Journal of King Saud University – Computer and Information Sciences 34 (2022) 8112–8121

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

DRaNN_PSO: A deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things

Jawad Ahmad [a,*], Syed Aziz Shah [b], Shahid Latif [c], Fawad Ahmed [d], Zhuo Zou [c], Nikolaos Pitropakis [a]

[a] *School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK*
[b] *Research Centre for Intelligent Healthcare, Coventry University, UK*
[c] *School of Information Science and Engineering, Fudan University, Shanghai, China*
[d] *Department of Cyber Security, Pakistan Navy Engineering College, NUST, Karachi 75350, Pakistan*

ARTICLE INFO

Article history:
Received 10 June 2022
Revised 3 July 2022
Accepted 29 July 2022
Available online 2 August 2022

Keywords:
Cybersecurity
Deep learning
IIoT
Intrusion detection
Random neural network

ABSTRACT

The Industrial Internet of Things (IIoT) is a rapidly emerging technology that increases the efficiency and productivity of industrial environments by integrating smart sensors and devices with the internet. The advancements in communication technologies have introduced stable connectivity and a higher data transfer rate in the IIoT. The IIoT devices generate a massive amount of information that requires intelligent data processing techniques for the development of cybersecurity mechanisms. In this regard, deep learning (DL) can be an appropriate choice. This paper proposes a Deep Random Neural Network (DRaNN) based fast and reliable attack detection scheme for IIoT environments. The RaNN is an advanced variant of the traditional Artificial Neural Network (ANN) with a highly distributed nature and better generalization capabilities. To attain a higher attack detection accuracy, the proposed RaNN is optimally trained by incorporating hybrid particle swarm optimization (PSO) with sequential quadratic programming (SQP). The SQP-enabled PSO facilitates the neural network to select optimal hyperparameters. The efficacy of the suggested scheme is analyzed in both binary and multiclass configurations by conducting extensive experiments on three new IIoT datasets. The experimental outcomes demonstrates the promising performance of the proposed design for all datasets.

1. Introduction

The IIoT has revolutionized industrial operations by integrating thousands of smart and intelligent devices with advanced communication technologies (Sisinni et al., 2018). In IIoT environments, a massive number of smart devices including sensors, actuators and intelligent modules are connected to the IoT network through a variety of communication infrastructures (Kang-Di et al., 2021). In this context, 5G networks with IIoT systems will help to improve stable connections and reliable communications. The advanced 5G technology has exceptional speed, high availability and low latency, which are the mandatory requirements of modern IIoT systems. The integration of IIoT with 5G enables exceptional flexibility and agility in the management of smart industrial systems that lead to resource efficiency and higher productivity and increased profitability (Peng et al., 2020).

However, this integration also holds the door open for cybercriminals and jeopardizes the integrity of IIoT networks and systems. According to the latest survey of the European Union, the security challenges are expected to increase in 5G-enabled networks. A successful attack on 5G networks might result in undesirable activities and significant repercussions (Moudoud et al., 2020). The trustworthiness of an IIoT system assures that it performs as designed under a set of security circumstances, including security, privacy, safety, resilience, and reliability. The trustworthiness improvement of the IIoT systems can be assured through service, data, and identity protection. Moreover, preventing industrial networks and their associated embedded devices from being infiltrated by hackers are the primary objectives of IIoT systems. (Latif et al., 2021).

Recent cyber threats expose the vulnerabilities of traditional defense frameworks. The techniques used in traditional cyber defense systems are frequently based on static and heuristic

[*] Corresponding author.
E-mail address: J.Ahmad@napier.ac.uk (J. Ahmad).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2022.07.023
1319-1578/

attack signatures and are incapable of detecting new variants of cyberattacks. Artificial intelligence (AI) based intrusion detection systems (IDS) have garnered substantial interest from industry and academics owing to their capacity to effectively learn massive amount of data and identify previously unknown malicious activities (Al-Hawawreh et al., 2020; Khan et al., 2022). In the last few years, a number of intrusion detection schemes have been proposed using machine learning (ML) and shallow learning schemes. By and large, the use of these methodologies has increased detection accuracy. However, these techniques have a few limitations, such as the requirement of human expert interaction at a higher level. Moreover, expert knowledge is an essential requirement to identify useful data and patterns. In addition, a huge volume of training data is required for successful operation, which can be a big challenge in a dynamic and heterogeneous environment (Moustafa et al., 2018). To address the aforementioned issues, deep learning (DL) has emerged as a viable option, having the capability to overcome several limitations of shallow learning. It enables a more in-depth analysis of network data and rapid detection of malicious activities. In addition, DL can be used to construct adaptive attack detection frameworks capable of efficiently dealing with massive, diverse, and unstructured IIoT datasets (Latif et al., 2021).

In this study, a novel DL-based cyberattack detection scheme is proposed for the IIoT. The proposed DL scheme extracts the hidden patterns of cyberattacks from network traffic. It extracts suitable threat patterns automatically, assisting in the understanding and detection of cyber threats, as well as providing appropriate intelligence to classify the type of attack. The main contributions of this study are summarized as follows:

- A fast and efficient DL-based cyberattack detection model is introduced to improve the security and trustworthiness of an IIoT system by using a DRaNN. The RaNN is an advanced version of ANN that efficiently represents the signal propagation in a neural network. Furthermore, its generalization capabilities are much better as compared to other neural networks because of its probability constraints and highly distributed nature.
- A hybrid particle swarm optimization (PSO) with sequential quadratic programming (SQP) is incorporated for the optimal training of DRaNN. PSO has great capability to deal with optimization problems with simplified and fast implementations. Moreover, the addition of SQP enables the PSO to deal with non- nonlinear constrained optimization issues in the systems.
- The proposed scheme is evaluated, and its effectiveness is verified in both binary class and multiclass settings by using three newlyreported IIoT datasets, namely DS2OS (Mahmudul Hasan et al., 2019), UNSW-NB15 (Moustafa and Slay, 2015) and ToN_IoT (Moustafa, 2021).

The rest of the article is structured as follows. Section 2 summarizes some latest DL-based studies for cyberattack detection in IoT/IIoT networks. Section 3 contains detailed mathematical modeling of the proposed DRaNN with PSO based training algorithm. Section 4 presents research methodology including block diagram of the system, datasets description and performance evaluation matrices. Section 5 elaborates on the experimentation platform and simulation results. Section 6 concludes the work and also presents future directions.

2. Related Works

Several DL-based schemes have been proposed and investigated in the research area of network intrusion detection. In the following, some of the most significant and latest DL-based studies are discussed.

Intrusion detection systems (IDSs) play an important role to protect IoT networks. Shone et al. (2018) introduced a non-symmetric deep autoencoder (NDAE) for unsupervised feature learning. A new DL-based IDS using stacked NDAE is presented. The proposed approach was analyzed through the NSL-KDD and KDD Cup 99 datasets. A federated DL technique for anomaly detection in industrial cyber-physical systems (CPS) has been proposed by Li et al. (2020). Using a convolutional neural network (CNN) and a gated recurrent unit (GRU), a federated learning architecture is designed for anomaly detection in industrial CPS. Extensive experiments are performed on a real industrial CPS dataset to evaluate the performance of the developed strategy. Zhou et al. (2020) introduced a variational long short-term memory (VLSTM) scheme for cyberattack detection. An encoder-decoder neural network is employed to learn the low-dimensional feature representations. In addition, to detect intrusions in IoT networks, an estimation network with better feature representation is used. The efficacy of the suggested scheme was analyzed through several performance metrics by conducting experiments on the UNSW-NB15 dataset. The trustworthiness of an IIoT system is a very important factor. Hassan et al. (2020) presented a reliable IDS to improve the trustworthiness of an IIoT network. For cyberattack detection, an ensemble learning technique based on the integration of a random subspace (RS) and a random tree (RT) is proposed. The proposed approach was tested on 15 datasets of a SCADA system. Experimental findings indicated the higher performance of the proposed technique over conventional attack detection models.

