Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.036822
Article

Optimal Wavelet Neural Network-Based Intrusion Detection in Internet of Things Environment

Heba G. Mohamed[1], Fadwa Alrowais[2], Mohammed Abdullah Al-Hagery[3], Mesfer Al Duhayyim[4,*], Anwer Mustafa Hilal[5] and Abdelwahed Motwakel[5]

[1]Department of Electrical Engineering, College of Engineering, Princess Nourah bint Abdulrahman University, P.O. Box, 84428, Riyadh 11671, Saudi Arabia
[2]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box, 84428, Riyadh 11671, Saudi Arabia
[3]Department of Computer Science, College of Computer, Qassim University, Saudi Arabia
[4]Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj, 16273, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Mesfer Al Duhayyim. Email: m.alduhayyim@psau.edu.sa
Received: 13 October 2022; Accepted: 17 February 2023

Abstract: As the Internet of Things (IoT) endures to develop, a huge count of data has been created. An IoT platform is rather sensitive to security challenges as individual data can be leaked, or sensor data could be used to cause accidents. As typical intrusion detection system (IDS) studies can be frequently designed for working well on databases, it can be unknown if they intend to work well in altering network environments. Machine learning (ML) techniques are depicted to have a higher capacity at assisting mitigate an attack on IoT device and another edge system with reasonable accuracy. This article introduces a new Bird Swarm Algorithm with Wavelet Neural Network for Intrusion Detection (BSAWNN-ID) in the IoT platform. The main intention of the BSAWNN-ID algorithm lies in detecting and classifying intrusions in the IoT platform. The BSAWNN-ID technique primarily designs a feature subset selection using the coyote optimization algorithm (FSS-COA) to attain this. Next, to detect intrusions, the WNN model is utilized. At last, the WNN parameters are optimally modified by the use of BSA. A widespread experiment is performed to depict the better performance of the BSAWNN-ID technique. The resultant values indicated the better performance of the BSAWNN-ID technique over other models, with an accuracy of 99.64% on the UNSW-NB15 dataset.

Keywords: Internet of things; wavelet neural network; security; intrusion detection; machine learning

1 Introduction

With the recent advancements in wireless communication technology that have increased Internet of Things (IoT) systems, several security threats are now ravaging IoT platforms, causing damage to the data [1]. And with the enormous applications of IoT platforms, guaranteeing that cyberattacks were being holistically identified to evade harm was vital [2]. If a system is under attack is paramount since prevention of the attack will be mandatory. Therefore, it grabs the high interest of authors to do more research in the intrusion detection system (IDS) field [3]. IDS will monitor network traffic flow for privacy violations and possible cyberattacks at various layers of the network and thwarts monitored attacks from happening [4]. Technological developments have led to augmented data collection sources in the IoT platform ranging from smart grids to network devices like switches, routers, hubs, smart devices, smart homes, etc. [5]. Data accumulated from such network nodes or end devices depends on the modes included in traffic monitoring. In IDS, there exist 3 modes of monitoring network traffic flow: network-oriented, hybrid, and host-oriented techniques [6].

A recent study on IDSs related to abnormal behaviours was conducted to detect outliers by learning intrusion detection (ID) data in integration with the machine learning (ML) approach [7]. Such conventional security detection methods were ineffective since the invader continually updated attack methods and leveraged advanced hacking approaches [8]. For example, security policies are eluded whenever the invader executes reverse engineering, like firewall configurations, routers, and network surveillance. The authors have started to explore deep learning (DL) and ML solutions to boost attack recognition [9]. The advent of processing and computing capabilities permits the employment of the DL and ML approaches at scale and estimates the attack events precisely. Intellectual IDS solutions were modelled in the literature for attack detection in classical networks using DL and ML approaches [10].

This article introduces a new Bird Swarm Algorithm with Wavelet Neural Network for Intrusion Detection (BSAWNN-ID) in an IoT environment. The major intention of the BSAWNN-ID technique lies in detecting and classifying intrusions in the IoT platform. To attain this, the BSAWNN-ID technique primarily designs a feature subset selection using a coyote optimization algorithm (FSS-COA). Next, to detect intrusions, the WNN model is utilized. At last, the WNN parameters are optimally modified by the use of BSA. A widespread experiment is performed to depict the better performance of the BSAWNN-ID technique.

2 Related Works

In [11], a hybrid ML technique named extreme gradient boosting with random forest (XGB-RF) was presented to detect intrusion attacks. The presented hybrid system can be executed to the N-BaIoT database comprising hazardous botnet attacks. RF has been utilized for feature selection (FS), and XGB classification is employed to detect attacks on IoT platforms. Fenanir et al. [12] generate a lightweight IDS dependent upon 2 ML approaches, feature selection (FS) and feature classifier. The FS is recognized by the filter-based approach, recognition of their comparatively minimal computing cost. The feature classifier approach for our system can be recognized with a comparative analysis.

In [13], a new hybrid weighted deep belief network (HW-DBN) technique was presented to create a productive and dependable IDS (DeepIoT.IDS) approach for detecting present and new cyberattacks. The HW-DBN system combines an improved Gaussian–Bernoulli restricted Boltzmann machine (Deep GB-RBM) feature learning function with a weighted deep neural network (WDNN) technique. In [14], an ensemble ID system was presented for mitigating malicious events in specific botnet attacks employed from IoT networks. A novel statistical flow feature is created in the protocols dependent

upon analyzing its potential properties. Afterwards, an AdaBoost ensemble learning approach was established employing 3 ML approaches, such as Naïve Bayes (NB), artificial neural network (ANN), and decision tree (DT), for evaluating the effect of these features and identifying malicious events efficiently.

Albulayhi et al. [15] present and executes a new FS and extracting system for anomaly-related IDS. This technique starts with utilizing 2 entropy-related techniques (gain ratio (GR) and information gain (IG)) for selecting and extracting relevant features from several ratios. Afterwards, the mathematical set model (union and intersection) is employed for extracting an optimum feature. Saheed et al. [16] examine an ML-related IDS (ML-IDS) to detect IoT network attacks. During the primary step of this study approach, feature scaling is done utilizing the min-max normalization method on the UNSW-NB15 database to limit data leakage on the test dataset. During the next step, dimensionality reduction can be executed with Principal Component Analysis (PCA). Finally, six presented ML techniques can be employed to investigate.

3 The Proposed Model

In this article, we have developed a novel BSAWNN-ID technique in the IoT platform. The main intention of the BSAWNN-ID technique lies in the recognition and classification of intrusions in the IoT platform. To attain this, the BSAWNN-ID technique designed the FSS-COA for feature subset election. Next, to detect intrusions, the WNN model is utilized. At last, the WNN parameters are optimally modified by the use of BSA. Fig. 1 represents the working process of the BSAWNN-ID system.

