to cyberattacks. Computer network [4].

However, IoT is vulnerable to cyberattacks due to its many attack surfaces and novelties, as well as the lack of security standards and requirements. There are many types of cyberattacks that an attacker can exploit against the IoT. Depending on the system component they are aiming for and the benefits they intend to obtain from the thread. Therefore, there is a lot of research on cybersecurity around IoT [5]. Security attacks against assets, data, networks, users, and applications represent a major challenge for the Energy Internet. Cybersecurity and risk management are major concerns in the face of security attacks.

In order to resolve these drawbacks, this research proposes a novel cybersecurity warning system (CWS) technique that lessens the accuracy, precision rate, f1 score, specificity and detection rate. The following are the main contributions of the proposed CWS system.

- In this paper, the cybersecurity warning system (CWS) is proposed by first pre-processing the input, then classifying, and finally optimizing it.
- With the modified particle swarm optimization algorithm (MPSO), the IDS is more effective at identifying both normal and abnormal connection in the networks.
- The smart initialization phase combines various pre-processing strategies to ensure that the informational features incorporated in the early development phase have been enhanced.
- Then, for classification and MPSO algorithm optimisation for attack detection, an extended convolutional neural network (di-CNN) is utilised.

The remainder of the study is organised as follows. Section 2 includes a representation of the literature review. Section 3 provides a thorough explanation of the suggested CWS strategy. Section 4 presents the findings, while section 5 presents the conclusions and suggested next steps.

2. Literature survey

Cybersecurity warning system techniques has increased the risks imposed by serious cyber security attacks such as timed attacks, coordinated. To address this issue, several research have been done. Some of such methods have been discussed in this section.

In 2019 Fu, N., et al [6] presented an innovative technique for detecting intruders that combines character-level information processing with a temporal convolutional network (TCN-IDS). This method produces high detection rates without complex function engineering and is applicable to both host-based and network intrusion detection systems (NIDS) and community intrusion detection systems (NIDS). The test results on the standard data set NSL-KDD to shows that the proposed model is outstanding to the previous techniques in terms of accuracy. However, it has a high computational cost.

In 2020 Hwang, R.H., et al [7] presents the D-PACK method, which combines an unsupervised deep learning model and a convolutional neural network (CNN) to automatically shape traffic patterns and filter anomalous traffic, as a method successfully detected anomalous traffic. In particular, for early identification, D-PACK checks only the first bytes of the first packets of each stream. Tests demonstrate that even when examining only two packets of each stream and 80 bytes of each packet, D-PACK can detect malicious traffic with an accuracy of approximately 100% and less than 1% of FNR and FPR. However, this method can only address the fundamental condition where intrusion detection is challenging and cannot account for many types of attacks.

In 2020 Qiu, W., et al [8] presented a multiview convolutional neural network (MCNN)-based technique for detecting data spoofing attacks. The detection of spoofing attacks is then carried out in accordance with the threshold criterion, as indicated by the MCNN output. To confirm the efficiency of the suggested technique, extensive experiments were run on FNET/Grid eye using real DSD from multiple locations. Due to the wide range of retrieved features, CNN's effectiveness is, however, constrained by a number of factors.

In 2021 Yue, C., et al [9] presenting a new intrusion detection system based on dynamic temporal convolutional networks (DyTCN-IDS) for detecting these transient attacks. A semi-physical TCE test bench that simulates real-world scenarios on TCE-based trains was initially built to create efficient datasets for training and testing. Test results shows that the system is easily trained, converges quickly, consumes fewer computing resources, and achieves satisfactory recognition performance. It has a macro-F-score of 99.39%, a macro false alarm rate of 0.09%, and an accuracy of 99.40%. However, they are highly time dependent.

In 2022 Liu, W., et al [10] presented a based-on

CNN MLP, an intrusion detection model trained by federated learning called fed batch. Local detection of each ship is performed by CNN for feature extraction and attack classification is performed by MLP. This simulation result demonstrates the effectiveness of CNN-MLP-based intrusion detection based on the NSL-KDD dataset. This is a challenging task due to difficulty with timely model parameters aggregation.