To enhance the security of edge-enabled IoT networks, Nie et al. (2021) introduced a generative adversarial network (GAN)-based intrusion detection model. The proposed scheme contains three stages that include feature selection, a GAN-based intrusion detection model, and evaluation. The authors evaluated the performance of the suggested scheme using two datasets, CIC-DDoS2019 and CSE-CIC-IDS2018. Experimental findings indicated the satisfactory performance of the proposed framework for both binary and multiclass configurations. Li et al. (2020) developed a bidirectional LSTM based intrusion detection scheme for IIoT. In the proposed scheme, sequence and stage feature layers are introduced that facilitate the model to learn corresponding attack intervals from the historical data. As compared to some related works, the proposed model demonstrates lower false-positive and false-negative rates. Keerthi Priya and Perumal (2021) proposed a DL-based technique for intrusion detection in wireless networks. Customized rotation forest (CRF) algorithm has been utilized for feature selections. Different types of cyberattacks were classified by the gated recurrent unit (GRU). The performance of the proposed system was analyzed by conducting extensive experiments using the NSL-KDD dataset in both binary and multiclass classifications. Huimin et al. (2021) designed a novel DL-based intrusion detection technique, the Cognitive Memory-guided Auto Encoder (CMAE). This approach utilized a memory module to increase the capacity for storing common feature patterns while retaining the benefits of AE. To achieve higher attack detection performance, feature construction loss and feature sparsity loss has been used. The experimental finding proved the efficiency of the proposed scheme. In another latest study, Khan (2021) presented a convolutional recurrent neural network (CRNN) for cyberattack detection in IoT networks. In the proposed scheme the authors utilized a convolutional neural network (CNN) to obtain the optimal features from the dataset. A recurrent neural network (RNN) is used for intrusion detection. The efficacy of the proposed CRNN was analyzed using the CSE-CIC-DS2018 dataset. The experimental results exhibits the higher attack detection accuracy of the proposed scheme.

From the above discussion, it is concluded that a variety of intrusion detection schemes have been proposed in recent years using DL-based techniques. Despite the fact that most of the proposed schemes have achieved high attack detection accuracy, there is still room for improvements. The main shortcomings of the existing models include reliance on human operators, long training time and manual selection of network configuration parameters. To overcome these limitations, a novel DRaNN model along with PSO is proposed in this paper to detect cyberattacks in IIoT. It is envisaged that the proposed scheme will be a significant contribution towards fast and reliable cyberattack detection in IIoT environments.

3. Mathematical Model of the Proposed DRaNN

Erol Gelenbe (Gelenbe, 1989) suggested a novel class of artificial neural networks (ANNs) referred to as the random neural network (RaNN) with either $+1$ or -1 signals. RaNN can provide more precise representation of a system's states since the neuron's potential is expressed in integer values instead of binary values (Javed et al., 2016; Latif et al., 2020). RaNNs have been extensively employed in multiple applications such as image processing, pattern recognition, modeling and communication systems. However, only a few studies are available related to the implementation of RaNN for intrusion detection applications.

In RaNN, signals are transmitted as impulses between the neurons. If the potential of the receiving signal is positive $(+1)$ or negative (-1), it will represent the excitation or inhibition states, respectively. In RaNN, each neuron f has a state $s_f(t)$ representing its potential at time t. The potential $s_f(t)$ is indicated by a non-negative integer. If $s_f(t) > 0$, then it indicates the excitation state of neuron f and if $s_f(t) = 0$, then neuron f is in an idle state.

During its excited state, the neuron f transmits impulses at the Poisson rate ψ_f. The transmitted signal can approach neuron g as an excitatory or inhibitory signal with probabilities $\varphi^+(f,g)$ or $\varphi^-(f,g)$, respectively. It can also leave the network with probability $\ell(f)$ as shown below

$$\ell(f) + \sum_{j=1}^{N}[\varphi^+(f,g) + \varphi^-(f,g)] = 1\forall_f \tag{1}$$

$$\omega^+(f,g) = \psi_f \varphi^+(f,g) \geqslant 0 \tag{2}$$

$$\omega^-(f,g) = \psi_f \varphi^-(f,g) \geqslant 0 \tag{3}$$

By combining Eqs. (1) to (3)

$$\psi(f) = (1 - d(f))^{-1}\sum_{g=1}^{N}[\omega^+(f,g) + \omega^-(f,g)] \tag{4}$$

The firing rate among neurons is indicated by $\psi(f) = \sum_{g=1}^{N}[\omega^+(f,g) + \omega^-(f,g)]$. Here ω matrices contain non-negative values and describe the product of firing rate and probability. The external positive or negative signals can also reach neuron f with a Poisson rate Λ_f and λ_f respectively. The potential of neuron f will increase to $+1$ when a positive signal is received. The potential of neuron f will decrease to zero if it receives a negative signal in the excitation state. The arrival of a negative signal will have no effect if the potential of the neuron f is already zero.

Consider the vector $S(t) = (s_1(t), \ldots s_n(t))$, where $s_f(t)$ represents neuron potential f and n represents the total number of neurons in the neural network. Assume that S is a continuous-time Markov process. The stationary distribution of S can be expressed as follows:

$$\lim_{t\to\infty} P_\psi(S(t)) = (s_1(t), \ldots, s_n(t)) = \prod_{f=1}^{n}(1 - \delta_f)\delta_f^{sf} \tag{5}$$

for each node f

$$\delta_f = \frac{G_f^+}{\psi_f + G_f^-} \tag{6}$$

where

$$G_f^+ = \Lambda_f + \sum_{g=1}^{N}\delta_g \omega^+(g,f) \tag{7}$$

$$G_i^- = \Lambda_i - \sum_{g=1}^{N}\delta\omega^-(g,f) \tag{8}$$

$\omega^+(g,f)$, and $\omega^-(g,f)$ indicate the positive and negative interconnecting weights among neurons of the g^{th} and f^{th} layers. $\omega^+(g,f)$ and $\omega^-(g,f)$ are equal to 0 for the input layer I. Therefore, δ_f for each layer can be computed by substituting Eqs. (7)and (8) into Eq. (6), where δ_f determines the probability of neuron f excited at time t.

$$\delta_{f\varepsilon I} = \frac{\Lambda_f}{\varphi_f + \lambda_f} \tag{9}$$

$$\delta_{f\varepsilon H} = \frac{\sum_{f\varepsilon I}\delta_f \omega^+(f,\hbar)}{r_\hbar + \sum_{f\varepsilon I}\delta_f \omega^-(f,\hbar)} \tag{10}$$

$$\delta_{f\varepsilon O} = \frac{\sum_{f\varepsilon H}\delta_\hbar \omega^+(\hbar,o)}{r_\hbar + \sum_{f\varepsilon I}\delta_\hbar \omega^-(\hbar,o)} \tag{11}$$

where I, H, and O represent the input, hidden, and output layers.