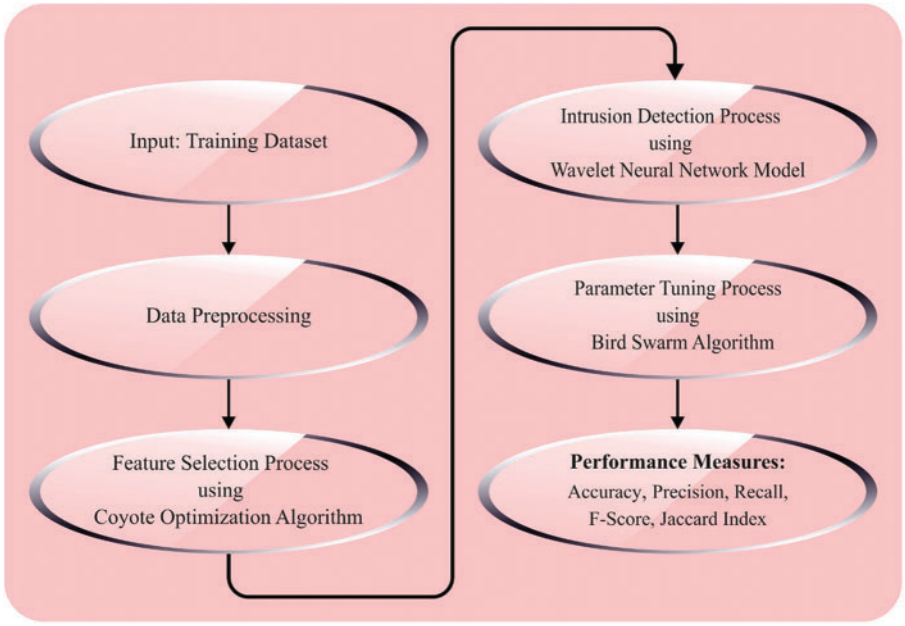

Figure 1: Working process of BSAWNN-ID system

3.1 Design of FSS-COA Model

In this work, the FSS-COA is derived from selecting features from the input data. COA is a meta-heuristic algorithm determined to tackle real-time optimization problems [17]. In the presented method, each one tries to discover the search space. Like the member of the colony, each was executing the duty. There exist 4 types of chimps exist: driver, attacker, chaser, and barrier. The driving and chasing are demonstrated in Eqs. (1) and (2). Where t indicates the existing iteration count, a, m, and c denote the parameter vector, X_{prey} determines the prey location, and X_{chimp} denotes the chimp location. a, c and m variables are evaluated as follows:

$$d = \left| c \,.\, X_{prey}(t) - m \,.\, X_{chimp}(t) \right| \tag{1}$$

$$X_{chimp}(t+1) = X_{prey}(t) - a \,.\, d \tag{2}$$

$$a = 2 \,.\, f \,.\, r_1 - a \tag{3}$$

$$c = 2 \,.\, r_2 \tag{4}$$

$$m = Chaotic\_Value \tag{5}$$

f was nonlinearly reduced in [2.5–0] through a chaotic vector. r_1 and r_2 denote the arbitrary vector within [0,1]. In addition, m indicates the chaotic vector evaluated by different chaotic maps. The chimp group employed different techniques for upgrading f, T indicates the maximal iteration count, and t denotes the existing iteration.

The research assumed that the attacker location is the prey location. The driver place, chase, and barrier are modified through the attacker's location. The 4 optimal solutions are stored, and other chimps upgrade the location according to the optimal chimp location.

$$\begin{aligned} d_{Attacker} &= |c_1 X_{Attacker} - m_1 X|, \\ d_{Barrier} &= |c_2 X_{Barrier} - m_2 X|, \\ d_{Chaser} &= |c_3 X_{Chaser} - m_3 X|, \\ d_{Driver} &= |c_4 X_{Driver} - m_4 X| \end{aligned} \tag{6}$$

$$X_1 = X_{Attacker} - a_1(d_{Attacker}), X_2 = X_{Barrier} - a_2(d_{Barrier})$$

$$X_3 = X_{Chaser} - a_3(d_{Chaser}), X_4 = X_{Driver} - a_4\left(d_{Driver}\right) \tag{7}$$

$$x(t+1) = \frac{x_1 + x_2 + x_3 + x_4}{4} \tag{8}$$

If $|a| > 1$, chimp forces to deviate in prey (avoid optimal local trap), and if $|a| <$ chimp forces to converge at prey location (global optima), c indicates the arbitrary integer from 0 and 2 that provides arbitrary weight to the prey for supporting ($c > 1$) or decreasing ($c < 1$) the effects of location prey. The chaotic map exploited for improving the COA efficacy:

$$X_{chimp}(t+1) = \begin{cases} X_{prey}(t) - a \,.\, d & \mu < 0.5 \\ Chaotic\_Value & \mu > 0.5 \end{cases} \tag{9}$$

From the expression, μ indicates the arbitrary integer from 0 and 1. To achieve this, COA was initialized through the arbitrary population of chimps. Then, each chimp modifies *the f* variable through the particular group technique. As well, each applicant solution modifies the distance. In addition, *c* and *m* avoid local optimal. Furthermore, *f* has decreased in [2.5–0] to boost the exploitation process.

The fitness function (FF) employed in the projected method was planned to take a balance between the number of particular features in all the solutions (lower) and classifier accuracy (higher) attained by employing these particular features; Eq. (10) defines the FF for evaluating the solution.

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \tag{10}$$

whereas $\gamma_R(D)$ signifies the classification error rate.

3.2 Intrusion Detection Using Optimal WNN

For the intrusion classification process, the WNN model is used. The wavelet method is a primary advantage of processing signals and is rapidly implemented from numerous interconnected areas [18]. The WNN benefits from optimum fault tolerance, stronger adjustability, and an easy network framework. Whereas $x_1, x_2, \ldots, x_k$ indicates the input of WNN; $y_1, y_2, \ldots, y_m$ denotes the predicted results. w_{ij} signifies the connection weight amongst input and hidden states.

$$h(j) = h_j\left(\frac{\sum_{i=1}^{k} w_{ij}x_i - b_j}{a_j}\right), j = 1, 2, \ldots, l \tag{11}$$

In Eq. (11), $h(j)$ refers to the outcomes of j^{th} hidden states, a_j indicates the scaling feature of the wavelet basis function (WBF), b_j denotes the translation factor of WBF h_j, and h_j has the wavelet basis function. In such cases, the Morlet WBF has applied as a function of hidden state node:

$$y = \cos(1.75x)e^{-x2/2} \tag{12}$$

The formula for the resulting state is:

$$y(k) = \sum_{i=1}^{l} wikh(i),\ k = 1, 2, \ldots, m \tag{13}$$

Now, w_{ik} denotes the weight connecting hidden to the resulting state $h(i)$, characterizes the result of *the* i^{th} hidden layer, l indicates the number of hidden layers, and m shows the number of resulting layers. Fig. 2 represents the architecture of the WNN technique.

