Computer Systems Science & Engineering
DOI:10.32604/csse.2023.025216
Article

Tech Science Press

Intelligent Intrusion Detection System for Industrial Internet of Things Environment

R. Gopi[1], R. Sheeba[2], K. Anguraj[3], T. Chelladurai[4], Haya Mesfer Alshahrani[5], Nadhem Nemri[6,*] and Tarek Lamoudan[7]

[1]Department of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, 621 212, India
[2]Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Tiruchirappalli, 621112, India
[3]Department of Electronics and Communication Engineering, Sona College of Technology, Salem, 636005, India
[4]Department of Electronics and Communication Engineering, PSNA College of Engineering and Technology, Dindigul, 624622, India
[5]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[6]Department of Information Systems, College of Science & Arts at Mahayil, King Khalid University, Muhayel Aseer, 62529, Saudi Arabia
[7]Department of Mathematics, College of Science & Arts at Mahayil, King Khalid University, Muhayel Aseer, 62529, Saudi Arabia
*Corresponding Author: Nadhem Nemri. Email: nnemri@kku.edu.sa

Received: 16 November 2021; Accepted: 05 January 2022

Abstract: Rapid increase in the large quantity of industrial data, Industry 4.0/5.0 poses several challenging issues such as heterogeneous data generation, data sensing and collection, real-time data processing, and high request arrival rates. The classical intrusion detection system (IDS) is not a practical solution to the Industry 4.0 environment owing to the resource limitations and complexity. To resolve these issues, this paper designs a new Chaotic Cuckoo Search Optimization Algorithm (CCSOA) with optimal wavelet kernel extreme learning machine (OWKELM) named CCSOA-OWKELM technique for IDS on the Industry 4.0 platform. The CCSOA-OWKELM technique focuses on the design of feature selection with classification approach to achieve minimum computation complexity and maximum detection accuracy. The CCSOA-OWKELM technique involves the design of CCSOA based feature selection technique, which incorporates the concepts of chaotic maps with CSOA. Besides, the OWKELM technique is applied for the intrusion detection and classification process. In addition, the OWKELM technique is derived by the hyperparameter tuning of the WKELM technique by the use of sunflower optimization (SFO) algorithm. The utilization of CCSOA for feature subset selection and SFO algorithm based hyperparameter tuning leads to better performance. In order to guarantee the supreme performance of the CCSOA-OWKELM technique, a wide range of experiments take place on two benchmark datasets and the experimental outcomes demonstrate the promising performance of the CCSOA-OWKELM technique over the recent state of art techniques.

Keywords: Intrusion detection system; artificial intelligence; machine learning; industry 4.0; internet of things

1 Introduction

Industry 4.0 characterizes the 4th stage of manufacturing and industry, promising to become the basis of intelligent buildings, smart systems, and automated factory. Using data driven decision-making and high usage of Cyber Physical System (CPS), Industry 4.0 is capable of changing various factors of their day-to-day life [1]. The word Industry 4.0 was projected by the German government in 2011 as a motivation to shift the manufacturing sectors to technical automation [2,3]. The early industrial phase consists of electricity, Information Technology (IT), and mechanization. The 4th stage of manufacturing and industry allows automation in manufacturing, with an integration of Internet of Things (IoT), CPS, big data, autonomous industrial, data exchanges, Cloud, and Fog computing techniques [4]. The capacity of modification given by the Industry 4.0 depends on computing devices, ubiquitous internet connectivity, heterogeneous and pervasive sensor networks. Also, Industry 4.0 is highly associated with smart machines, particularly in the field of manufacturing. The smart machine provides faster recalibration, greater customization, and improved manufacturing speed allows for the improvement of novel partnership and business techniques for meeting the user needs. Also, this integration reduces waste, increases profitability and flexibility. An instance of present industrial developments is the electrical grid usage [5], management of electricity storage, and integrating renewable energy using IoT techniques. Power balancing methods were introduced for addressing the challenges of energy saving and dynamic pricing. Even though Industry 4.0 system has the capacity of improving the profitability and productivity of organization, still they face huge challenge associated with the privacy and cybersecurity. Fig. 1 shows the industry evolution model [6].

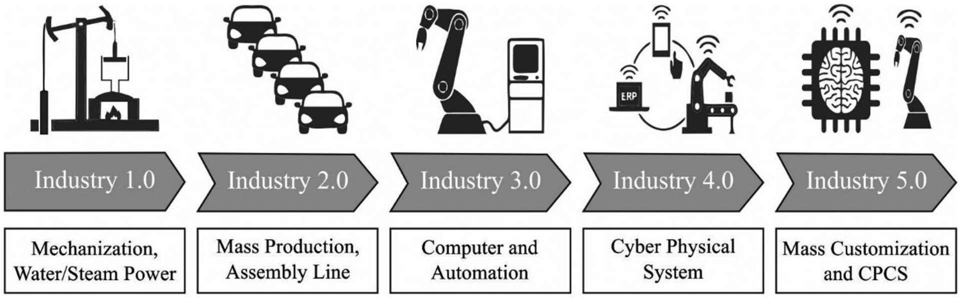

Figure 1: Industry evolution

The emergence of this Industry 4.0 implies that each device is open and interconnected to the external world, almost all the information’s are stored and deported in media except the normal local hard drives like information technology (IT) and Clouds the world is especially interconnected to the operational technology (OT) [7,8]. It centralizes each data regarding the maintenance, production, product, and stock quality. At present the borders are open, some attacks developed in the previous in the IT world could be repeated in the OT world. The concept of cyber-security has to turn into an urgent requirement in future industries.