3.1. Hybrid Particle Swarm Optimization

The majority of researchers have utilized the gradient descent (GD) approach to train the RaNN model. Although the GD method is reasonably straightforward to develop, its zigzag nature may allow it to get stuck around a local minimum in applications with several local minima. To address the optimization problems, evolutionary algorithms can be used. These approaches are superior to gradient-based methods because of the non-requirement of derivative computation and also not being stuck at local minima.

Researchers have used evolutionary algorithms to effectively train the neural networks. In Chau (2006), the authors used the PSO approach for training of a feed-forward neural network and discovered that PSO quickly converges as compared to backpropagation. While the PSO technique is effective at locating the global minima but it may be sluggish to converge to this point. On the other hand, the sequential quadratic programming (SQP) optimization method can identify the optimal weights but it can get stuck at the local minima (Mehmood et al., 2020). In another study (Georgiopoulos et al., 2011), the PSO and differential evolution (DE) algorithms for RaNN training were built and compared to GD and resilient backpropagation (RPROP) methods. The experimental findings demonstrated that the RPROP algorithm outperformed the GD method for a limited number of epochs, and the PSO algorithm proved its higher efficiency over the RPROP approach for generalization. The main objective of the training process is to determine the input–output relationship by altering the weights of the interconnections. In this paper, a hybrid PSO-SQP has been employed for training of the RaNN. The RaNN is trained through the PSO technique to locate the global minima, followed by the SQP optimization technique to converge at the global minima using a viable start point determined by the PSO algorithm.

The process of the adaptive inertial weight (AIW) PSO algorithm is described as follows.

1. Proceed by populating the problem space with d dimensions with a population of K particles with random positions and velocities.
   The position vector is an array of RaNN weights of interconnected I input, H hidden, and O output nodes. D has the dimensions $2(I.H + H.O)$. The position vector is written as $\mathbf{X}_{kd} = \left[\omega f\hbar^{+L1}\omega\hbar o^{+L2}\omega f\hbar^{-L1}\omega\hbar o^{+L2}\right]$ where $1 \leqslant I \leqslant I, 1 \leqslant \hbar \leqslant H$, $1 \leqslant o \leqslant 0$. The weights are randomly distributed throughout $[0;1]$.
2. Using the PSO equation (Eq. 12), each particle from the position in generation s goes to a new place $s+1$. The constant values c_1 and c_2 are set as 2.48 and 1.21, respectively

$$\mathbf{V}_{kd}^{s+1} = w\mathbf{V}_{kd}^{s} + c_1\mathrm{rand}()\left(\partial_{\mathrm{bestd}}^{s} - \mathbf{X}_{kd}^{s}\right) + c_2\mathrm{rand}()\left(\xi_{\mathrm{bestd}}^{s} - \mathbf{X}_{kd}^{s}\right) \tag{12}$$

$$\mathbf{X}_{kd}^{s+1} = \mathbf{X}_{kd}^{s} + \mathbf{V}_{kd}^{s+1} \tag{13}$$

   where $\partial_{\mathrm{bestsd}}$ and ξ_{bestsd} indicates local best and global best for the position vector $\mathbf{X}_{kd}$, respectively

$$w_{kd}^{s} = 1 - \frac{1}{1 + \exp\left(-\alpha.IKA_{kd}^{s}\right)} \tag{14}$$

   where α is a constant in the range of 0 and 1 and IKA_{kd}^{s} is described as

$$IKA = 1 - \frac{\mathbf{X}_{kd}^{s+1} - \partial_{\mathrm{bestd}}^{s}}{\partial_{\mathrm{bestd}}^{s} - \xi_{\mathrm{bestd}}^{s}} + \varepsilon \tag{15}$$

   where ε represents a small position constant.
3. Evaluate the fitness function for each particle as described in (16)

$$E = \frac{1}{2}\sum_{\mathscr{P}=1}^{N}\sum_{o=1}^{o}\left[\delta_o(\varphi) - \delta_{\mathrm{des},o}\right]^2 \tag{16}$$

   here N represents the number of patterns, $\delta_{\mathrm{des},o}$ is the desired output in training pattern, O is the number of output, and $\delta_o(\varphi)$ is the output of the RaNN computed by (9) to (11).
4. Compare the evaluation of particle fitness with its local best ∂_{best}. If the current fitness assessment value is smaller than ∂_{best}, then update it to the current value.
5. Evaluate fitness in comparison to all ∂_{best} members of population K. If ∂_{best} is smaller than ξ_{best} then set ξ_{best} to the array index of the current particle.
6. Calculate the average squared error. Repeat step 2 if the mean squared error (MSE) is greater than the threshold. The learning process is finished when the halting requirements are fulfilled. In this work, the RaNN is trained for 75 iterations using the AIW-PSO method. The weights of the RaNN are tuned using the SQP optimization technique after 75 iterations.

4. The Proposed Architecture

This section presents the detailed architecture of the proposed attack detection scheme. The block diagram of the suggested framework is illustrated in Fig. 1. It contains multiple stages which are described in the following.

4.1. Datasets

The first stage of the suggested design is data collection and observation. The proposed model is trained and analyzed on the three latest security datasets; DS2OS, UNSW-NB15, and ToN_IoT. A short description of each dataset is presented below.

4.1.1. DS2OS

Pahl and Aubet (2018) presented this new generation IIoT security dataset in 2018. This is an open-source dataset that is very useful to evaluate the efficiency of AI-based cybersecurity schemes for smart industries, smart cities and many other IIoT applications. The DS2OS comprises a total of 357952 samples, out of which 347935 are classified as normal samples and 10017 are anomalous values. This dataset contains 13 features and 8 classes. Detailed class distribution of the DS2OS is presented in Fig. 2.

4.1.2. UNSW-NB15

This is also a very useful dataset that was provided by the Cyber Range Lab of the Australian Centre for Cyber Security (Moustafa and Slay, 2016) in 2015. The UNSW-NB15 comprises a total of 257673 samples, out of which 93000 are classified as normal samples and 164673 are malicious samples. This dataset contains 49 features and 10 classes. Detailed class distribution of the UNSW-NB15 is presented in Fig. 3.

4.1.3. ToN_IoT

This is one of the latest datasets for IoT/IIoT applications. It was presented by the Cyber Range and IoT Labs, University of New South Wales, Australia in 2019 (Alsaedi et al., 2020). It is a very useful dataset for evaluation of the efficiency and fidelity of multiple cybersecurity applications based on ML/DL algorithms. The ToN_IoT comprises a total of 1379274 samples, out of which 270279 are classified as normal samples and 1108995 are anomalous values. This dataset contains 10 classes. Fig. 4 shows the ToN IoT dataset's detailed class distribution.

4.2. Data Preparation

The preparation of the dataset is a critical stage that involves data curation before applying it to any AI scheme to expedite the training and attain higher accuracy. Multiple operations are involved at this stage, including the deletion of superfluous features, the transformation of non-numerical characteristics, and the substitution of relevant data for missing values. We used a two-step data preparation procedure for our experiments, which involves pre-processing and normalization.

4.2.1. Pre-processing

Categorical features are transformed into numerical data to ensure their compatibility with the neural network's input. In our experiments, this operation is performed through label encoding. As time, date, and time stamp features have no significant contribution to attack detection, therefore, these features are completely removed.

4.2.2. Normalization

Some features of the dataset containing large values may result in a biased model. These features can decrease the result accuracy. The normalization process transforms all the features in the range of 0.0 to 1.0 while maintaining the data behavior. In our experiments, the min–max scaling technique is used for data normalization.