To adjust the WNN parameters, the BSA is utilized. BSA developed by Meng et al. [19], is an intelligent bionic approach inspired by multigroup and multi-search methods; it stimulates the bird flight, foraging, and vigilance performances and applies these SI for resolving the optimized problem.

(1) Foraging behavior

Once the iteration count is lower when compared to FQ and $\delta \leq P$, the bird is foraging performance. Rule2 was mathematically formulated in the following:

$$x_{i,j}^{t+1} = x_{i,j}^{t} + \left(p_{i,j}^{t} - x_{i,j}^{t}\right) \times C \times rand(0, 1) + \left(g_j^{t} - x_{i,j}^{t}\right) \times S \times rand(0, 1), \tag{14}$$

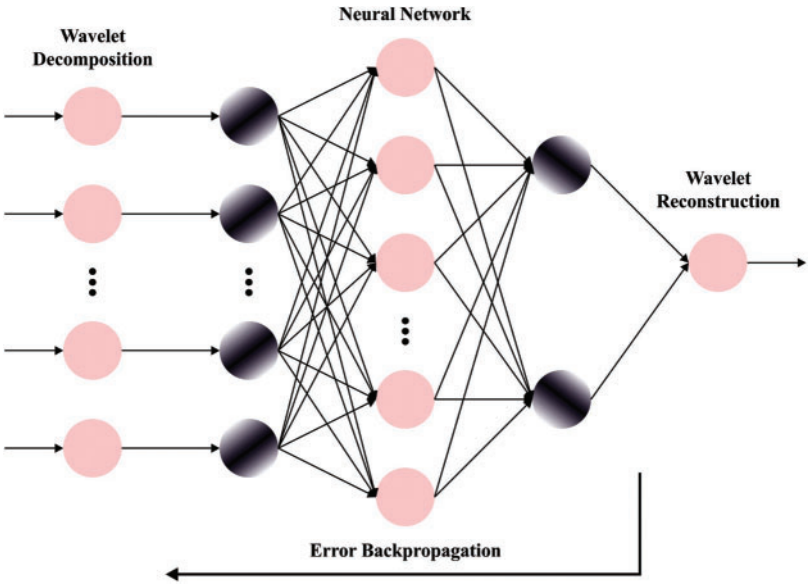

Figure 2: Structure of WNN

In Eq. (14), C and S denote the 2 positive integers; the former one is called a cognitive accelerated coefficient, and the last one is called a social accelerated coefficient. Currently, $p_{i,j}$ denotes the *i-th* bird optimal prior location, and g_j refers to the optimal prior swarm location.

(2) Vigilance behaviour

Once the iteration count is lower than FQ and $\delta > P$, the bird is vigilance performance. Rule3 is formulated mathematically as:

$$x_{i,j}^{t+1} = x_{i,j}^{t} + A_1\left(mean_j^t - x_{i,j}^t\right) \times rand\,(0,1) \tag{15}$$

$$+A_2\left(p_{k,j}^t - x_{i,j}^t\right) \times rand\,(-1,1)\,,$$

$$A_1 = a_1 \times \exp\left(-\frac{pFit_i}{sumFit + \varepsilon} \times N\right), \tag{16}$$

$$A_2 = a_2 \times \exp\left(\left(\frac{pFit_i - pFit_k}{|pFit_k - pFit_i| + \varepsilon}\right) \times \frac{N \times pFit_k}{sumFit + \varepsilon}\right), \tag{17}$$

From the expression, a_1 and a_2 characterizes the 2 positive constants within [0,2], $pFit_i$ denotes the optimal fitness value of i^{th} bird and *sumFit* show the sum of swarms' optimal fitness value [20]. Now, ε is applied to prevent zero-division error. $mean_j$ describes the j^{th} component of the average swarm location.

(3) Flight behaviour

Once the iteration count is equivalent to *FQ*, the bird's flight performance is classified as producer and scrounger by fitness. Rule3 and 4 are mathematically given below:

$$x_{i,j}^{t+1} = x_{i,j}^{t} + randn\,(0,1) \times x_{i,j}^{t}, \tag{18}$$

$$x_{i,j}^{t+1} = x_{i,j}^{t} + \left(x_{k,j}^{t} - x_{i,j}^{t}\right) \times FL \times rand\,(0,1)\,, \tag{19}$$

whereas FL ($FL \in [0, 2]$) shows the scrounger following the producer to search for food.

4 Results and Discussion

The result analysis of the BSAWNN-ID method is tested on two datasets: The toN_IoT dataset (https://research.unsw.edu.au/projects/toniot-datasets) and the UNSW-NB15 dataset. Tables 1 and 2 demonstrate the details of the two datasets.

Table 1: Details on ToN-IoT dataset

ToN-IoT dataset		
Label	Class	No. of records
C-1	Backdoor	1000
C-2	Denial of service (DoS)	1000
C-3	Distributed denial of service (DDoS)	1000
C-4	Injection	1000
C-5	Man in the middle (MITM)	1000
C-6	Scanning	1000
C-7	Ransomware	1000
C-8	Password	1000
C-9	Cross-site scripting (XSS)	1000
C-10	Normal	1000
Total number of records		**10000**

Table 2: Details on UNSW-NB15 dataset

UNSW-NB15 dataset		
Label	Class	No. of records
C-1	Normal	500
C-2	Generic	500
C-3	Exploits	500
C-4	Fuzzers	500
C-5	Reconnaissance	500
C-6	DoS	500
C-7	Analysis	500
C-8	Backdoor	500
C-9	Shellcode	500
C-10	Worms	174
Total number of records		**4674**

The confusion matrix of the BSAWNN-ID model on the applied ToN-IoT dataset is reported with different training (TR) and testing (TS) data in Fig. 3. The outcomes defined that the ToN-IoT dataset has recognized ten classes of intrusions properly and accurately.