In 2022 Asam, M., et al [11] presenting an IoT device malware detection, a CNN-based IoT malware detection architecture (iMDA). Local structural changes in the malicious layer are instructed from edge, and smoothing operations are performed in split-transform-merge (STM) blocks. Multiple extended convolution operations are used to uncover the overall structure of the forms of cyber-attack. A reference IoT dataset is used to evaluate the performance of the proposed iMDA, along with CNN architectures. This results in critical unobserved errors in the detection of system state.

In 2022 Liang, Q., et al [12] presented a lightweight detection framework based on convolutional neural networks (CNNs). This includes live traffic pre-processing mechanisms to extract features from the data. The data features are transmitted to a central dual convolutional network for training. Test results show this technique recognizes both legitimate and malicious data streams. Comparatively speaking to other cutting-edge approaches, it has the benefits of high performance and low cost. This is appropriate for efficient DDoS identification in contexts with limited resources. It requires high computational time.

In 2023 Khan, S.H., et al [13] presented a deep squeezed-boosted and ensemble learning (DSBEL), a new malware detection framework. This includes the CNN squeezed-boosted boundary-region split-transform-merge (SB-BR-STM) and master instruction. The suggested STM block uses convolutional operations across multiple paths, boundaries, and regions to capture uniform and heterogeneous global malicious code patterns. The experimental result shows excellent performance with 98.50% accuracy, 97.12% F1 score, 95.97% recall, and 98.42% accuracy. Not able to secure data from poisoning attacks.

In 2022 Liu, Z., et al [14] presented a novel and practical fast ensemble model (FastCBLA-EM) for detecting LDDoS attacks. In FastCBLA-EM, an advanced padding-based dual-slip scheme is developed to generate time-series fixed-length samples from well-tuned packet-step flows. Test results show that FastCBLA-EM detection accuracy reaches 99.7% and time complexity is O(n). Not able to secure data from inference attacks.

In 2023, Rizvi, S., et al [15] Presented a 1D dilated causal neural network (1D-DCNN) based IDS for binary classification. The received field can be enhanced via dilated convolution without affecting the network's settings or limiting its capacity. The efficiency of 1D-DCNN has previously been shown in several application domains. The method proposed here is more reliable for IDS than other conventional techniques. Experimentally, the proposed model has high accuracy with a malware assault detecting rate of 99.98% for CSE-CIC-IDS2018 and 99.7% for CIC-IDS2017. Due to the complex architecture, it.

From the above reviews, is found that these methods possess some drawbacks such as the algorithm is not able to secure data from poisoning and inference attacks, requires long processing time high computational time and are highly time dependent. In order to overcome these drawbacks a novel cybersecurity warning system technique is suggested in this paper.

3. Proposed method

In this paper, the cybersecurity warning system (CWS) is proposed by first pre-processing the input, then classifying, and finally optimizing it. With the modified particle swarm optimization algorithm (MPSO), the IDS is more effective at identifying both normal and abnormal connection in the networks. The smart initialization phase combines various pre-processing strategies to ensure that the informational features incorporated in the early development phase have been enhanced. Then, an extended convolutional neural network (di-CNN) is used for classification and optimized by MPSO algorithm for attack detection. The proposed block diagram has been given in Fig. 1.

3.1 Dilated convolutional neural network (DI-CNN)

Traditional techniques for social networking sentiment analysis that rely on CNNs have limitations to the convolution kernel size, which presents two major issues. First, CNNs can only conceptually capture short-term dependencies. The second is related to the expansion of convolution kernels, which leads to a significant increase in parameters. Dilated convolutional neural networks (D-CNN) were presented to solve these problems. Another hyperparameter is added to the receiving layer in this improved CNN version. Utilizing no-fill filter components, D-CNN enhances network