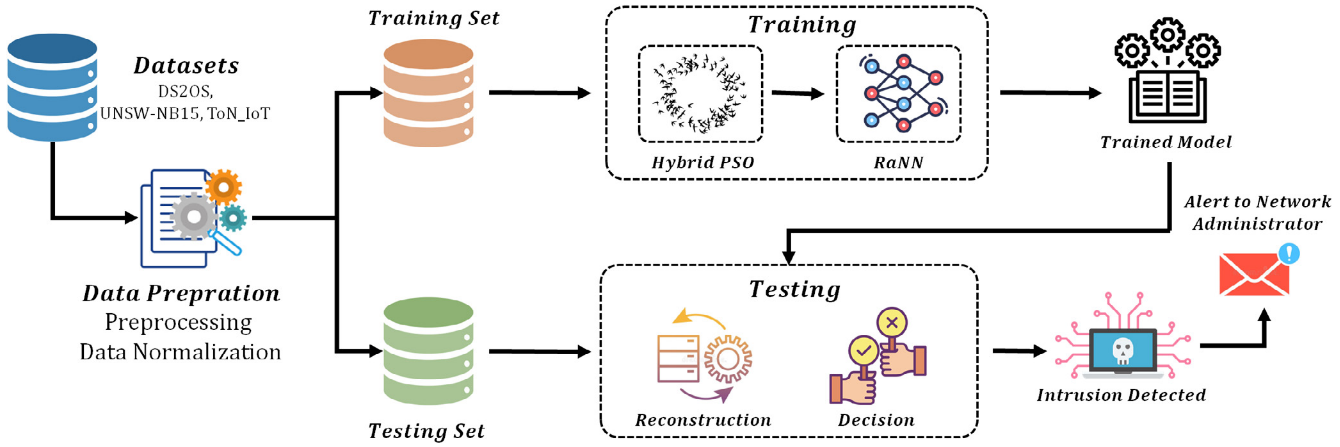


Fig. 1. Block diagram of the proposed intrusion detection scheme.

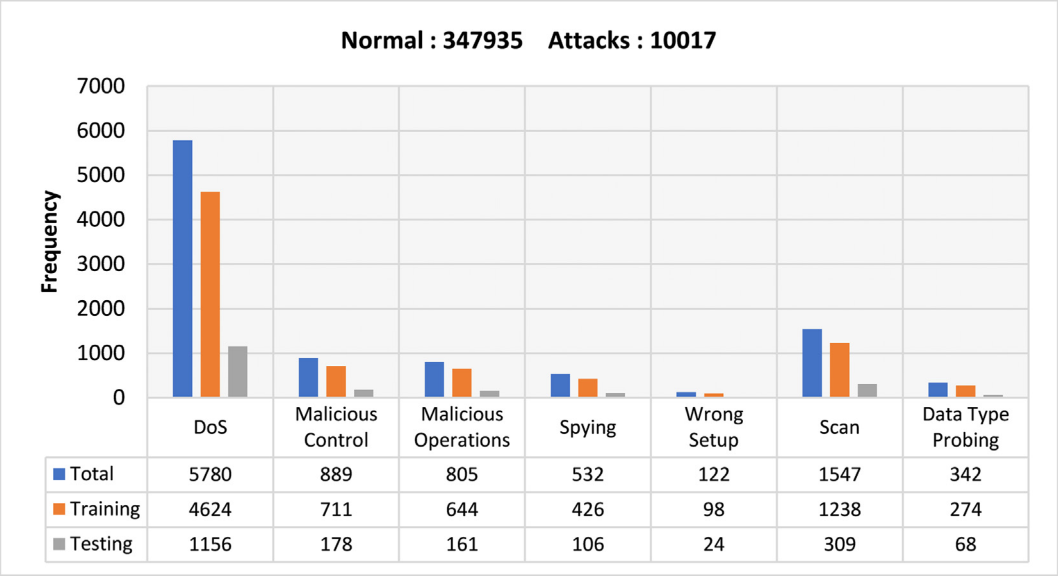


Fig. 2. Class distribution of the DS2OS dataset.

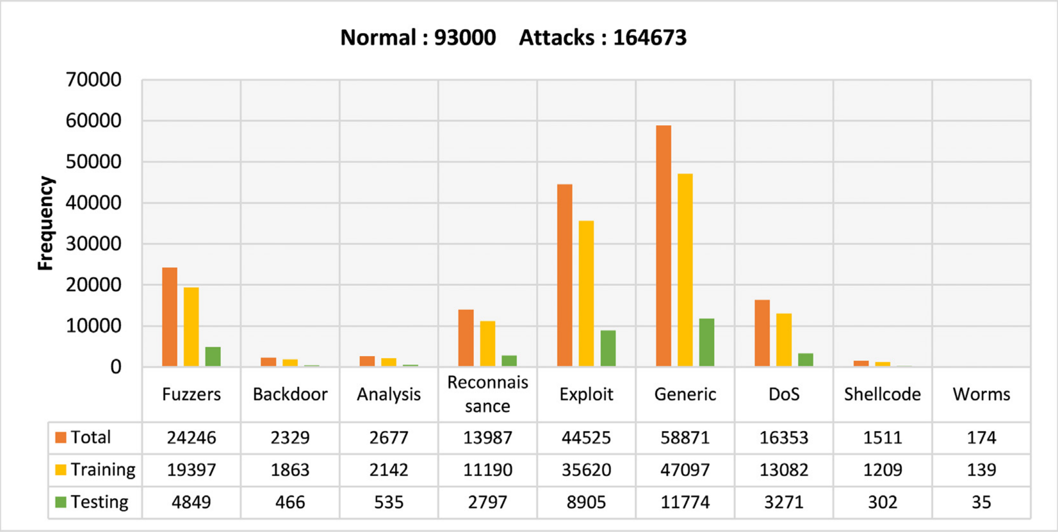
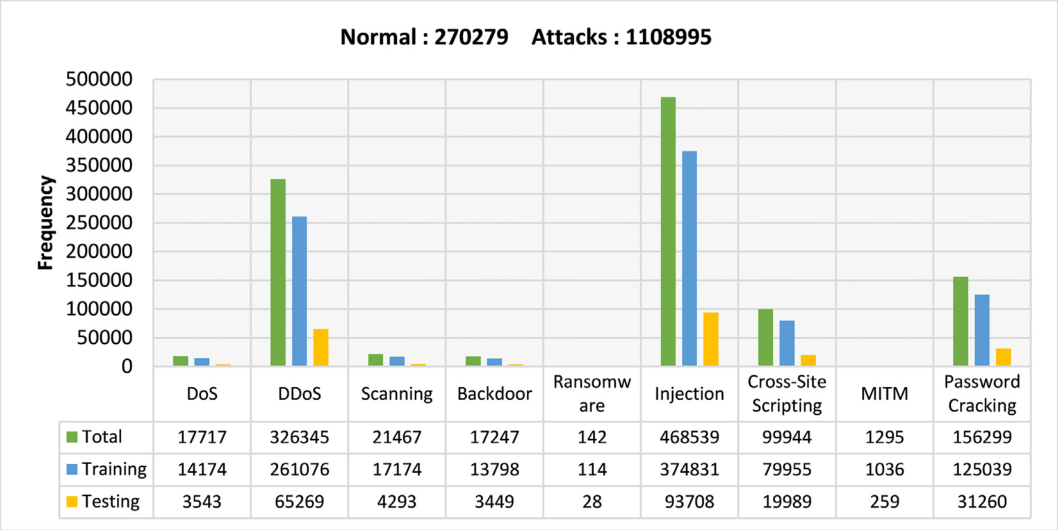


Fig. 3. Class distribution of the UNSW-NB15 dataset.