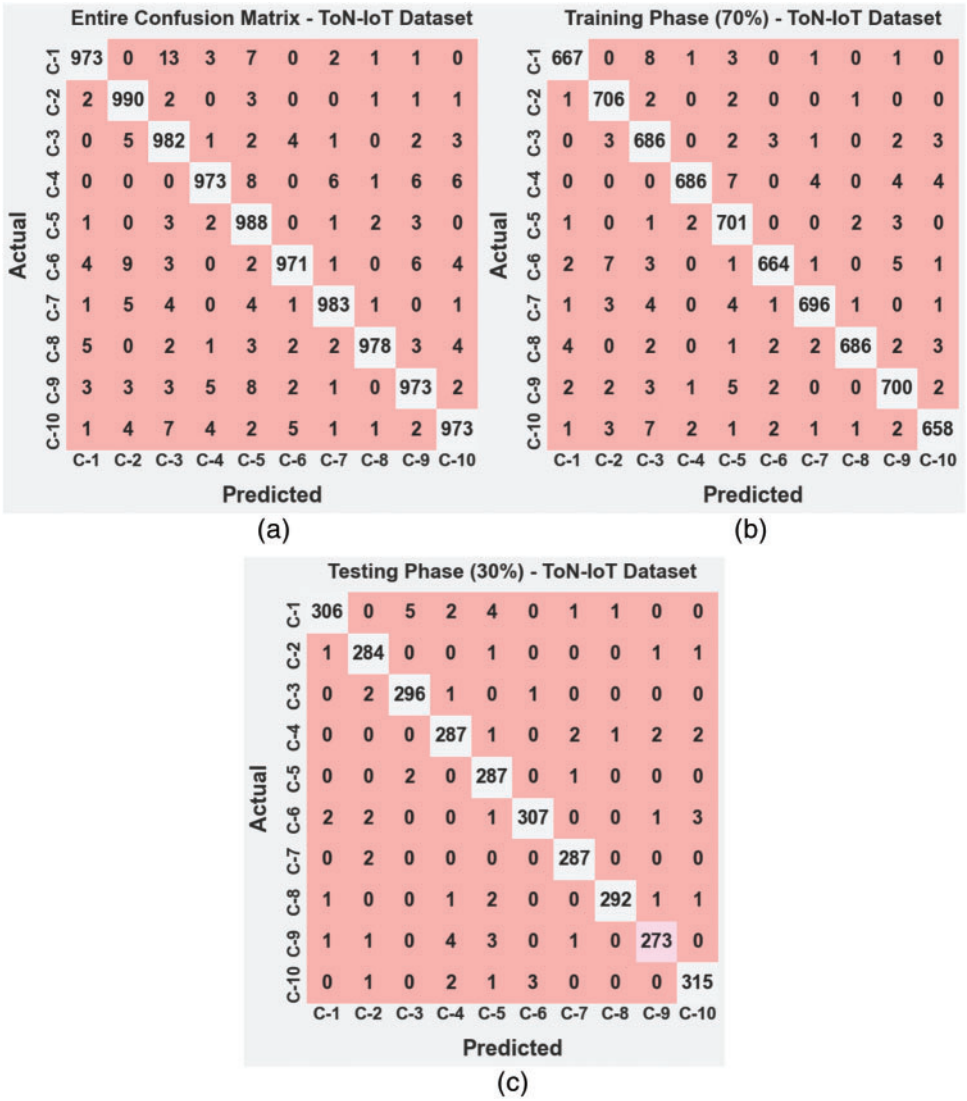

Figure 3: Confusion matrices of BSAWNN-ID system under ToN-IoT dataset (a) entire database, (b) 70% of TR database, and (c) 30% of TS database

Table 3 illustrates the overall ID outcomes of the BSAWNN-ID model on the ToN-IoT dataset. The outcomes described that the BSAWNN-ID technique had shown enhanced results. With the entire dataset, the BSAWNN-ID method has accomplished average $accu_y$, $prec_n$, $reca_l$, F_{score}, and $Jaccard_{index}$ of 99.57%, 97.85%, 97.84%, 97.84%, and 95.78%. In addition, with 70% of the TR database, the BSAWNN-ID approach has attained average $accu_y$, $prec_n$, $reca_l$, F_{score}, and $Jaccard_{index}$ of 99.57%, 97.88%, 97.85%, 97.86%, and 95.81%. Also, with 30% of the TS database, the BSAWNN-ID algorithm has achieved average $accu_y$, $prec_n$, $reca_l$, F_{score}, and $Jaccard_{index}$ of 99.56%, 97.80%, 97.82%, 97.80%, and 95.71%.

Table 3: Result analysis of the BSAWNN-ID system with various classes under the ToN-IoT dataset

Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	$Jaccard_{index}$
			Entire dataset		
C-1	99.56	98.28	97.30	97.79	95.67
C-2	99.64	97.44	99.00	98.21	96.49
C-3	99.45	96.37	98.20	97.28	94.70
C-4	99.57	98.38	97.30	97.84	95.77
C-5	99.49	96.20	98.80	97.48	95.09
C-6	99.57	98.58	97.10	97.83	95.76
C-7	99.68	98.50	98.30	98.40	96.85
C-8	99.71	99.29	97.80	98.54	97.12
C-9	99.49	97.59	97.30	97.45	95.02
C-10	99.52	97.89	97.30	97.59	95.30
Average	**99.57**	**97.85**	**97.84**	**97.84**	**95.78**
			Training phase (70%)		
C-1	99.63	98.23	97.94	98.09	96.25
C-2	99.66	97.51	99.16	98.33	96.71
C-3	99.37	95.81	98.00	96.89	93.97
C-4	99.64	99.13	97.30	98.21	96.48
C-5	99.50	96.42	98.73	97.56	95.24
C-6	99.57	98.52	97.08	97.79	95.68
C-7	99.64	98.58	97.89	98.24	96.53
C-8	99.70	99.28	97.72	98.49	97.03
C-9	99.49	97.36	97.63	97.49	95.11
C-10	99.51	97.92	97.05	97.48	95.09
Average	**99.57**	**97.88**	**97.85**	**97.86**	**95.81**
			Testing phase (30%)		
C-1	99.40	98.39	95.92	97.14	94.44
C-2	99.60	97.26	98.61	97.93	95.95
C-3	99.63	97.69	98.67	98.18	96.42
C-4	99.40	96.63	97.29	96.96	94.10
C-5	99.47	95.67	98.97	97.29	94.72
C-6	99.57	98.71	97.15	97.93	95.94
C-7	99.77	98.29	99.31	98.80	97.62
C-8	99.73	99.32	97.99	98.65	97.33
C-9	99.50	98.20	96.47	97.33	94.79
C-10	99.53	97.83	97.83	97.83	95.74
Average	**99.56**	**97.80**	**97.82**	**97.80**	**95.71**

The training accuracy (TACC) and validation accuracy (VACC) of the BSAWNN-ID approach are investigated under the ToN-IoT dataset performance in Fig. 4. The figure referred that the

BSAWNN-ID system has exhibited higher performance with improved values of TACC and VACC. It can be clear that the BSAWNN-ID method has gained maximal TACC outcomes.

