Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4553502, 9 pages
https://doi.org/10.1155/2022/4553502

Research Article

A Hybrid Model for Intrusion Detection in IoT Applications

Mohammed I. Alghamdi

Department of Engineering and Computer Sciences, Al-Baha University, Al-Baha City 1988, Saudi Arabia

Correspondence should be addressed to Mohammed I. Alghamdi; mialmushilah@bu.edu.sa

Received 19 February 2022; Revised 11 April 2022; Accepted 25 April 2022; Published 14 May 2022

Academic Editor: Muhammad Imran

Internet of Things (IoT) networks has recently become an important component of smart cities, smart buildings, health care, and other applications. It finds it beneficial due to the inherent characteristics of low cost, compact, and low-powered IoT devices. At the same time, security remains a challenging issue in the design of IoT networks. Intrusion detection systems (IDS) can be used to identify the occurrence of intrusions in the network, i.e., abnormal activities in the network. The latest advances in machine learning (ML) and metaheuristics can be employed to design effective IDS models for IoT networks. This article develops a novel political optimizer with cascade forward neural network (PO-CFNN-)-based IDS in the IoT environment. The major intention of the PO-CFNN technique is to determine the occurrence of intrusions from the IoT environment. The PO-CFNN technique follows three major processes, namely, preprocessing, classification, and parameter optimization. Initially, the networking data is preprocessed to transform it into a useful format. Following that, the CFNN technique is employed for the identification and classification of intrusions in the IoT environment. In the final stage, the PO algorithm is applied for the optimal adjustment of the parameters involved in the CFNN model. The experimental validation of the PO-CFNN technique on a benchmark dataset stated the better outcomes of the PO-CFNN technique over recent approaches.

1. Introduction

In the digital era, the Internet of Things (IoT) is known as the most interesting advancement. The web permits associated gadgets to develop dramatically each day, and it has been suggested that more than 75 billion Internet of Things (IoT)-connected devices to be in use by 2025; according to current projections as of 2019, the installed base of IoT devices had grown by approximately thrice [1, 2]. The IoT innovation's motivation is to interconnect all objects to make all PCs smarter and make it safer to speak with people. Sensors and organizations permit everything to speak with one another straightforwardly to trade basic data [2]. Later on, it is conceivable through machine-to-machine (M2M) correspondence [3]. Various down-to-earth IoT applications can be utilized practically in many fields, like shrewd city applications (brilliant homes, savvy networks, medical services, and others), where those applications work on personal satisfaction [4]. The idea of the intrusion identification framework (IDS) aims to distinguish a danger or intrusion into the organization, and it effectively tracks the organization by recognizing likely occasions and logging data about them by halting episodes. The intrusion detection and prevention system (IDPS), which is a mix of two frameworks used to screen events happening in an organization and assess them for potential infringements or occurrences in security strategies, is the most common way of performing intrusion recognition and stopping to identify episodes [5]. Involving the IoT framework in numerous application areas like medical services, smart homes, shrewd industry, nature observing, and others gives critical advantages to the IoT framework. IoT security issues are a huge concern, which are classification, honesty, accessibility, and approval [6]. The combination of true articles with IoT, in any case, raises the scope of cybersecurity dangers every day.

Cyberspace is a fairly weak foundation, not intended to do what it does today, and on which increasing usefulness is constructed [7]. The way that the web is utilized for a wide range of basic activities at the level of people, firms, associations, and even countries has drawn in a wide range of malevolent activities. Cyberattacks can affect a wide range of structures. The issue is how to treat them. For some

different types of assault, discovery is an issue and, here and there, the primary issue. Part of the problem is that intrusion detection systems (IDS) are used to alert clients or organizations that they are under attack, or, as in the case of web applications, may not include any malware, but it depends on how a convention is handled [8].

Involving AI in intrusion discovery is not new. To be sure, it is now many years old, nearly as old as the field of intrusion detection, for example. Today, AI is not utilized strongly in intrusion identification. It is self-evident that AI could work on fundamentally improving the presentation of IDS, but what is subtler is how to operationalize this thought. There are a few explanations behind that [9]. The main one is that AI is a troublesome subject, a long way from being an adult and just security individuals appear to be keen on involving AI in intrusion identification. Individuals associated with AI appear to be substantially more intrigued by different applications, albeit in numerous ways that cybersecurity should be a characteristic space of utilization for AI [10]. The issue might lie more with cybersecurity than with the AI group. Cybersecurity extends the impression of a turbulent world without intelligence and lacking codification [11].