	DoS	DDoS	Scanning	Backdoor	Ransomware	Injection	Cross-Site Scripting	MITM	Password Cracking
🟩 Total	17717	326345	21467	17247	142	468539	99944	1295	156299
🟦 Training	14174	261076	17174	13798	114	374831	79955	1036	125039
🟨 Testing	3543	65269	4293	3449	28	93708	19989	259	31260

Fig. 4. Class distribution of the ToN_IoT dataset.

4.3. Hyperparameter

These are the important variables that define the network configuration and regulate the training process. In our experiments, the primary architecture of DRaNN is fixed. The hybrid PSO algorithm determines the optimum values of hyperparameters to ensure higher attack detection accuracy. These parameters include learning rate, the number of epochs, momentum, batch size and dropout. The aforementioned parameters are defined in the following. The optimal hyperparameres for all datasets suggested by hybrid PSO algorithm are presented in Table 1.

4.3.1. Learning Rate

The DL algorithm's training speed is controlled by learning rate. A smaller value of learning rate can facilitate better learning but can also increase the training time. A higher learning rate, on the other hand, can enable quick learning but also result in a large errors. In DL model design, choosing an optimal learning rate is a crucial challenge.

4.3.2. Number of Epochs

The number of times the learning algorithm will traverse the entire training set is specified by number of epochs. This parameter decides that how many times the weights of the neural network will be updated.

4.3.3. Momentum

This parameter aids in determining the direction of the following stage depending on the previous stage's knowledge. It contributes to the model's stability by preventing oscillations.

4.3.4. Batch Size

This hyperparameter regulates the number of training samples that are required to be processed before updating the model's internal parameters.

4.3.5. Dropout

It is a regularization approach utilized during training to estimate the number of neurons in a neural network. Dropout allows the model to reduce overfitting, which can aid in making accurate predictions.

4.4. Performance Assessment Parameters

The efficacy of the suggested design was investigated through a number of performance parameters. The predicted outcomes of trained models were compared with the real values. Based on this comparison, True-Positives (TP), False-Positives (FP), True-Negatives (TN), and False-Negatives (FN) were calculated. TP and TN represent the trained model's number of correct predictions for both intrusions and normal behaviors. FP and FN indicate the trained model's inaccurate predictions for intrusions and normal behaviors. The aforementioned parameters are utilized to compute the performance scores in terms of accuracy, precision, recall, and F1 score.

4.4.1. Accuracy

This indicator shows the percentage of correct attacks and normal events predicted. It is simple to compute by dividing the number of correct predictions by the total number of predictions.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{17}$$

Table 1
The utilized hyperparameters for the proposed scheme.

Dataset	Hyperparameters				
	Learning Rate	Epochs	Momentum	Batch Size	Dropout
DS2OS	0.001	75	0.65	128	0.01
USNW-NB15	0.005	75	0.70	64	0.00
ToN_IoT	0.010	75	0.57	256	0.05

4.4.2. Precision

It indicates the fraction of correctly predicted anomalous observations compared to the total number of anomalous observations.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{18}$$

4.4.3. Recall

This statistic estimates the fraction of correctly anticipated abnormal values in comparison to correctly predicted abnormal observations and incorrectly predicted normal observations.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{19}$$

4.4.4. F1 Score

It is defined as the harmonic mean of the model's precision and recall.

$$\text{F1Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{20}$$

5. Experiments and Performance Analysis

This section discusses the experimentation methodology and a brief discussion on the results of the suggested technique.

5.1. Implementation Platform

The proposed scheme is implemented and its performance assessment has been carried out on an HP Z4 G4 Workstation which is equipped with an Intel® Core^{TM} i9-10900X processor and 16 GB DDR4-2933 MHz RAM. An NVIDIA® Quadro RTX^{TM} 4000 graphics card enable the smooth operations of DL algorithms. The proposed DRaNN and PSO-SQP are implemented in the Python language using Anaconda Navigator installed on Windows 10 Professional.

5.2. Discussion on Results

The efficacy of the suggested scheme is analyzed for three datasets in both binary and multiclass scenarios. In our experiments, the 5-fold cross-validation approach is utilized. The k-fold cross-validation approach is the most often used and is primarily used to objectively analyze the performance of different ML/DL algorithms. In the following, the experimental findings of each dataset are briefly analyzed.

5.2.1. Performance evaluation for the DS2OS Dataset

In our experiments, the train-test split ratio for the DS2OS dataset is selected as 80:20. The optimal hyperparameters are tuned by a hybrid PSO-SQP algorithm as shown in Table 1. The 11 most prominent features are selected as the input of the intrusion detection model and simulation is executed for 75 epochs. First, we analyze the performance for the binary class scenario. For 5-fold cross-validation, the training set is divided into five groups based on the number of samples. The experimental results for each fold are presented in Table 2. According to the results, the proposed DRaNN achieved the highest attack detection accuracy in the fifth fold with the maximum number of samples. The train and test accuracies for this fold are achieved as 98.97% and 98.64%, respectively. For the first fold, the proposed algorithms attained the lowest train and test accuracies which are 96.25% and 95.97%, respectively. The main reason for lower attack detection accuracy was the minimum number of samples in this fold. For the other 3 folds, the attack detection accuracies achieved are 97.89%, 97.31%, and 98.10%. For the fifth fold, all the other performance assessment score, precision, recall and F1 confirm higher attack detection performance of the proposed DRaNN for the DS2OS dataset.

In multiclass classification experiments for this dataset, the DRaNN successfully classified 8 different types of classes with higher attack detection accuracy. The experimental findings of multiclass classification for the DS2OS dataset are presented in Fig. 5. According to the results, the DRaNN accurately classified "DoS", "scan" and "wrong setup" with the accuracies of 99.01%, 98.57%, and 98.51%, respectively. The attack detection accuracies for "malicious operation", "spying", "malicious control" and "data type probing" are observed as 98.42%, 98.60%, 98.12%, and 98.35%, respectively. The "normal" class attained the accuracy of 98.54% and the remaining 1.46% samples of this class are classified as malicious entities. The average attack detection accuracy for multiclass classification is achieved as 98.52%.

5.2.2. Performance evaluation for the UNSW-NB15 Dataset

For the UNSW-NB dataset, the train-test split ratio is the same as used for the first dataset. The utilized hyperparameters for this dataset are shown in Table 1. The 41 most prominant features are selected as the input of the DRaNN and simulation is executed for 75 epochs. First, we analyze the performance for the binary class scenario. The same 5-fold cross-validation is used for this dataset. The experimental results for each fold are presented in Table 3. According to the results, the DRaNN achieved the highest attack detection accuracy in the fifth fold with the maximum number of samples. The train and test accuracies for this fold are achieved as 99.48% and 99.12%, respectively. Again, for the first fold, the proposed algorithms attained the lowest train and test accuracies, which are 95.98% and 95.46%, respectively. For the other 3 folds, the attack detection accuracies achieved are 97.22%, 98.76%, and 98.28%. For the fifth fold, all the other performance assessment score such as precision, recall and F1 confirm the promising performance of the DRaNN for the UNSW-NB15 dataset.