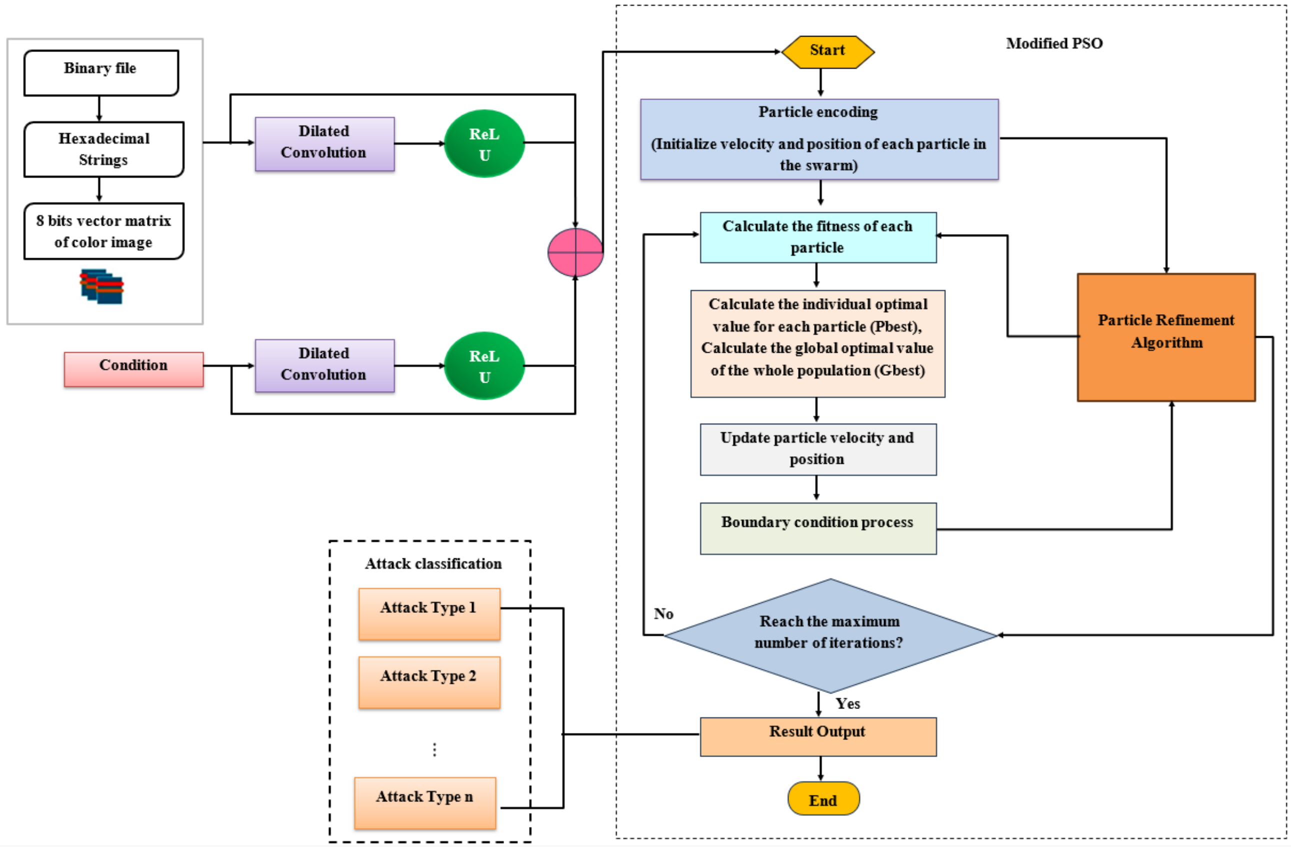
Binary file
Hexadecimal Strings
8 bits vector matrix of color image
Condition
Dilated Convolution
ReL U
Dilated Convolution
ReL U
Modified PSO
Start
Particle encoding (Initialize velocity and position of each particle in the swarm)
Calculate the fitness of each particle
Calculate the individual optimal value for each particle (Pbest), Calculate the global optimal value of the whole population (Gbest)
Update particle velocity and position
Boundary condition process
Particle Refinement Algorithm
No
Reach the maximum number of iterations?
Yes
Result Output
End
Attack classification
Attack Type 1
Attack Type 2
⋮
Attack Type n

Figure. 1 Overall block diagram of proposed CWS framewor

efficiency overall while enlarging the received field size and gathering larger amounts of data. Prediction and classification tasks call for an extended receptive field. The one-way D-CNN extension "l" integrates the signal "E" with the kernel "R," which includes the specified received field size "r." This can be extended to a 2D dilated convolution as follows:

$$(E *_{p_x} R)_s = \sum_\tau R_\tau \, E_{s-p_x\tau} \qquad (1)$$

Where $E *_{p_x}$ is the exponentially increased dilation width of the corresponding layer “l” of the p_x dilated convolution.