The authors in [12] presented several kinds of attacks in the IoT environment, and a *distributed denial-of-service* (DDoS) is a vulnerable attack. Blockchain (BC) is used to design a model for secure IoT networks and is employed for cryptocurrency transactions. A new BIoTIDS technique is derived to identify the existence of intrusions by the use of BC. It can determine the occurrence of intrusions from the IoT networks and detect DDoS attacks. Sarhan et al. [13] proposed and evaluated a standard NIDS feature set depending upon NetFlow network metadata gathering status. A set of two NetFlow enabled feature set versions are employed. Next, the authors in [14] proposed a novel feature selection for IDS by the use of information gain (IG) and gain ratio (GR) with the top 50% of features to detect DoS as well as DDoS attacks. The presented model has obtained an optimal subset of features by the use of insertion and union operations on subsets offered by the top 50% of IG and GR features. The authors in [15] presented a novel unified IDS model for the IoT environment for securing the network from various kinds of attacks, such as exploits, DoS, probes, and generics.

This article develops a novel political optimizer with cascade forward neural network (PO-CFNN-)-based IDS in the IoT environment. The major intention of the PO-CFNN technique is to define the occurrence of intrusions in the IoT environment. The PO-CFNN approach follows three major processes, namely, preprocessing, classification, and parameter optimization. Initially, the networking data is preprocessed to transform it into a useful format. Following that, the CFNN technique is employed for the identification and classification of intrusions in the IoT environment. In the final stage, the PO algorithm is applied for the optimal adjustment of the parameters involved in the CFNN technique. The experimental validation of the PO-CFNN technique on a benchmark dataset stated the better outcomes of the PO-CFNN technique over recent approaches.

2. The Proposed Model

In this study, a novel PO-CFNN approach has been developed for the identification and classification of intrusions in the IoT environment. The PO-CFNN technique follows three major processes, namely preprocessing, classification, and parameter optimization. Firstly, the networking data is preprocessed to transform it into a useful format. Then, the CFNN technique is employed for the identification and classification of intrusions in the IoT environment. In the end, the PO algorithm is used to find the best way to change the parameters in the CFNN model. CFNM-based Intrusion Detection and Classification.

During this phase, the CFNN approach was utilized for the identification and classification of intrusions in the IoT environment [16, 17]. The perceptron connection has been developed between input and output through the process of straight linking. Nonetheless, the FFNN connection intended between input and output was an ambiguous link. The linking is nonlinear in shape using an activation function from the hidden state. The system with an ambiguous link between the output and input layer was intended once the association process on perceptron and multilayer systems was collective. The system intended by this technique is called cascade forward neural network (CFNN).

$$y = \sum_{i=1}^{n} f^{i}\omega_i^i x_i + f^o\left(\sum_{j=1}^{k}\omega_j^o f_j^h\left(\sum_{i=1}^{n}\omega_{ji}^h x_i\right)\right), \tag{1}$$

whereas f^{i} indicates the activation function in the input to output layers as well as ω_i^i characterizes the weight from the input to output layers. The activation function and bias and input layer from the hidden layer denote ef^{h}:

$$y = \sum_{i=1}^{n} f^{i}\omega_i^i x_i + f^o\left(\omega^b + \sum_{j=1}^{k}\omega_j^o f^h\left(\omega_j^b + \sum_{i=1}^{n}\omega_{ji}^h x_i\right)\right). \tag{2}$$

Here, the CFNN model was executed in time sequence information. Hence, the neuron from the input layer is intervals of time sequence $X_{t-1}, X_{t-2}, \cdots, X_{t-p}$; however, the output is the existing information X_t.

Consider that going to weight vector ω of length s represents the collection of network weights and the objective function as $e = 1/2(X_t - \widehat{X})^2$.

Described Q was a positive matrix of size $s \times s$, whereas $\mathrm{Q}^{\mathrm{T}} = Q$. The stage of the method for conjugate gradient optimization is defined below:

Set $k = 0$, and choose the primary point $\Omega^{(0)}$.

Estimate the weight gradient.

$$g^{(0)} = \frac{\partial e}{\partial \omega^{(0)}} = \frac{\partial e}{\partial \omega}\bigg|_{\omega=\omega^{(o)}} = \left[\frac{\partial e}{\partial \omega_1^{(0)}} \;\; \frac{\partial e}{\partial \omega_s^{(0)}}\right]^T. \tag{3}$$

Once $g^{(0)} = 0$ afterward stop, and it gained an optimum weight $= \Omega^{(0)}$. Or else, set $d^{(0)} = g^{(0)}$.

Estimate $\alpha_k = \text{argmin}_{\alpha \geq 0} e(\omega^{(k)} + \alpha d^{(k)}) = -\, g^{(k)T} d^{(k)} / d^{(k)T} Q d^{(k)}$.

Estimate $\Omega^{(k+1)} = \Omega^{(k)} + \alpha_k d^{(k)}$.

Estimate $g^{(k+1)} = \partial e / \partial \omega^{(k+1)}$, if $g^{(k+1)} = 0$ stop and the optimal weight is $\omega^{(k+1)}$.

Estimate

$$\beta_k = \frac{g^{(k+1)T} Q d^{(k)}}{d^{(k)T} Q d^{(k)}} \tag{4}$$

Estimate $d^{(k+1)} = -g^{(k+1)} + \alpha_k d^{(k)}$.

$k = k + 1$; go to step 3.