In multiclass classification experiments for this dataset, the DRaNN successfully classified 10 different types of classes with

Table 2
Performance comparison for the DS2OS dataset in the binary class scenario.

Performance Indicators		5-Fold Cross-Validation				
		Fold 1	Fold 2	Fold 3	Fold 4	Fold 5
Training	Accuracy	0.9625	.09792	0.9774	0.9843	0.9897
	Precision	0.9682	0.9805	0.9777	0.9861	0.9903
	Recall	0.9621	0.9794	0.9769	0.9847	0.9884
	F1 Score	0.9651	0.9799	0.9773	0.9854	0.9893
Testing	Accuracy	0.9597	0.9789	0.9731	0.9810	0.9864
	Precision	0.9621	0.9801	0.9750	0.9829	0.9899
	Recall	0.9603	0.9780	0.9742	0.9799	0.9861
	F1 Score	0.9612	0.9790	0.9746	0.9814	0.9880

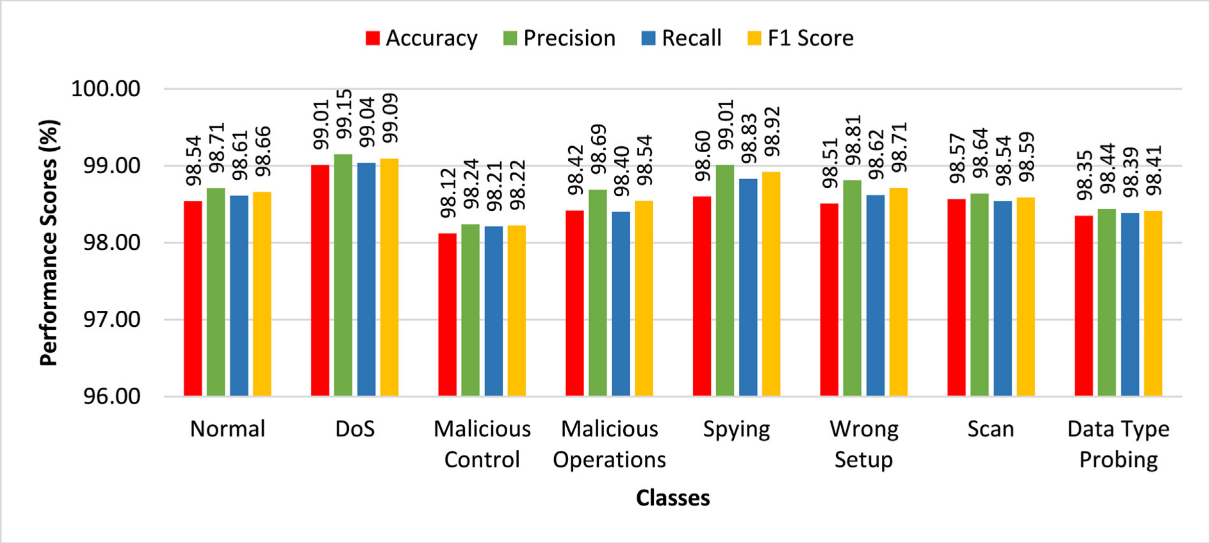


Fig. 5. Performance comparison for DS2OS dataset in the multiclass scenario.

Table 3
Performance comparison for the UNSW-NB15 dataset in the binary class scenario.

Performance Indicators		**5-Fold Cross-Validation**				
		Fold 1	**Fold 2**	**Fold 3**	**Fold 4**	**Fold 5**
Training	Accuracy	0.9598	0.9794	0.9892	0.9867	0.9948
	Precision	0.9609	0.9811	0.9907	0.9899	0.9953
	Recall	0.9579	0.9790	0.9884	0.9851	0.9950
	F1 Score	0.9594	0.9800	0.9895	0.9875	0.9951
Testing	Accuracy	0.9546	0.9722	0.9876	0.9828	0.9912
	Precision	0.9587	0.9761	0.9877	0.9837	0.9927
	Recall	0.9575	0.9759	0.9864	0.9824	0.9908
	F1 Score	0.9581	0.9760	0.9870	0.9830	0.9917

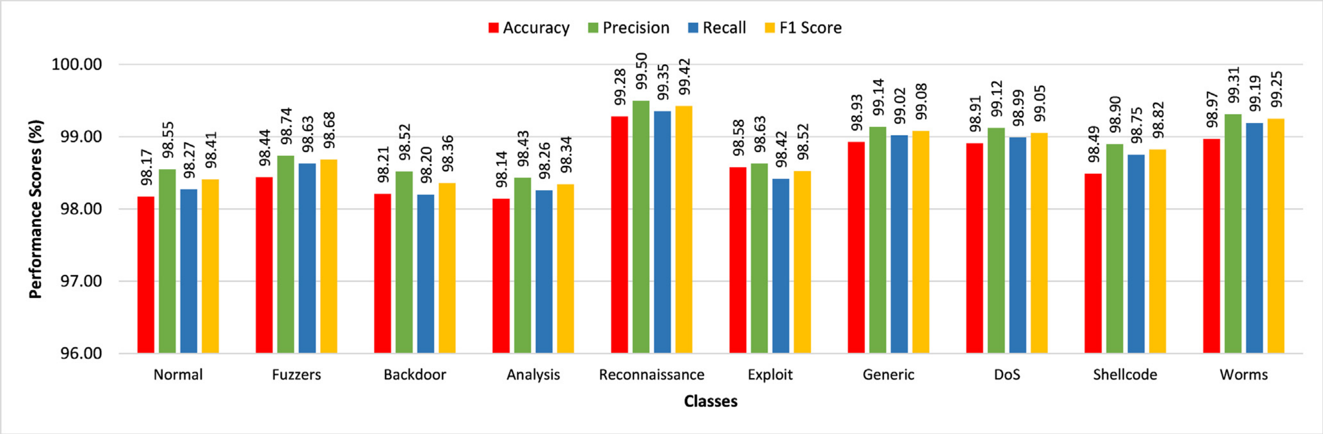


Fig. 6. Performance comparison for UNSW-NB15 dataset in the multiclass scenario.

higher attack detection accuracy. The experimental findings of multiclass classification for the UNSW-NB15 dataset are shown in Fig. 6. According to the results, the DRaNN accurately classified "reconnaissance", "generic" and "worms" with the higher accuracies of 99.28%, 98.93%, and 98.97%, respectively. The "DoS" and "exploits" attained the accuracies of 99.11% and 98.58%, respectively. The attack detection accuracies for "analysis", "backdoor", "fuzzer" and "shellcode" are observed in the range of 98.14% and 98.49%. The "normal" class attained the accuracy of 98.17% and the remaining 1.83% samples of this class are classified as malicious entities. The average attack detection accuracy for multiclass classification is achieved as 98.61%.

5.2.3. Performance evaluation for the ToN_IoT Dataset

The train-test ratio is maintained for the ToN_IoT dataset as used for the other two datasets. The utilized hyperparameters for this dataset are presented in Table 1. A total of 22 most significant features are selected as the input of the DRaNN and simulation is executed for 75 epochs. First, we analyze the performance for the binary class scenario. The same 5-fold cross-validation is used for

Table 4
Performance comparison for the ToN_IoT dataset in the binary class scenario.