3.2 Modified particle swarm optimization algorithm (MPSO)

According to the research, population diversity reduction causes an excessively focused particle swarm to encounter local minimums quickly. The ability to search toward the global minimum would be enhanced if the particle swarm aggregation degrees could be legally modified.

3.2.1. Aggregation degree of the particles swarm

The degree of swarm fragmentation, called diversity, is described by the size of the swarm as a whole. The separation between particles represents its representation. In this study, the distance was indicated by using the absolute difference between the values at every dimensional coordinate.

The particle swarm aggregation degree is what it specifies as having the highest value. The x^{th} value of n^{th} particles can be computed where m^{th} is the swarm dimension, N is the problem's dimension, P_{mx} is the x^{th} value of m particles, and n_{mx} is the x^{th} value of n^{th} particles. The formula follows determines the swarm's overall degree.

$$x(s) = \max\{|d_{mx} - d_{nx}|, m, n = 1,2, \ldots, \\ i \neq n; x = 1,2, \ldots P\} \qquad (2)$$

3.2.2. Strategy of mutation

Method mutation operators have two components. It should be noted that when periodically checking the degree of agglomeration of particle clusters, if the degree of coherence is less than the specified value $(x(s) < e)$, all particles particle position and velocity should be reset while pbest and gbest values should be kept. Another possibility is that the mutation for gbest is performed as follows after the PSO algorithm fails to find the global optimal:

Table 1. Simulation parameters

Parameters	Input
No. of Nodes	100
Area Size	60x60
Mac	802.11g
Radio Range	250m
Simulation Time	50ms
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point

$$new\_gbest \ = gbest^{*}(1+\eta\sigma) \tag{3}$$

Where σ is a Gaussian-distributed random number. So not only can you generate smaller clutter areas where you are more likely to perform local searches. However, jumping out of the local optimum can also create larger spurious regions. The initial value of η is fixed 1.0, $\eta = \beta\eta$, at f intervals of generations, β is a random no. in the range [0.01, 0.9].

3.2.3. MPSO algorithm

Modified PSO (MPSO) complements particle swarm aggregated levels monitoring as part of standard PSO. A mutation operation is also performed on gbest if gbest does not reach a global optimum. Below are the steps to implement MPSO.

Step 1: Set the current iteration generation Iter=1.

Compute the population with m seeds. Set current location as pbest position. gbest is the best seed location for the seed swarm to be initialized with.

Step 2: Determine the fitness of each particle.

Step 3: Calculate each particle's predicted fitness value in relation to its pbest. If the current value exceeds pbest, move the actual position to the pbest position. The gbest is also reset to the particle array's current index if the present value exceeds the threshold;

Step 4: Modify the particle's position and velocity in accordance with Eqs. (1) and (2), respectively;

Step 5: if Iter%Ie==0) {

According to equation (3), determine the aggregated degree d(t); if x(s) is smaller than the specified threshold value e, reset the particle's positioning and speed;

}

Step 6: Iter=Iter+1,

If the stopping criterion is met, terminate the algorithm; if not, perform mutations operations to gbest, accordance with Eq. (3) in step 2.

4. Results

This segment presents the experimental analysis of the suggested approach to cybersecurity warning system (CWS) techniques. This section provides a description of the performance analysis and comparison analysis. The simulation parameters for the IoT security are given in Table 1.

4.1 Performance analysis

In this section, performance analyses such as accuracy, precision ratio, F1 score, specificity, and detection rate are evaluated.

4.1.1. Accuracy

The accuracy of all correctly predicted categories to the dataset's actual classifications represents the prediction algorithm's accuracy. Eq. (4) determines the model's accuracy.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{4}$$

4.1.2. Specificity

The ability to recognise secure instances with accuracy. The calculation is done by determining the percentage of genuine negativity in the underlying data. Eq. (5) determines the model's Specificity.

$$\text{Specificity} = \frac{TN}{TN+FP} \tag{5}$$

4.1.3. Precision ratio

Precision is an exact definition of the frequency of positive abnormalities in a particular picture. The higher proportion of information is highlighted by precision. Eq. (6) determines the model's precision ratio.