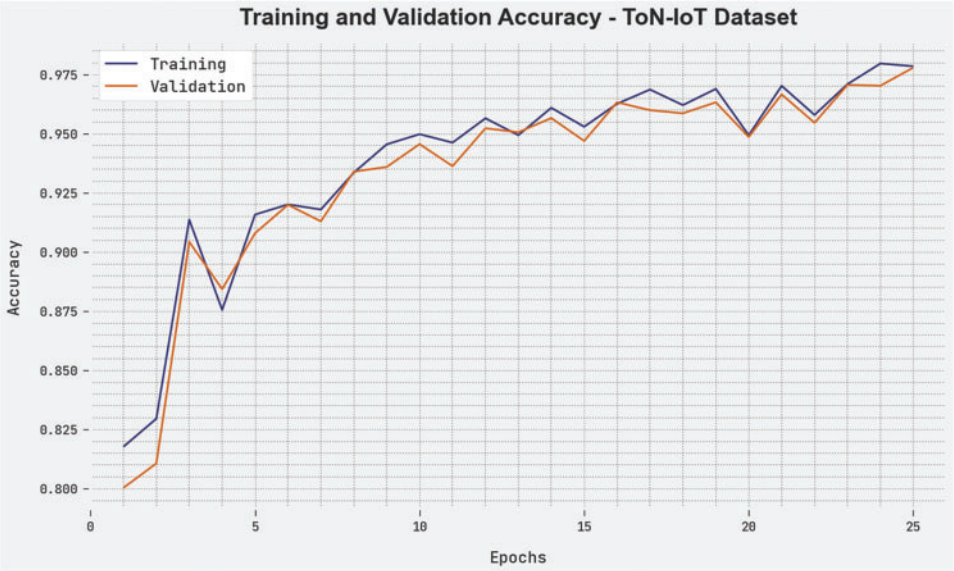

Figure 4: TACC and VACC analysis of the BSAWNN-ID system under the ToN-IoT dataset

The training loss (TLS) and validation loss (VLS) of the BSAWNN-ID model are tested under the ToN-IoT dataset performance in Fig. 5. The figure revealed that the BSAWNN-ID approach revealed better performance with minimal values of TLS and VLS. It is stated that the BSAWNN-ID model has resulted in reduced VLS outcomes.

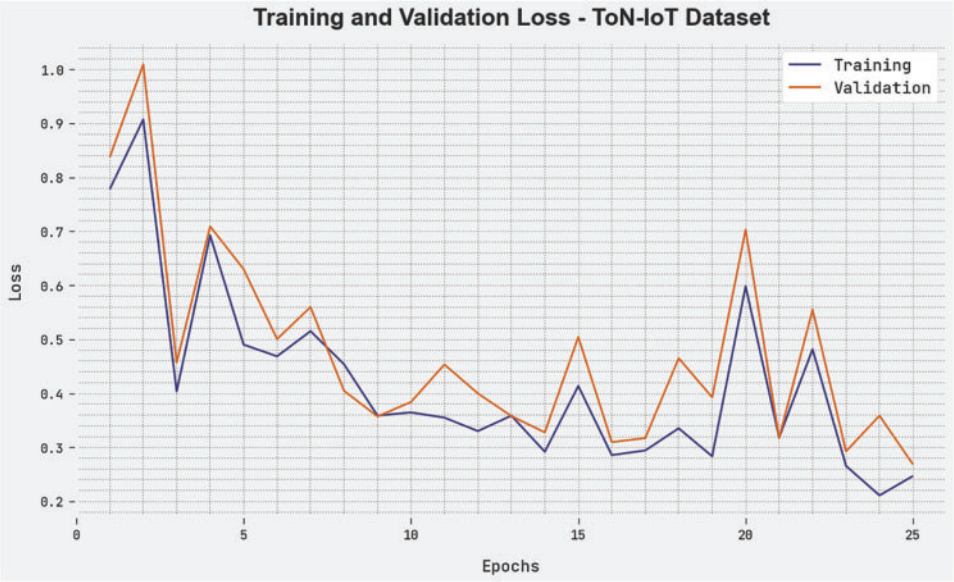

Figure 5: TLS and VLS analysis of BSAWNN-ID system under the ToN-IoT dataset

The confusion matrix of the BSAWNN-ID system on the applied UNSW-NB15 dataset is given in Fig. 6. The outcomes determine that the UNSW-NB15 dataset has recognized ten classes of intrusions properly and accurately.