Performance Indicators		5-Fold Cross-Validation				
		Fold 1	**Fold 2**	**Fold 3**	**Fold 4**	**Fold 5**
Training	Accuracy	0.9662	0.9864	0.9856	0.9941	0.9972
	Precision	0.9667	0.9843	0.9868	0.9951	0.9981
	Recall	0.9964	0.9849	0.9859	0.9946	0.9969
	F1 Score	0.9813	0.9846	0.9863	0.9948	0.9975
Testing	Accuracy	0.9619	0.9858	0.9812	0.9909	0.9957
	Precision	0.9672	0.9897	0.9836	0.9917	0.9966
	Recall	0.9651	0.9871	0.9821	0.9913	0.9959
	F1 Score	0.9661	0.9884	0.9828	0.9915	0.9962

this dataset. The experimental results for each fold are presented in Table 4. The experimental findings indicate that the DRaNN achieved the highest attack detection accuracy in the fifth fold with the maximum number of samples. The train and test accuracies for this fold are achieved as 99.72% and 99.57%, respectively. Again, for the first fold, the proposed algorithms attained the lowest train and test accuracies as 96.62% and 96.19%, respectively. For the other 3 folds, the attack detection accuracies are achieved as 98.58%, 98.12%, and 99.09%. For the fifth fold, all the other performance assessment score such as precision, recall and F1 confirm the higher performance of the DRaNN for the ToN_IoT dataset.

In multiclass classification experiments for this dataset, the DRaNN successfully classified 10 different types of classes with higher attack detection accuracy. The experimental outcomes of multiclass classification for the ToN_IoT dataset are presented in Fig. 7. The results indicates that the DRaNN accurately classified “DoS”, “DDoS”, “ransomware” and “MTM” with the higher accuracies of 99.51%, 99.61%, 99.05%, and 99.19%, respectively. The “backdoor”, “cross-site scripting”, and “password cracking” attained the accuracies of 98.53%, 98.92% and 98.41%, respectively. The attack detection accuracies for “injection”, and “scanning” are observed as 98.52% and 98.49% respectively. The “normal” class attained the accuracy of 98.56% and the remaining 1.44% samples of this class are classified as malicious entities. The average attack detection accuracy for multiclass classification is achieved as 98.88%.

The overall performance of the suggested DRaNN model is optimum for these datasets. The experimental outcomes of this research shows that the DRaNN achieved higher attack detection

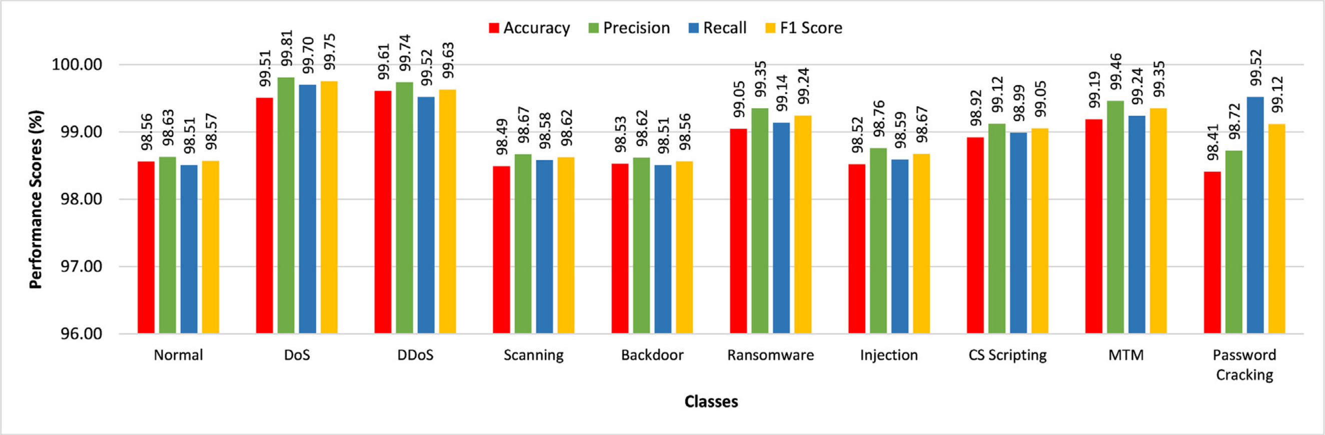


Fig. 7. Performance comparison for ToN_IoT dataset in the multiclass scenario.

Table 5
Performance comparison with stae-of-the-art IDSs.

Reference	Proposed Scheme	Utilized Dataset	Hyperparameters Selection	Evaluation		Accuracy
				Binary Class	Multiclass	
Shone et al. (2018)	NDAE	KDD Cup ’99 and NSL-KDD	No	Yes	Yes	97.85%, 85.42%
Li et al. (2020)	CNN-GRU	Real Industrial CPS	Yes	Yes	No	99.20%
Zhou et al. (2020)	VLSTM	UNSW-NB15	No	Yes	No	89.50%
Hassan et al. (2020)	RSRT	SCADA Dataset	Yes	Yes	No	96.78%
Nie et al. (2021)	GAN	CIC-DDoS2019, CSE-CIC-IDS2018	Yes	Yes	Yes	98.53%, 95.32%
Li et al. (2020)	B-MLSTM	CTU-13, Gas–Water, AWID	No	Yes	No	95.01%, 93.41% 97.58%
Keerthi Priya and Perumal (2021)	GRU	NSL-KDD	No	Yes	Yes	97.32%, 97.32%
Huimin et al. (2021)	CMAE	KDDCUP	No	Yes	Yes	96.67%
Khan (2021)	CRNN	CSE-CIC-DS2018	No	Yes	No	97.75%
The proposed scheme	**DRaNN**	**DS2OS, UNSW-NB15, TON_IoT**	**Yes**	**Yes**	**Yes**	**98.64%, 99.12%, 99.57%**

accuracies for the ToN_IoT dataset in both binary and multiclass settings as compared to the other two datasets.

5.2.4. Performance Comparison with State-of-the-art IDSs

The performance of the proposed intrusion detection scheme is compared to several state-of-the-art IDSs. The performance is analyzed based on the DL scheme, utilized dataset, hyperparameter selection, evaluation criteria, and attack detection accuracy. A detailed performance comparison is presented in Table 5. First, most of the related works utilized the old generation datasets that generally do not represent the true IIoT environment. We utilized three new generation IIoT datasets for experimentation and performance evaluation. Second, only three works utilized the pre-defined hyperparameters. In the proposed scheme PSO-SQP is utilized to obtain optimal hyperparameters. Third, most of the schemes focus on binary class evaluation and there is a lack of multiclass evaluation. The suggested scheme is evaluated for both binary and multiclass configurations. Finally, the proposed IDS attained higher attack detection accuracy as compared to all other schemes.

6. Conclusion

In this article, a novel DRaNN architecture is proposed for intrusion detection and trustworthiness improvements in IIoT environments. A hybrid particle swarm optimization (PSO) with sequential quadratic programming (SQP) is incorporated to tune the hyperparameters for the proposed scheme. The proposed PSO-SQP based optimization method ensured optimum attack detection performance for all datasets used in this work. To analyze the efficacy of the proposed framework, extensive experimentation was performed on three new generation IIoT security datasets, namely DS2OS, UNSW-NB15 and ToN_IoT. The performance of the DRaNN was assessed through a number of performance metrics for both binary class and multiclass scenarios. In binary class classification experiments, DS2OS, UNSW-NB15 and ToN_IoT attained the attack detection accuracy of 98.64%, 99.12%, and 99.57%, respectively. In the multiclass scenario, the DRaNN successfully classified 22 different types of attacks with higher attack detection accuracies. In future, we intend to combine the deep RaNN with traditional conventional neural networks (CNN) to propose a novel hybrid scheme for higher accuracy and real-time detection of intrusion in IIoT.