As for the FFNN, the iteration method to weight searching on CFNN is typically termed as an epoch. Assume that the highest amount of epochs represent K. Once the iteration termination criteria could not be occurred, still the epoch$k = K$, and subsequently, the iteration method is ended. Substituting the procedure of $Qd\,(k)$ with another procedure such as the Hestenes-Stiefel model, especially, the technique $Qd^{(k)}$ is substituted with $(g^{k+1} - g^k)/\alpha_k$.

$$\beta_k = \frac{g^{(k+1)T} \left[g^{(k+1)} - g^{(k)} \right]}{d^{(k)T} \left[g^{(k+1)} - g^{(k)} \right]}. \tag{5}$$

For determining the optimum weight of the CFNN, the PO approach is employed and in that way enhances the classifier accuracy.

2.1. PO-Based Parameter Optimization. Finally, the PO algorithm is applied for optimal adjustment of the parameters contained in the CFNN model [18, 19]. PO approach is encouraged by *b*, the western political optimization algorithm which comprises 2 features. The primary statement that all the citizens try to enhance their helpfulness to win the election. PO has been comprised of 5 phases, namely, election campaign, party switching, interparty election, parliamentary affairs, party establishment, and constituency apportionment. The entire population is divided into n political parties, as follows:

$$P = \{P_1, P_2, P_3, \cdots, P_n\}. \tag{6}$$

All the parties include n party members that are given as

$$P_i = \left\{ p_i^1, p_i^2, p_i^3, \cdots, p_i^n \right\}. \tag{7}$$

All the party members induce d dimension as shown as

$$p_i^j = \left[p_{i,1}^j, p_{i,2}^j, p_{i,3}^j, \cdots, p_{i,d}^j \right]^T. \tag{8}$$

Al solutions are election candidates. Consider n electoral district as follows:

$$C = \{C_1, C_2, C_3, \cdots, C_n\}. \tag{9}$$

Assume there is a n member in all the constituencies.

$$c_j = \left\{ p_1^j, p_2^j, p_3^j, \cdots, p_n^j \right\}. \tag{10}$$

The party leader is described by the member as optimum fitness.

$$q = \text{argmin}_{1 \leq j \leq n} f\left(p_1^j \right), \forall i \varepsilon \{1, \cdots, n\}, \tag{11}$$

$$p_i^* = p_i^q. \tag{12}$$

All the party leaders are shown as

$$P^* = \{p_1^*, p_2^*, p_3^*, \cdots, p_n^*\}. \tag{13}$$

The winner of the constituency is named a member of parliament.

$$C = \{c_1^*, c_2^*, c_3^*, \cdots, c_n^*\}. \tag{14}$$

It is possible to split the population into n constituencies, and each constituency has n political parties, where $n = \sqrt{\text{Pop.Size}}$ as seen in Figure 1.

In the election campaign stage, the below equations are utilized to update the position of the probable solution.

$$p_{i,k}^j(z+1) = \begin{cases} \text{if } p_{i,k}^j(z-1) \leq p_{i,k}^j(z) \leq m^* \text{or} p_{i,k}^j(z-1) \geq p_{i,k}^j(z) \geq m^*, \\ m^* + r\left(m^* - p_{i,k}^j(z) \right); \\ \text{if } p_{i,k}^{\text{i}}(z-1) \leq m^* \leq p_{ik}^{\text{i}}(z) \text{or} p_{i,k}^{\text{i}}(z-1) \geq m^* \geq p_{i,k}^{\text{i}}(z), \\ m^* + (2r-1)\left| m^* - p_{i,k}^j(t) \right|; \\ \text{if } m^* \leq p_{i,k}^{\text{i}}(z-1) \leq p_{i,k}^{\text{i}}(z) \text{ or } m^* \geq p_{i,k}^{\text{i}}(z-1) \geq p_{i,k}^{\text{i}}(z), \\ m^* + (2r-1)\left| m^* - p_{ik}^l(z-1) \right|. \end{cases} \tag{15}$$

$$p_{i,k}^j(z+1) = \begin{cases} \text{if } p_{i,k}^j(z-1) \leq p_{i,k}^j(z) \leq m^* \text{ or } p_{i,k}^j(z-1) \geq p_{i,k}^j(z) \geq m^*, \\ m^* + (2r-1)\left| m^* - p_{i,k}^j(z) \right|; \\ \text{if } p_{i,k}^j(z-1) \leq m^* \leq p_{i,k}^j(z) \text{ or } p_{i,k}^j(z-1) \geq m^* \geq p_{i,k}^j(z), \\ p_{i,k}^j(z-1) + r\left(p_{i,k}^j(z) - p_{i,k}^j(z-1) \right); \\ \text{if } m^* \leq p_{i,k}^i(z-1) \leq p_{i,k}^j(z) \text{ or } m^* \geq p_{i,k}^j(z-1) \geq p_{i,k}^j(z), \\ m^* + (2r-1)\left| m^* - p_{i,k}^j(z-1) \right|. \end{cases} \tag{16}$$