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP}) \tag{6}$$

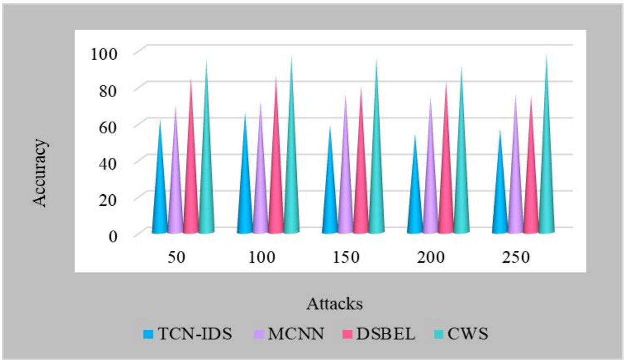

Figure. 2 Comparison of accuracy

Received: September 27, 2023. Revised: December 8, 2023.

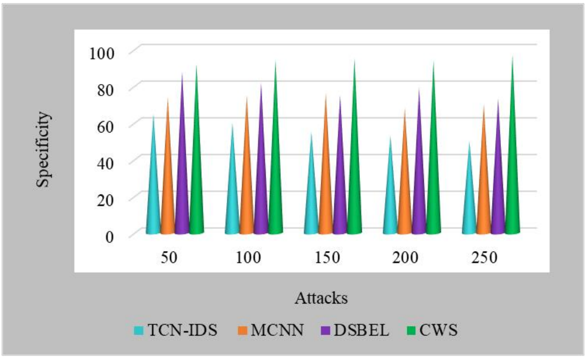

Figure. 3 Comparison of specificity

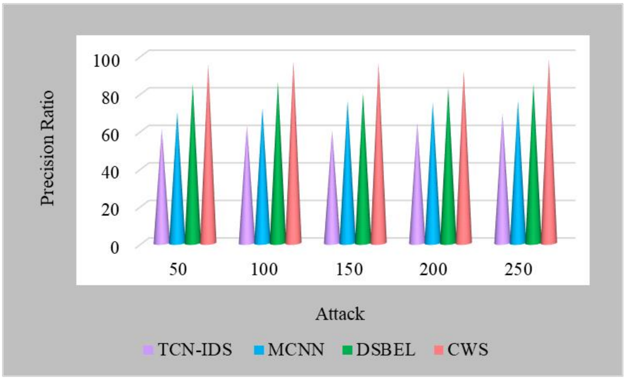

Figure. 4 Comparison of precision ratio

4.1.4. F1 score

The method of calculating the harmonic mean of the precision and recall of a classifier. It is possible to turn it into a single metric. Eq. (7) determines the model's F1 score.

$$\text{F1 Score} = \frac{\text{TP}}{\text{TP}+\frac{1}{2}(\text{FP}+\text{FN})} \qquad (7)$$

4.1.5. Detection rate

In terms of detection rate, also referred to as true positive rate, there is consensus. Eq. (8) determines the model's detection rate.

$$\text{TPR} = \text{TPTP} + \text{FN} \qquad (8)$$

4.2 Comparison analysis

Compared to existing methods such as TCN-IDS [6], MCNN [8], and DSBEL [13], this cybersecurity warning system (CWS) techniques performs better than other existing methods.

Fig. 2 illustrates the stability of the suggested cybersecurity warning system (CWS) methods with existing techniques. The proposed method outperforms other existing techniques such as TCN-IDS [6], MCNN [8] and DSBEL [13] with accuracies of 57%, 76%, 75% and 98% respectively.