Declaration of Competing 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.

References

Al-Hawawreh, Muna, Moustafa, Nour, Garg, Sahil, Shamim Hossain, M., 2020. Deep learning-enabled threat intelligence scheme in the internet of things networks. IEEE Trans. Network Sci. Eng. 8 (4), 2968–2981.

Alsaedi, Abdullah, Moustafa, Nour, Tari, Zahir, Mahmood, Abdun, Anwar, Adnan, 2020. Ton_iot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems. IEEE Access 8, 165130–165150.

Chau, Kwok Wing, 2006. Particle swarm optimization training algorithm for anns in stage prediction of shing mun river. J. Hydrol. 329 (3–4), 363–367.

Gelenbe, Erol, 1989. Random neural networks with negative and positive signals and product form solution. Neural computation 1 (4), 502–510.

Georgiopoulos, Michael, Li, Cong, Kocak, Taskin, 2011. Learning in the feed-forward random neural network: A critical review. Performance Evaluation 68 (4), 361–384.

Hassan, Mohammad Mehedi, Gumaei, Abdu, Huda, Shamsul, Almogren, Ahmad, 2020. Increasing the trustworthiness in the industrial iot networks through a reliable cyberattack detection model. IEEE Trans. Industr. Inf. 16 (9), 6154–6162.

Huimin, Lu., Wang, Tian, Xing, Xu., Wang, Ting, 2021. Cognitive memory-guided autoencoder for effective intrusion detection in internet of things. IEEE Trans. Industr. Inf. 18 (5), 3358–3366.

Javed, Abbas, Larijani, Hadi, Ahmadinia, Ali, Gibson, Des, 2016. Smart random neural network controller for hvac using cloud computing technology. IEEE Trans. Industr. Inf. 13 (1), 351–360.

Kang-Di, Lu., Zeng, Guo-Qiang, Luo, Xizhao, Weng, Jian, Luo, Weiqi, Yongdong, Wu., 2021. Evolutionary deep belief network for cyber-attack detection in industrial automation and control system. IEEE Trans. Industr. Inf. 17 (11), 7618–7627.

Keerthi Priya, L., Perumal, Varalakshmi, 2021. A novel intrusion detection system for wireless networks using deep learning. In: Proceedings of International Joint Conference on Advances in Computational Intelligence. Springer, pp. 485–494.

Khan, Muhammad Ashfaq, 2021. Hcrnnids: hybrid convolutional recurrent neural network-based network intrusion detection system. Processes 9 (5), 834.

Muhammad Almas Khan, Muazzam A Khan Khattk, Shahid Latif, Awais Aziz Shah, Mujeeb Ur Rehman, Wadii Boulila, Maha Driss, and Jawad Ahmad. Voting classifier-based intrusion detection for iot networks. In Advances on Smart and Soft Computing, pages 313–328. Springer, 2022.

Latif, Shahid, Zou, Zhuo, Idrees, Zeba, Ahmad, Jawad, 2020. A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. IEEE Access 8, 89337–89350.

Latif, Shahid, Idrees, Zeba, Ahmad, Jawad, Zheng, Lirong, Zou, Zhuo, 2021. A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things. J. Ind. Inform. Integration 21, 100190.

Shahid Latif, Zil e Huma, Sajjad Shaukat Jamal, Fawad Ahmed, Jawad Ahmad, Adnan Zahid, Kia Dashtipour, Muhammad Umar Aftab, Muhammad Ahmad, and Qammer Hussain Abbasi. Intrusion detection framework for the internet of things using a dense random neural network. IEEE Transactions on Industrial Informatics, 2021.

Li, Beibei, Yuhao, Wu., Song, Jiarui, Rongxing, Lu., Li, Tao, Zhao, Liang, 2020. Deepfed: Federated deep learning for intrusion detection in industrial cyber–physical systems. IEEE Trans. Industr. Inf. 17 (8), 5615–5624.

Li, Xinghua, Mengfan, Xu., Vijayakumar, Pandi, Kumar, Neeraj, Liu, Ximeng, 2020. Detection of low-frequency and multi-stage attacks in industrial internet of things. IEEE Trans. Veh. Technol. 69 (8), 8820–8831.

Mahmudul Hasan, Md., Milon Islam, Md., Zarif, Ishrak Islam, Hashem, M.M.A., 2019. Attack and anomaly detection in iot sensors in iot sites using machine learning approaches. Internet of Things 7, 100059.

Mehmood, Ammara, Zameer, Aneela, Ling, Sai Ho, Raja, Muhammad Asif Zahoor, et al., 2020. Integrated computational intelligent paradigm for nonlinear electric circuit models using neural networks, genetic algorithms and sequential quadratic programming. Neural Comput. Appl. 32 (14), 10337–10357.

Moudoud, Hajar, Khoukhi, Lyes, Cherkaoui, Soumaya, 2020. Prediction and detection of fdia and ddos attacks in 5g enabled iot. IEEE Network 35 (2), 194–201.

Moustafa, Nour, 2021. A new distributed architecture for evaluating ai-based security systems at the edge: Network ton_iot datasets. Sustainable Cities Society 72, 102994.

Moustafa, Nour, Slay, Jill, 2015. Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 military communications and information systems conference (MilCIS). IEEE, pp. 1–6.

Moustafa, Nour, Slay, Jill, 2016. The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set. Inform. Security J.: Global Perspective 25 (1–3), 18–31.

Moustafa, Nour, Misra, Gaurav, Slay, Jill, 2018. Generalized outlier gaussian mixture technique based on automated association features for simulating and detecting web application attacks. IEEE Transactions on Sustainable Computing 6 (2), 245–256.

Nie, Laisen, Yixuan, Wu., Wang, Xiaojie, Guo, Lei, Wang, Guoyin, Gao, Xinbo, Li, Shengtao, 2021. Intrusion detection for secure social internet of things based on collaborative edge computing: a generative adversarial network-based approach. IEEE Trans. Comput. Social Syst. 9 (1), 134–145.

Marc-Oliver Pahl and François-Xavier Aubet. Ds2os traffic traces iot traffic traces gathered in a the ds2os iot environment, 2018. URL:https://www.kaggle.com/francoisxa/ds2ostraffictraces.

Peng, Yu., Yang, Mo, Xiong, Ao, Ding, Yahui, Li, Wenjing, Qiu, Xuesong, Meng, Luoming, Kadoch, Michel, Cheriet, Mohamed, 2020. Intelligent-driven green resource allocation for industrial internet of things in 5g heterogeneous networks. IEEE Trans. Industr. Inf. 18 (1), 520–530.

Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi. A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1):41–50, 2018.

Sisinni, Emiliano, Saifullah, Abusayeed, Han, Song, Jennehag, Ulf, Gidlund, Mikael, 2018. Industrial internet of things: Challenges, opportunities, and directions. IEEE Trans. Industr. Inf. 14 (11), 4724–4734.

Zhou, Xiaokang, Yiyong, Hu., Liang, Wei, Ma, Jianhua, Jin, Qun, 2020. Variational lstm enhanced anomaly detection for industrial big data. IEEE Trans. Industr. Inf. 17 (5), 3469–3477.