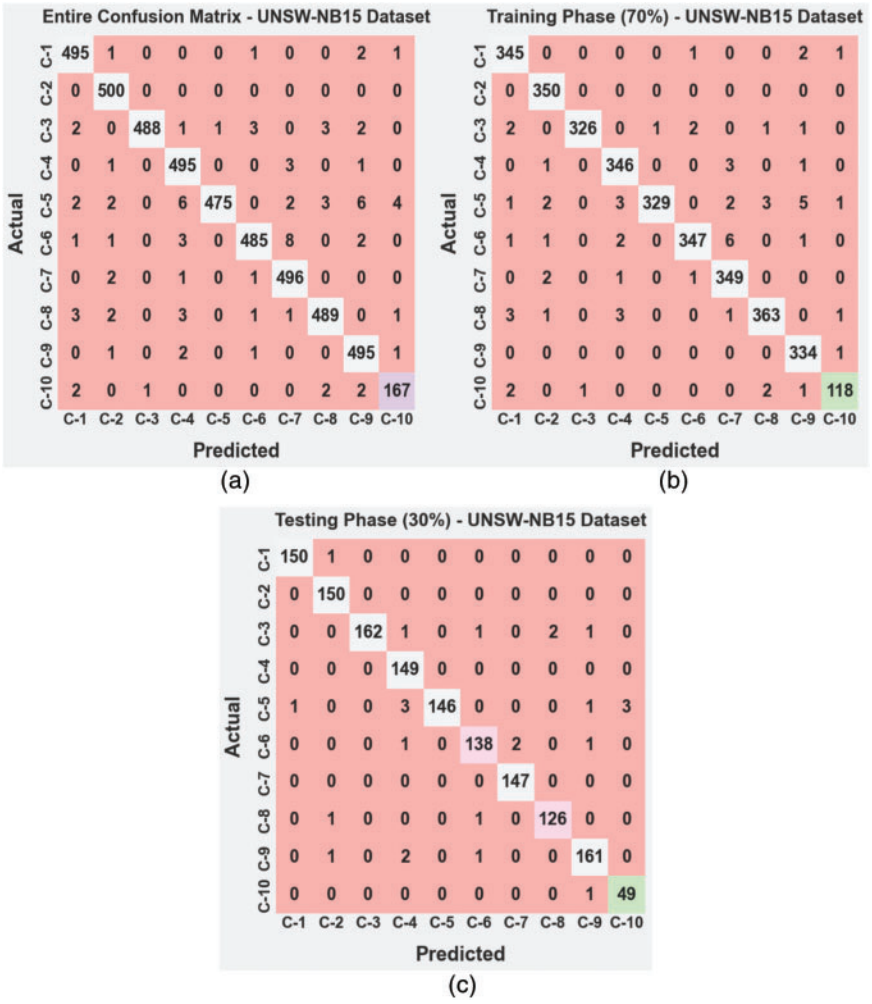

Figure 6: Confusion matrices of BSAWNN-ID system under UNSW-NB15 dataset (a) Entire database, (b) 70% of TR database, and (c) 30% of TS database

Table 4 depicts an overall ID outcome of the BSAWNN-ID approach on the UNSW-NB15 dataset. The outcomes demonstrated that the BSAWNN-ID algorithm had shown improved results. With the entire dataset, the BSAWNN-ID system has attained average $accu_y$, $prec_n$, $reca_l$, F_{score}, and $Jaccard_{index}$ of 99.62%, 97.98%, 97.96%, 97.96%, and 96%. Followed by, 70% of the TR database, the BSAWNN-ID technique has obtained average $accu_y$, $prec_n$, $reca_l$, F_{score}, and $Jaccard_{index}$ of 99.61%, 97.98%, 97.87%, 97.91%, and 95.92%. Moreover, with 30% of the TS database, the BSAWNN-ID methodology has reached average $accu_y$, $prec_n$, $reca_l$, F_{score}, and $Jaccard_{index}$ of 99.64%, 97.97%, 98.23%, 98.08%, and 96.25%.

Table 4: Result analysis of the BSAWNN-ID system with various classes under the UNSW-NB15 dataset

Labels	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	$Jaccard_{index}$
			Entire dataset		
C-1	99.68	98.02	99.00	98.51	97.06
C-2	99.79	98.04	100.00	99.01	98.04
C-3	99.72	99.80	97.60	98.69	97.41
C-4	99.55	96.87	99.00	97.92	95.93
C-5	99.44	99.79	95.00	97.34	94.81
C-6	99.53	98.58	97.00	97.78	95.66
C-7	99.61	97.25	99.20	98.22	96.50
C-8	99.59	98.39	97.80	98.09	96.26
C-9	99.57	97.06	99.00	98.02	96.12
C-10	99.70	95.98	95.98	95.98	92.27
Average	**99.62**	**97.98**	**97.96**	**97.96**	**96.00**
			Training phase (70%)		
C-1	99.60	97.46	98.85	98.15	96.37
C-2	99.79	98.04	100.00	99.01	98.04
C-3	99.76	99.69	97.90	98.79	97.60
C-4	99.57	97.46	98.58	98.02	96.11
C-5	99.45	99.70	95.09	97.34	94.81
C-6	99.54	98.86	96.93	97.88	95.86
C-7	99.51	96.68	98.87	97.76	95.62
C-8	99.54	98.37	97.58	97.98	96.03
C-9	99.63	96.81	99.70	98.24	96.53
C-10	99.69	96.72	95.16	95.93	92.19
Average	**99.61**	**97.98**	**97.87**	**97.91**	**95.92**
			Testing phase (30%)		
C-1	99.86	99.34	99.34	99.34	98.68
C-2	99.79	98.04	100.00	99.01	98.04
C-3	99.64	100.00	97.01	98.48	97.01
C-4	99.50	95.51	100.00	97.70	95.51
C-5	99.43	100.00	94.81	97.33	94.81
C-6	99.50	97.87	97.18	97.53	95.17
C-7	99.86	98.66	100.00	99.32	98.66
C-8	99.71	98.44	98.44	98.44	96.92
C-9	99.43	97.58	97.58	97.58	95.27
C-10	99.71	94.23	98.00	96.08	92.45
Average	**99.64**	**97.97**	**98.23**	**98.08**	**96.25**

The TACC and VACC of the BSAWNN-ID approach are examined under UNSW-NB15 dataset performance in Fig. 7. The figure pointed out that the BSAWNN-ID model has revealed improved performance with increased values of TACC and VACC. It is visible that the BSAWNN-ID system has reached higher TACC outcomes.

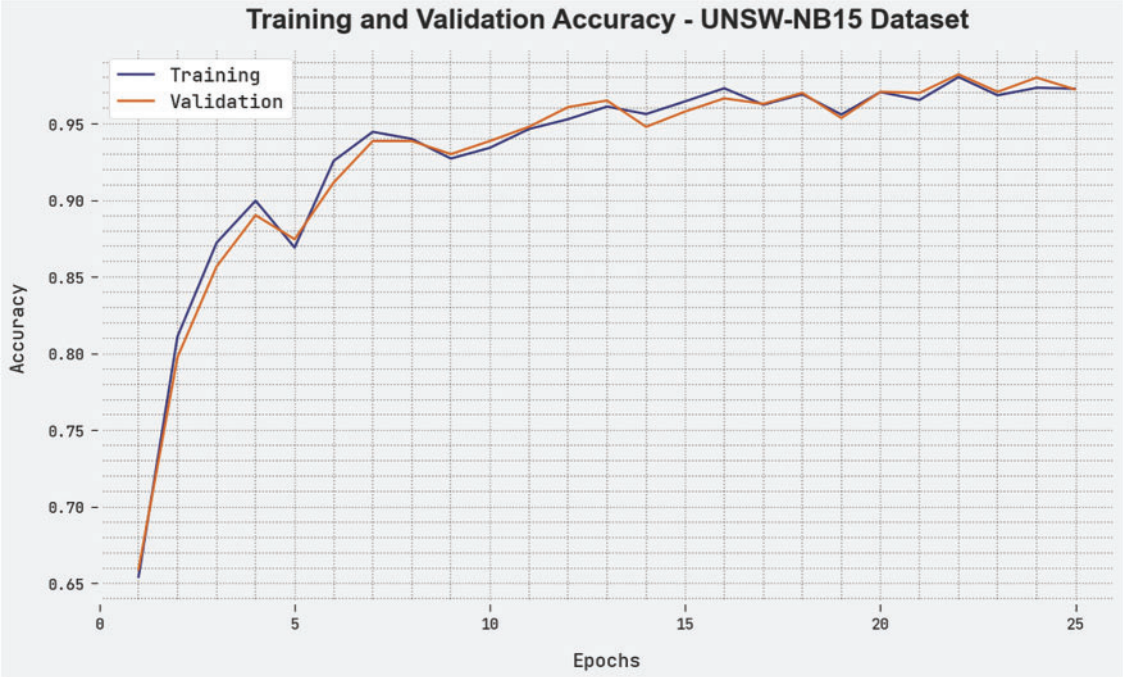

Figure 7: TACC and VACC analysis of the BSAWNN-ID system under the UNSW-NB15 dataset

The TLS and VLS of the BSAWNN-ID algorithm are tested under UNSW-NB15 dataset performance in Fig. 8. The figure inferred that the BSAWNN-ID methodology had exposed better performance with the least values of TLS and VLS. It is noticeable that the BSAWNN-ID methodology has resulted in lesser VLS outcomes.