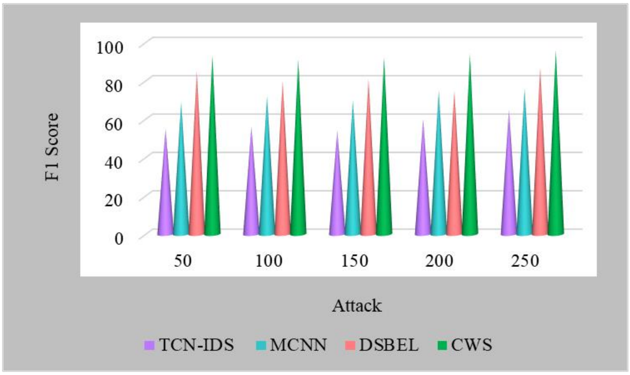

Figure. 5 Comparison of F1 score

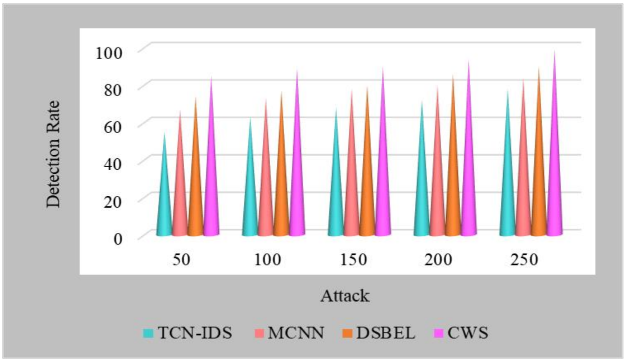

Figure. 6 Comparison of detection rate

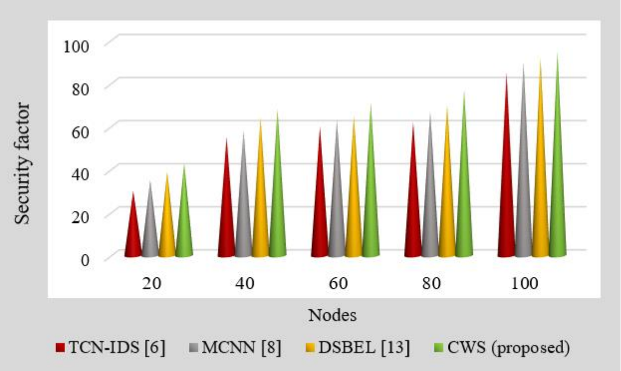

Figure. 7 Comparison of detection rate

Fig. 3 illustrates the stability of the suggested cybersecurity warning system (CWS) methods with existing techniques. The proposed method outperforms other existing techniques such as TCN-IDS [6], MCNN [8] and DSBEL [13] with a specificity of 50%, 70%, 73% and 96% respectively.

Fig. 4 illustrates the stability of the suggested cybersecurity warning system (CWS) methods with existing techniques. The proposed method outperforms other existing techniques such as TCN-IDS [6], MCNN [8] and DSBEL [13] with precision ratio of 69%, 76%, 85% and 94% respectively.

Fig. 5 illustrates the stability of the suggested cybersecurity warning system (CWS) methods with existing techniques. The proposed method outperforms other existing techniques such as TCN-IDS [6], MCNN [8] and DSBEL [13] with an F1 Score of 65%, 76%, 87% and 97% respectively.

Fig. 6 illustrates the stability of the suggested cybersecurity warning system (CWS) methods with existing techniques. The proposed method outperforms other existing techniques such as TCN-IDS [6], MCNN [8] and DSBEL [13] with detection rates of 78%, 84%, 90% and 97% respectively.

Fig. 7 illustrates the security factor of the suggested cybersecurity warning system (CWS) methods with existing techniques. The proposed CWS method achieves a high security factor of 17.51%, 11.58 %, 6.77% than other existing techniques such as TCN-IDS [6], MCNN [8] and DSBEL [13] respectively.

5. Conclusions

In this paper, the cybersecurity warning system (CWS) is proposed by first pre-processing the input, then classifying, and finally optimizing it. With the modified particle swarm optimization algorithm (MPSO), the IDS is more effective at identifying both normal and abnormal connection in the networks. The smart initialization phase combines various pre-processing strategies to ensure that the informational features incorporated in the early development phase have been enhanced. Then, an extended convolutional neural network (di-CNN) is used for classification and optimized by MPSO algorithm for attack detection. The recommended method is implemented in MATLAB stimulator. The effectiveness of the proposed CWS method approach has been assessed utilising performance evaluation, namely accuracy, F1 score, specificity, precision ratio, and detection rate. According to experimental findings, the proposed CWS technique 99% in which is relatively high compared to existing methods of 78%, 84%, and 90% than TCN-IDS [6], MCNN [8] and DSBEL [13].

Conflicts of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author contributions

The authors confirm contribution to the paper as follows: Study conception and design: Karthick M, Salomi Samsudeen; Data collection: Likewin Thomas; Analysis and interpretation of results: Ahilan A; Draft manuscript preparation: Salomi Samsudeen, Prabaakaran K. All authors reviewed the results and approved the final version of the manuscript.