To balance exploitation, party switch is adopted [20]. Adaptive variable λ is applied; that is drastically minimized from 1 to 0 in the entire iteration method. All the candidates

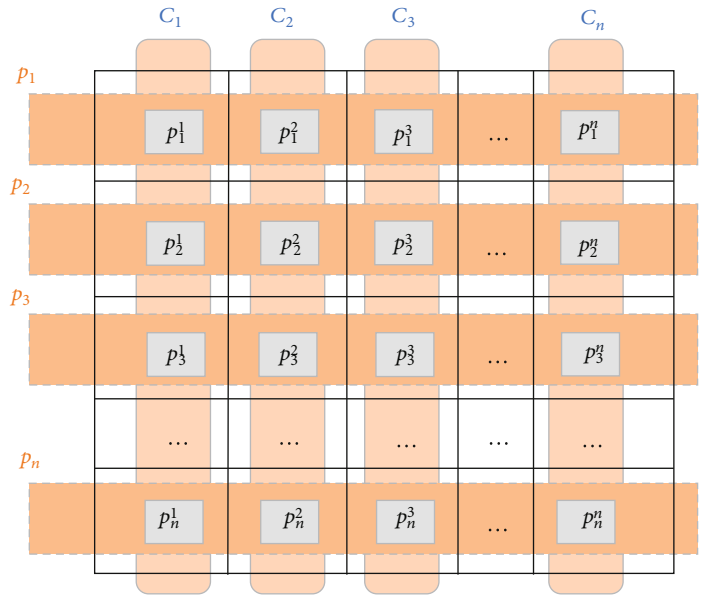

Figure 1: PO logical division of the population.

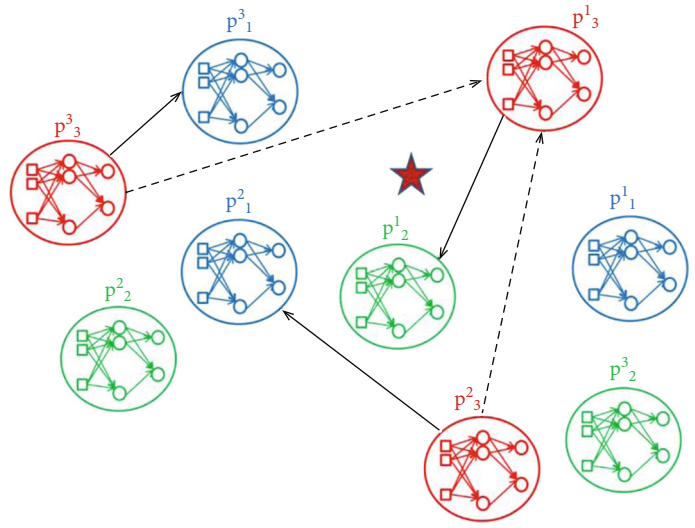

Figure 2: Depiction of the position updating of CFNNs through PO.

are chosen as per the possibility λ as well as substituted with the worst member of the arbitrarily chosen party.

$$q = \arg \max_{i \le j \le n} f\left(p_i^j\right). \tag{17}$$

During the election stage, the winner in the constituency is gained as follows:

$$q = \arg \min_{i \le j \le n} f\left(p_i^j\right), \tag{18}$$

$$c_j^* = p_q^j. \tag{19}$$

Figure 2 shows how PO updates the location of CFNNs. The position of the global optimum is shown by the star symbol. With regard to the party leader, dotted arrows show the position updating of party 3 members, and plain arrows show the position updating of party 3 members in relation to the constituency winners.

3. Performance Validation

This section investigates the intrusion detection outcomes of the PO-CFNN model on three distinct datasets with 80 : 20 for training and testing. Table 1 and Figures 3 and 4 report the comparative results of the PO-CFNN model with existing methods on the test NSL-KDD++ dataset [21]. The

Table 1: Comparative analysis of PO-CFNN technique with recent approaches to the NSL-KDD++ dataset.

Methods	Accuracy	Precision	Recall	F score
PO-CFNN	99.86	99.89	99.58	99.72
SHOLEN model [22]	99.62	99.76	99.49	99.60
ASCH model [23]	98.74	96.62	98.82	93.36
RNN model	97.70	96.25	95.55	93.36
Deep NN model	96.55	95.58	95.47	92.50
DBN model [24]	95.44	94.25	93.28	92.39

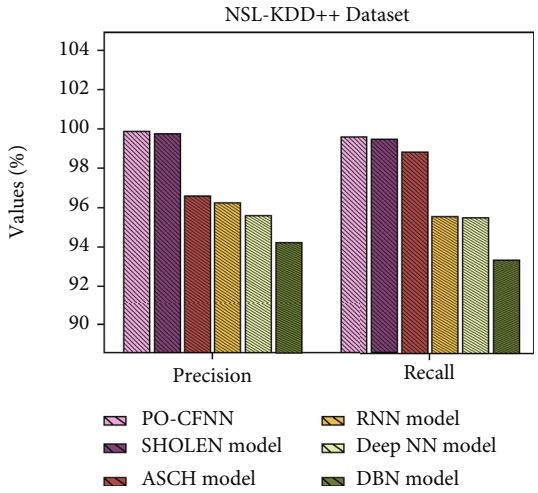

Figure 3: Prec_n and reca_l analysis of PO-CFNN technique under NSL-KDD++ dataset.