Table 5 and Fig. 9 highlight the comparison ID results of the BSAWNN-ID model on the ToN-IoT dataset. The results defined the improvement of the BSAWNN-ID model over other models. Based on $accu_y$, the BSAWNN-ID model has shown improved results with $an\ accu_y$ of 99.57%. Meanwhile, in terms of $prec_n$, the BSAWNN-ID system has exhibited higher outcomes with $prec_n$ of 97.88%. Similarly, concerning $reca_l$, the BSAWNN-ID approach has revealed maximal results with $a\ reca_l$ of 97.85%. Last, based on the $F1_{score}$, the BSAWNN-ID methodology has displayed enhanced results with an $F1_{score}$ of 97.86%.

Table 6 and Fig. 10 demonstrate the comparison ID outcomes of the BSAWNN-ID approach on the UNSW-NB15 dataset. The outcomes defined the enhancement of the BSAWNN-ID approach over other techniques.

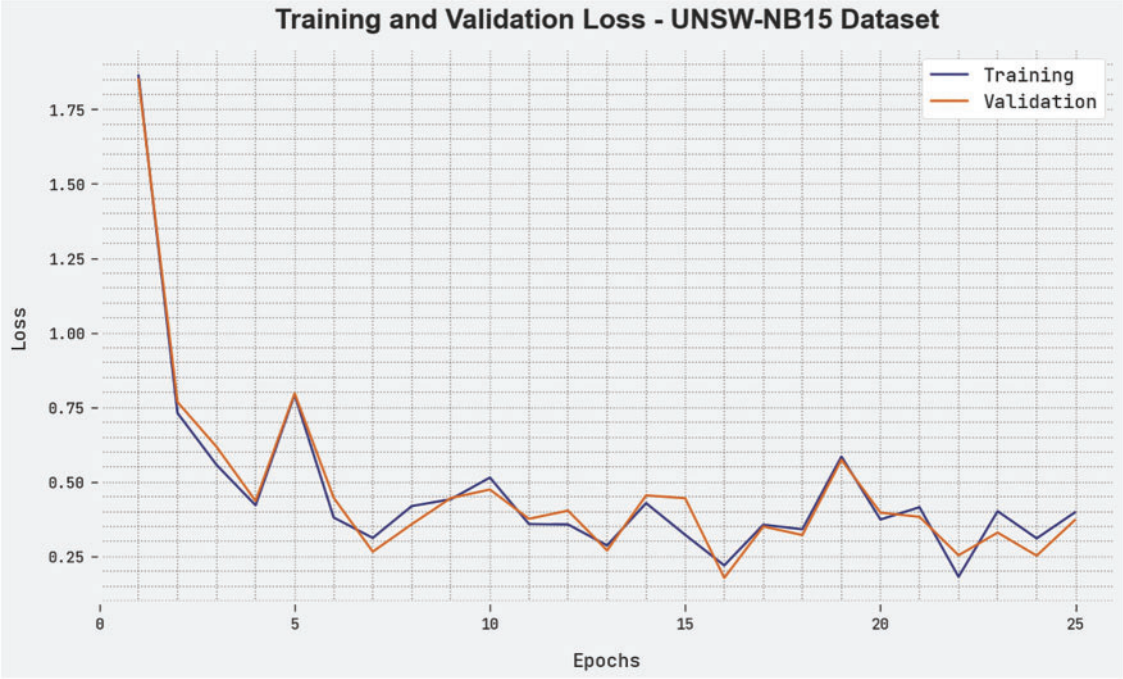

Figure 8: TLS and VLS analysis of the BSAWNN-ID system under the UNSW-NB15 dataset

Table 5: Comparative analysis of the BSAWNN-ID system with other approaches under the ToN-IoT dataset

ToN-IoT dataset				
Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
BSAWNN-ID	99.57	97.88	97.85	97.86
DT model	97.51	97.49	96.92	97.57
NB model	96.48	96.91	96.87	96.36
XGBoost	97.94	96.35	95.18	95.91
Inception time	99.22	97.35	97.32	96.63
LSTM model	98.95	97.57	96.68	97.32
DNN model	98.23	96.39	96.33	96.28
ENS-SVM	93.82	93.46	94.05	93.26

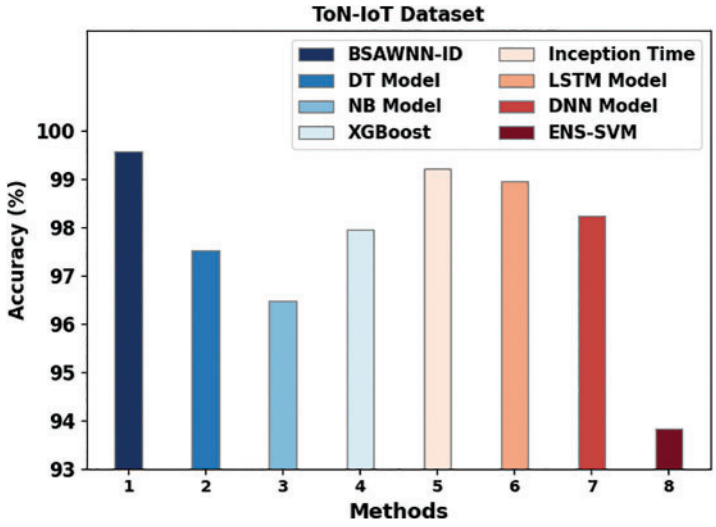

Figure 9: Comparative analysis of the BSAWNN-ID system under the ToN-IoT dataset

Table 6: Comparative analysis of the BSAWNN-ID system with other approaches under the UNSW-NB15 dataset