Acknowledgments

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

References

[1] D. A. S. Resul and M. Z. Gündüz, “Analysis of cyber-attacks in IoT-based critical infrastructures”, *International Journal of Information Security Science*, Vol. 8, No. 4, pp.122-133, 2020.

[2] T. T. Nguyen and V. J. Reddi, “Deep reinforcement learning for cyber security”, *IEEE Transactions on Neural Networks and Learning Systems*. 2021.

[3] A. Samy, H. Yu, and H. Zhang, “Fog-based attack detection framework for internet of things using deep learning”, *IEEE Access*, Vol. 8, pp. 74571-74585, 2020.

[4] S. Chesney, K. Roy, and S. Khorsandroo, “Machine learning algorithms for preventing IoT cybersecurity attacks”, In: *Intelligent Systems and Applications: Proc. of the 2020 Intelligent Systems Conference (IntelliSys)* Vol. 3, pp. 679-686, 2021.

[5] M. Kuzlu, C. Fair, and O. Guler, “Role of artificial intelligence in the Internet of Things (IoT) cybersecurity”, *Discover Internet of things*, Vol. 1, pp. 1-14, 2021.

[6] N. Fu, N. Kamili, Y. Huang, and J. Shi, “A Novel Deep Intrusion Detection Model Based on a Convolutional Neural Network”, *Aust. J. Intell. Inf. Process. Syst.*, Vol. 15, No. 2, pp. 52-59, 2019.

[7] R. H. Hwang, M. C. Peng, C. W. Huang, P. C. Lin, and V. L. Nguyen, “An unsupervised deep learning model for early network traffic anomaly detection”, *IEEE Access*, Vol. 8, pp. 30387-30399, 2020.

[8] W. Qiu, Q. Tang, Y. Wang, L. Zhan, Y. Liu, and W. Yao, “Multi-view convolutional neural network for data spoofing cyber-attack detection in distribution synchrophasors”, *IEEE Transactions on Smart Grid*, Vol. 11, No. 4, pp. 3457-3468, 2020.

[9] C. Yue, L. Wang, D. Wang, R. Duo, and H. Yan, “Detecting Temporal Attacks: An Intrusion Detection System for Train Communication Ethernet Based on Dynamic Temporal Convolutional Network”, *Security and Communication Networks*, 2021, pp. 1-21, 2021.

[10] W. Liu, X. Xu, L. Wu, L. Qi, A. Jolfaei, W.

Ding, and M. R. Khosravi, “Intrusion detection for maritime transportation systems with batch federated aggregation”, *IEEE Transactions on Intelligent Transportation Systems,* 2022.

[11] M. Asam, S. H. Khan, A. Akbar, S. Bibi, T. Jamal, A. Khan, U. Ghafoor, and M. R. Bhutta, “IoT malware detection architecture using a novel channel boosted and squeezed CNN”, *Scientific Reports*, Vol. 12, No. 1, pp. 1-12, 2022.

[12] Q. Liang, C. Liu, Y. Zhong, and X. Ren, “A Lightweight Flow-based DDoS Detection Approach using Dual Convolutional Kernels”, In: *Proc. of 2022 China Automation Congress (CAC)*, pp. 2838-2843, 2022.

[13] S. H. Khan, T. J. Alahmadi, W. Ullah, J. Iqbal, A. Rahim, H. K. Alkahtani, W. Alghamdi, and A. O. Almagrabi, “A new deep boosted CNN and ensemble learning based IoT malware detection”, *Computers & Security*, Vol. 133, p. 103385, 2023.

[14] Z. Liu, J. Yu, B. Yan, and G. Wang, “A Deep 1-D CNN and Bidirectional LSTM Ensemble Model with Arbitration Mechanism for LDDoS Attack Detection”, *IEEE Transactions on Emerging Topics in Computational Intelligence*, Vol. 6, pp. 1396-1410, 2022.

[15] S. Rizvi, M. Scanlon, J. McGibney, and J. Sheppard, “Deep learning-based network intrusion detection system for resource-constrained environments”, In: *Proc. of the 13th EAI International Conference on Digital Forensics and Cyber Crime*, 2023.