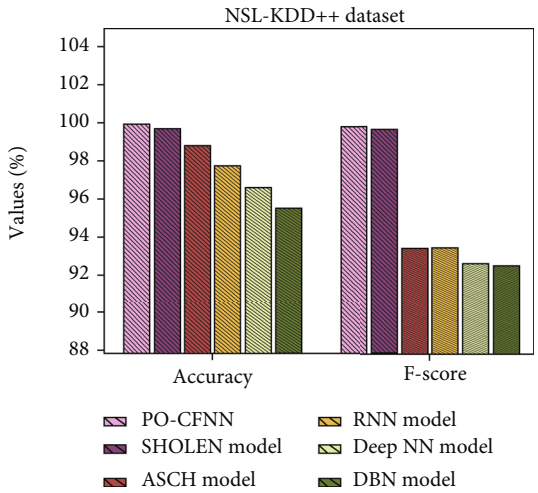

Figure 4: Acc_y and F_{score} analysis of PO-CFNN technique under NSL-KDD++ dataset.

results indicated that the DBN model has gained ineffective outcomes over the other methods with an accuracy of 95.44%. At the same time, the deep NN model has resulted in a slightly increased accuracy of 96.55%. In line with this, the ASCH and RNN models have obtained moderately improved accuracy of 98.74% and 97.70%, respectively. Though the SHOLEN model has accomplished reasonable accuracy of 99.62%, the PO-CFNN model has showcased superior results with an accuracy of 99.86%.

Figure 5 establishes the ROC analysis of the PO-CFNN technique on the NSL-KDD++ dataset. The figure exposed that the PO-CFNN technique has reached an enhanced outcome with a higher ROC of 99.9928.

Table 2 and Figures 6 and 7 report the comparative results of the PO-CFNN model with existing methods on the test UNSWNB15 dataset [25]. The results indicated that the DBN model has gained ineffective outcomes over the other methods with an accuracy of 98.92%. Simultaneously, the deep NN model has resulted in a slightly increased accuracy of 98.57%. Also, the ASCH and RNN models have obtained moderately improved accuracy of 98.88% and 98.99%, respectively. But, the SHOLEN model has accomplished reasonable accuracy of 98.99%, and the PO-CFNN model has showcased superior results with an accuracy of 99.46%.

Figure 8 depicts the ROC analysis of the PO-CFNN technique on the UNSWNB15 dataset [26]. The figure exposed that the PO-CFNN technique has reached an enhanced outcome with a higher ROC of 99.9378.

Table 3 and Figures 9 and 10 report the comparative results of the PO-CFNN technique with existing methods on the test CIDCC-2017 dataset. The results indicated that the DBN model has gained ineffective outcomes over the other methods with an accuracy of 98.83%. Likewise, the deep NN model has resulted in a slightly increased accuracy of 98.69%. The ASCH and RNN models have obtained moderately improved accuracy of 98.65% and 98.92%, respectively. Finally, the SHOLEN model has accomplished reasonable accuracy of 99.05%; the PO-CFNN model has showcased superior results with an accuracy of 99.38%.

Figure 11 portrays the ROC analysis of the PO-CFNN technique on the CIDCC-2017 dataset. The figure exposed that the PO-CFNN technique has reached an enhanced outcome with a higher ROC of 99.9900. Figure 12 provides a comparative study for all datasets as an average accuracy for all models. The figure shows the superiority of the proposed PO-CFNN model.

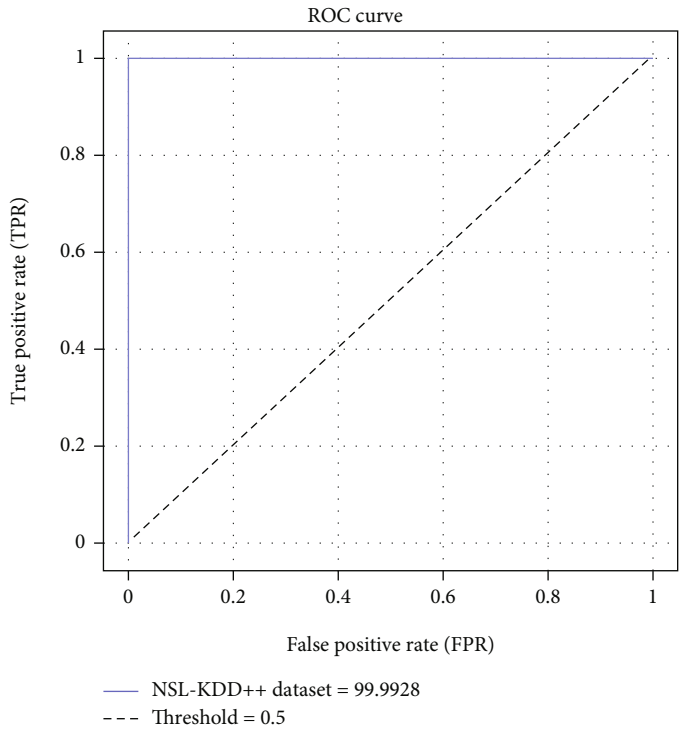

Figure 5: ROC analysis of PO-CFNN technique under NSL-KDD++ dataset.