UNSW-NB15 dataset				
Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
BSAWNN-ID	99.64	97.97	98.23	98.08
Densely-ResNet	74.48	81.17	96.66	88.01
RF model	95.38	96.45	96.7	96.69
DT model	94.32	93.54	97.89	96.33
MLP model	84.94	84.26	84.84	82.72
LSTM model	89.53	92.72	85.72	91.25
DNN model	75.92	80.16	75.4	76.67
Inception	98.65	97.49	97.53	96.12

Concerning $accu_y$, the BSAWNN-ID methodology has outperformed superior outcomes with an $accu_y$ of 99.64%. In the meantime, based on $prec_n$, the BSAWNN-ID method has exposed maximum results with $prec_n$ of 97.97%. Likewise, in terms of $reca_l$, the BSAWNN-ID algorithm has exhibited enhanced outcomes with $a\,reca_l$ of 98.23%. Finally, concerning $F1_{score}$, the BSAWNN-ID algorithm has demonstrated higher results with $an\,F1_{score}$ of 98.08%. Therefore, the BSAWNN-ID model has shown effectual ID results in the IoT environment.

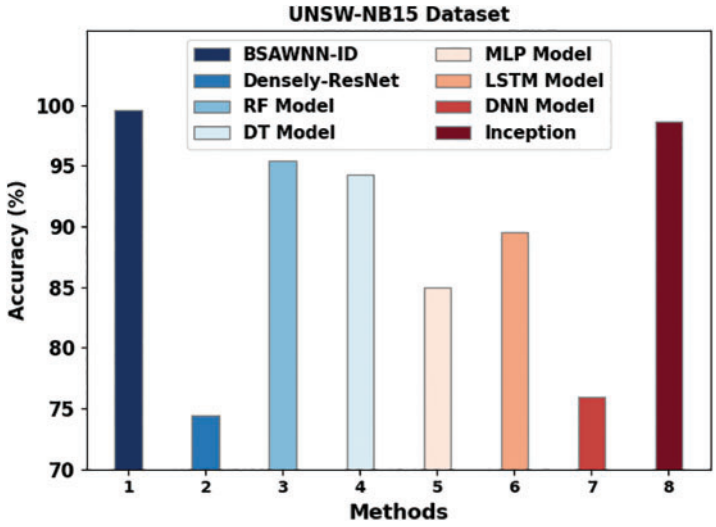

Figure 10: Comparative analysis of BSAWNN-ID system under UNSW-NB15dataset

5 Conclusion

In this article, a novel BSAWNN-ID technique was developed in the IoT platform. The main intention of the BSAWNN-ID algorithm lies in the recognition and classification of intrusion in the IoT platform. The BSAWNN-ID technique designed the FSS-COA for feature subset election to attain this. Next, to detect intrusions, the WNN model is utilized. At last, the WNN parameters are optimally modified by the use of BSA. A widespread experimental analysis is performed to depict the enhanced performance of the BSAWNN-ID approach. The resultant values indicated the better performance of the BSAWNN-ID technique over other models, with an accuracy of 99.64% on the UNSW-NB15 dataset. Thus, the BSAWNN-ID technique can be used for real-time intrusion recognition purposes. In the future, the BSAWNN-ID technique can be extended to the outlier detection process.

Funding Statement: This work was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University, through the Research Groups Program Grant No. (RGP-1443-0048).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider *et al.,* "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, pp. 1177, 2020.

[2] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb *et al.,* "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review," *Applied Sciences*, vol. 11, no. 18, pp. 8383, 2021.

[3] E. Gyamfi and A. Jurcut, "Intrusion detection in internet of things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, pp. 3744, 2022.

[4] A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," *Wireless Personal Communications*, vol. 111, no. 4, pp. 2287–2310, 2020.
[5] A. Fatani, A. Dahou, M. A. Al-Qaness, S. Lu and M. A. Elaziz, "Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system," *Sensors*, vol. 22, no. 1, pp. 140, 2021.
[6] N. Islam, F. Farhin, I. Sultana, M. S. Kaiser, M. S. Rahman *et al.,* "Towards machine learning based intrusion detection in IoT networks," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1801–1821, 2021.
[7] 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, pp. 1113, 2021.
[8] A. Amouri, V. T. Alaparthy and S. D. Morgera, "A machine learning based intrusion detection system for mobile internet of things," *Sensors*, vol. 20, no. 2, pp. 461, 2020.
[9] G. Abdelmoumin, D. B. Rawat and A. Rahman, "On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4280–4290, 2021.
[10] E. Rehman, M. H. Din, A. J. Malik, T. K. Khan, A. A. Abbasi *et al.,* "Intrusion detection based on machine learning in the internet of things, attacks and counter measures," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8890–8924, 2022.
[11] J. A. Faysal, S. T. Mostafa, J. S. Tamanna, K. M. Mumenin, M. M. Arifin *et al.,* "XGB-RF: A hybrid machine learning approach for IoT intrusion detection," *Telecom*, vol. 3, no. 1, pp. 52–69, 2022.
[12] S. Fenanir, F. Semchedine and A. Baadache, "A machine learning-based lightweight intrusion detection system for the internet of things," *Revue d'Intelligence Artificielle*, vol. 33, no. 3, pp. 203–211, 2019.
[13] Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa *et al.,* "DeepIoT," IDS: hybrid deep learning for enhancing IoT network intrusion detection," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3945–3966, 2021.
[14] N. Moustafa, B. Turnbull and K. K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4815–4830, 2018.
[15] K. Albulayhi, Q. Abu Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman *et al.,* "IoT intrusion detection using machine learning with a novel high performing feature selection method," *Applied Sciences*, vol. 12, no. 10, pp. 5015, 2022.
[16] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395–9409, 2022.
[17] A. Abaza, R. A. El-Sehiemy, K. Mahmoud, M. Lehtonen and M. M. Darwish, "Optimal estimation of proton exchange membrane fuel cells parameter based on coyote optimization algorithm," *Applied Sciences*, vol. 11, no. 5, pp. 2052, 2021.
[18] L. Yang and H. Chen, "Fault diagnosis of gearbox based on RBF-PF and particle swarm optimization wavelet neural network," *Neural Computing and Applications*, vol. 31, no. 9, pp. 4463–4478, 2019.
[19] X. B. Meng, X. Z. Gao, L. Lu, Y. Liu and H. Zhang, "A new bio-inspired optimization algorithm: Bird swarm algorithm," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 28, no. 4, pp. 673–687, 2016.
[20] X. Ma, Y. Mu, Y. Zhang, C. Zang, S. Li *et al.,* "Multi-objective microgrid optimal dispatching based on improved bird swarm algorithm," *Global Energy Interconnection*, vol. 5, no. 2, pp. 154–167, 2022.