Table 2: Comparative analysis of PO-CFNN technique with recent approaches to UNSWNB15 dataset.

Methods	Accuracy	Precision	Recall	F score
PO-CFNN	99.46	99.75	99.62	99.76
SHOLEN model	98.99	99.63	99.45	99.68
ASCH model	98.88	96.68	98.74	93.58
RNN model	98.99	96.40	97.94	94.55
Deep NN model	98.57	95.60	95.64	92.98
DBN model	98.92	94.28	93.30	93.61

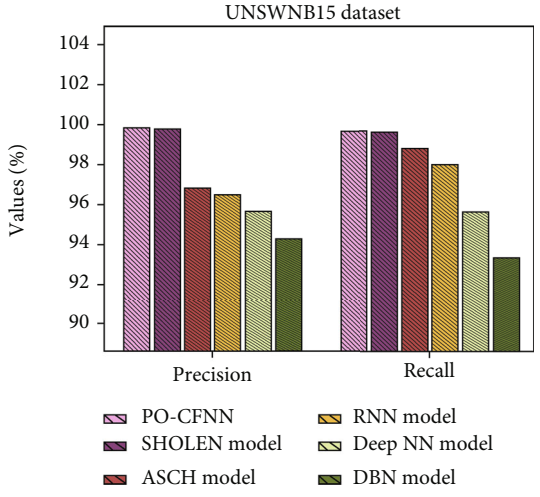

Figure 6: Prec$_n$ and reca$_l$ analysis of PO-CFNN technique under UNSWNB15 dataset.

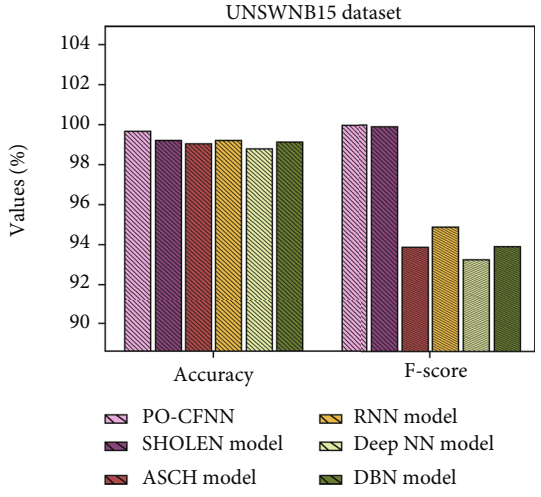

Figure 7: Acc$_y$ and F_{score} analysis of PO-CFNN technique under UNSWNB15 dataset.

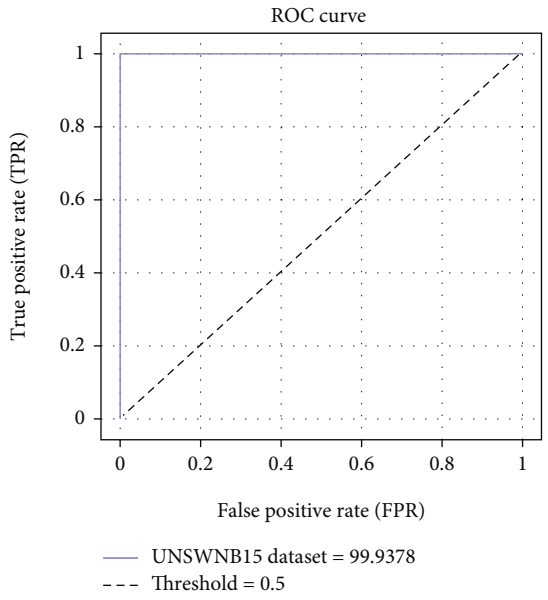

Figure 8: ROC analysis of PO-CFNN technique under UNSWNB15 dataset.

Table 3: Comparative analysis of PO-CFNN technique with recent approaches on the CIDCC-2017 dataset.

Methods	Accuracy	Precision	Recall	F score
PO-CFNN	99.38	99.69	99.66	99.69
SHOLEN model	99.05	99.61	99.52	99.54
ASCH model	98.65	95.55	98.74	93.31
RNN model	98.92	95.96	95.46	94.21
Deep NN model	98.69	93.31	92.10	90.93
DBN model	98.83	95.87	94.97	92.37

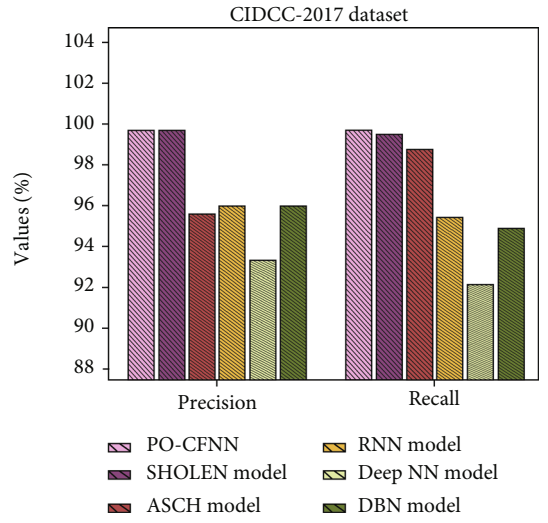

Figure 9: Prec_n and reca_l analysis of PO-CFNN technique under CIDCC-2017 dataset.

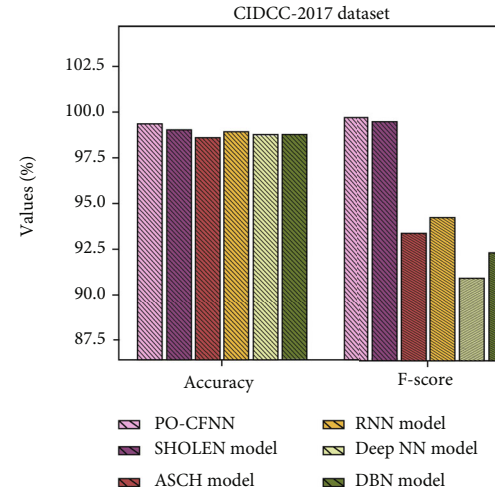

Figure 10: Acc_y and F_{score} analysis of PO-CFNN technique under the CIDCC-2017 dataset.

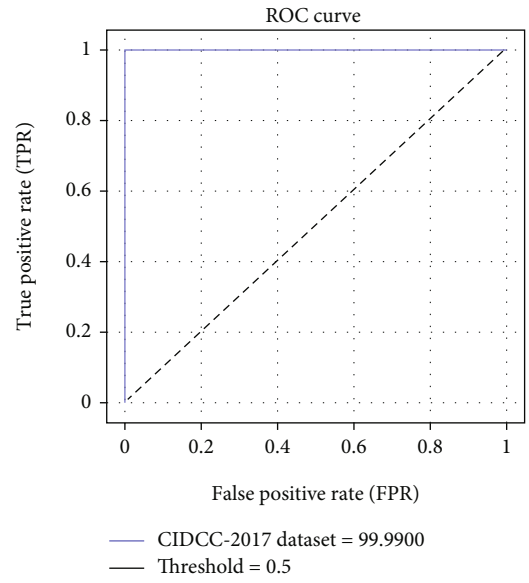

Figure 11: ROC analysis of PO-CFNN technique under the CIDCC-2017 dataset.

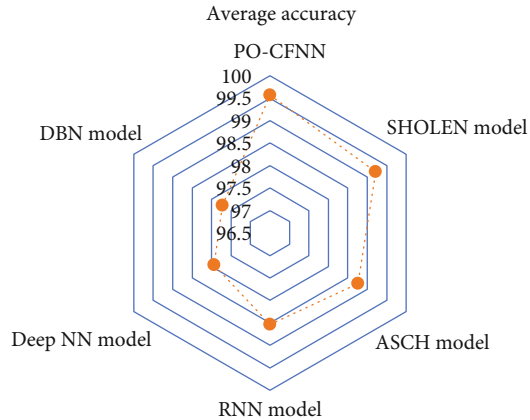

Figure 12: Average accuracy for all models with all datasets.

4. Conclusion

In this work, a novel PO-CFNN approach for identifying and classifying IoT intrusions has been created. Before classification and parameter optimization, the PO-CFNN algorithm undergoes preprocessing and preclassification. In the beginning, the network data is preprocessed to make it easier to analyze. The CFNN algorithm is used to identify and classify intrusions in the IoT environment. Final adjustments to the CFNN model's parameters are made using the PO algorithm at this point. When compared to other contemporary techniques, the PO-CFNN algorithm performed better in an experiment on a benchmark dataset. As a result, the PO-CFNN approach offers superior performance over the alternatives. In future work, feature selection techniques might be developed utilizing the metaheuristics algorithms.

Data Availability

This article develops a novel political optimizer with cascade forward neural network (PO-CFNN-)-based IDS in the IoT environment. The major intention of the PO-CFNN technique is to define the occurrence of intrusions in the IoT environment. The PO-CFNN approach follows three major processes, namely, preprocessing, classification, and parameter optimization. Initially, the networking data is preprocessed to transform them into a useful format. The CFNN technique is employed for the identification and classification of intrusions in the IoT environment. At the final stage, the PO algorithm is applied for optimal adjustment of the parameters involved in the CFNN technique. The experimental validation of the PO-CFNN technique on benchmark dataset stated the better outcomes of the PO-CFNN technique over the recent approaches.

Conflicts of Interest

The author declares that he has no conflicts of interest.

References

[1] R. Kaur, R. K. Ramachandran, R. Doss, and L. Pan, "The importance of selecting clustering parameters in VANETs: a survey," *Computer Science Review*, vol. 40, no. 2021, p. 100392, 2021.

[2] S. Smys, A. Basar, and H. Wang, "Hybrid intrusion detection system for internet of things (IoT)," *Journal of ISMAC*, vol. 2, no. 4, pp. 190–199, 2020.

[3] M. A. Rahman, A. T. Asyhari, L. S. Leong, G. B. Satrya, M. H. Tao, and M. F. Zolkipli, "Scalable machine learning-based intrusion detection system for IoT-enabled smart cities," *Sustainable Cities and Society*, vol. 61, article 102324, 2020.

[4] M. Almiani, A. Abu Ghazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, article 102031, 2020.

[5] M. Zhong, Y. Zhou, and G. Chen, "Sequential model-based intrusion detection system for IoT servers using deep learning methods," *Sensors*, vol. 21, no. 4, p. 1113, 2021.

[6] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset," *IEEE Access*, vol. 9, pp. 142206–142217, 2021.

[7] P. K. Keserwani, M. C. Govil, E. S. Pilli, and P. Govil, "A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model," *Journal of Reliable Intelligent Environments*, vol. 7, no. 1, pp. 3–21, 2021.

[8] M. Ibrahim, "Intelligent differential evolution based feature selection with deep neural network for intrusion detection in wireless sensor networks," *Journal of Intelligent Systems and Internet of Things*, no. 2, pp. 78–89, 2019.

[9] J. Shareena, A. Ramdas, and H. Ap, "Intrusion detection system for IoT botnet attacks using deep learning," *SN Computer Science*, vol. 2, no. 3, pp. 1–8, 2021.

[10] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design-based intrusion detection system using fog computing to protect the internet of things networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9555–9572, 2021.

[11] X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera, and M. Sanz Rodrigo, "An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets," *Sensors*, vol. 21, no. 2, p. 656, 2021.

[12] A. K. Bediya and R. Kumar, "A novel intrusion detection system for internet of things network security," *Journal of Information Technology Research (JITR)*, vol. 14, no. 3, pp. 20–37, 2021.

[13] M. Sarhan, S. Layeghy, and M. Portmann, "Towards a standard feature set for network intrusion detection system datasets," *Mobile Networks and Applications*, vol. 27, no. 1, pp. 1–14, 2022.

[14] P. Nimbalkar and D. Kshirsagar, "Feature selection for intrusion detection system in internet-of-things (IoT)," *ICT Express*, vol. 7, no. 2, pp. 177–181, 2021.

[15] V. Kumar, A. K. Das, and D. Sinha, "UIDS: a unified intrusion detection system for IoT environment," *Evolutionary Intelligence*, vol. 14, no. 1, pp. 47–59, 2021.

[16] M. S. S. Abujazar, S. Fatihah, I. A. Ibrahim, A. E. Kabeel, and S. Sharil, "Productivity modelling of a developed inclined stepped solar still system based on actual performance and using a cascaded forward neural network model," *Journal of Cleaner Production*, vol. 170, pp. 147–159, 2018.

[17] B. Warsito, R. Santoso, and H. Yasin, "Cascade forward neural network for time series prediction," *In Journal of Physics: Conference Series*, vol. 1025, no. 1, p. 12097, 2018.

[18] Q. Askari, I. Younas, and M. Saeed, "Political optimizer: a novel socio-inspired meta-heuristic for global optimization," *Knowledge-Based Systems*, vol. 195, article 105709, 2020.

[19] A. Zhu, Z. Gu, C. Hu, J. Niu, C. Xu, and Z. Li, "Political optimizer with interpolation strategy for global optimization," *Plo S one*, vol. 16, no. 5, article e0251204, 2021.

[20] M. A. Taha, S. E. Assad, A. Queudet, and O. Deforges, "Design and efficient implementation of a chaos-based stream cipher," *Transactions*, vol. 7, no. 2, pp. 89–114, 2017.

[21] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, 2009.

[22] S. Otoum, B. Kantarci, and H. Mouftah, "A comparative study of ai-based intrusion detection techniques in critical infrastructures," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 4, pp. 1–22, 2021.

[23] S. Otoum, B. Kantarci, and H. Mouftah, "Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures," in *2018 IEEE international conference on communications (ICC)*, Kansas City, MO, USA, 2018.

[24] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network intrusion detection combined hybrid sampling with deep hierarchical Network," *Access*, vol. 8, pp. 32464–32476, 2020.

[25] N. Moustafa, *Designing an online and reliable statistical anomaly detection framework for dealing with large high-speed network traffic*, Diss. University of New South Wales, Canberra, Australia, 2017.

[26] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *4th International Conference on Information Systems Security and Privacy (ICISSP)*, Portugal, January 2018.