Industry 4.0 concentrated on the optimization problem in the industry for utilizing data driven services with the help of smart devices. This intelligence could attain manufacturing enhancement and more efficiencies. But, this prolonged network opens up these interconnected devices to certain threats of cyberattacks [9]. The industrial facility becomes more related, and attackers are highly complicated. Industrial Control System (ICS) encompass the different classes of control system and incorporated component used for controlling the industrial processes. The ICS is confronting a huge amount of cyberattacks which have many challenges. Ineffective securities have an adversative impact on the organization and workforce. Few impacts are building damage, production delays, material losses, compensation and medical costs, loss of business, tool and equipment damages, legal expenses. IDS detects the susceptibilities within network traffics on network framework. It can define if the attackers initiate probing devices i.e., the first stage for generating safe IIoT.

In previous years, IDS have turn into more efficient and reliable also hackers have emerged more diverse attack modes for defeating this detection system. IDS scheme identifies and collects audit data, network traffic, information, and security logs from systems key point for checking either they exist security damage in the networks. The solutions of IDS for IIoT require to be customized to the nature of device. The deep learning (DL) method is utilized by IoT for improving the efficacy of IIoT applications. Numerous studies have given various methods for IDS in industries. Furthermore, conventional IDS could not handle complicated network layers in IoT [10]. The most recent development in smart systems has stimulated scientists to apply shared IDSs as well as several ML methods, for example, ANN, DL, and RL. Regular ANN has certain constraints in handling the complication of IDS. Developing techniques by solving this shortcoming is a necessity to realize the significance of IDS in real-time.

This paper designs a new Chaotic Cuckoo Search Optimization Algorithm (CCSOA) with optimal wavelet kernel extreme learning machine (OWKELM) named CCSOA-OWKELM technique for IDS on the Industry 4.0 platform. The CCSOA-OWKELM technique involves the design of CCSOA based feature selection technique, which includes the ideas of chaotic maps into the CSOA. Moreover, the OWKELM technique is applied for the intrusion detection and classification process and the hyperparameter tuning of the WKELM technique takes place using sunflower optimization (SFO) algorithm. The utilization of CCSOA for feature subset selection and SFO algorithm based hyperparameter tuning shows the novelty of the work. An extensive experimental analysis is carried out on the two benchmark datasets and examined the results interms of different measures.

The rest of the paper is given as follows. Section 2 offers related works, Section 3 introduces the proposed model, Section 4 provides experimental validation, and Section 5 draws the conclusion.

2 Literature Review

Alsaedi et al. [11] proposed a novel data driven IIoT or IoT dataset using the ground truth which integrates label features indicate attack and usual classes, and type features indicate the subclasses of attack aiming IIoT or IoT application for multiclassification challenges. The presented datasets, i.e., called TON_IoT, consist of Telemetry data of IoT or IIoT service, and Network traffic of IoT network, and OS logs gathered from an accurate depiction of a medium scale network at the IoT Labs and Cyber Range at the UNSW Canberra (Australia). Latif et al. [12] introduced a DRaNN based system for detecting intrusions in IIoT. The presented method is calculated via a novel generation IIoT security datasets UNSW-NB15. Stimulation result proves that the developed framework effectively categorized 9 distinct kinds of attack.

Abdel-Basset et al. [13] proposed a forensics based DL method (known as Deep-IFS) to identify intrusion in IIoT traffic. It learns local representation through LocalGRU, and present MHA layers for capturing and learning global representations. Residual connections among layers are developed for preventing loss of data. These challenges are tackled by training and deploying the presented Deep-IFS in a fog computing platform. The master fog nodes are accountable to share training parameters and aggregate worker's node output. Qureshi et al. [14] proposed architecture and methodology for detecting intrusion against IIoT. Particularly, they are aiming to identify the attacks against RPL through genetic programming. The result indicates that the proposed model could effectively (higher true positive, lower false positive rate and higher accuracy) detects routing attack in RPL based Industrial IoT network.

Priya et al. [15] develop a 2 stage anomaly detection method for enhancing the consistency of an IIoT network. Initially, NB and SVM are incorporated with an ensemble blending method. K-fold cross-validation is executed when training the data using distinct testing and training ratios for obtaining optimized test and training sets. Ensemble blending exploits an RF method for predicting class labels. Also, ANN classifiers utilize the Adam optimizer for achieving optimal accuracy is utilized for predictions. Next, the RF and ANN outcomes are fed into the model's classification unit, and the maximum accuracy value is deliberated with the concluding results.

Zhou et al. [16] employs Fog computing idea in DDoS mitigation by assigning traffic monitoring and analyses study closer to local device, and, alternatively, consolidating and coordinating works to cloud central server for achieving faster respond when at lower false alarm rate. The mitigation system includes real world traffic filtering through field firewall device. Al-Hawawreh et al. [17] proposed a detection method on the basis of DL methods that can learn and test with the help of data gathered from RTU stream of gas pipeline scheme. It uses the denoising and sparse AE approaches for DNN and unsupervised learning for supervised learning to generate a higher level data depiction from noisy and unlabelled data.

Hassan et al. [18] proposed an adaptive trust boundary protection for IIoT network through DL, FE based semi supervised method. This technique is a new one since it is consistent using multilevel protocols of IIoT. The presented method doesn't need any manual efforts for updating the attack database and could learn the quickly increasing nature of unknown attack methods with the help of unsupervised learning. Hence, the presented method is strong to emerge cyber-attacks and their dynamic nature. Qiao et al. [19] introduce a method which monitors the actions of factory network traffic on the basis of 2 linear FE methods, viz., PCA and LDA. An ML based approaches are utilized for analyzing the record of networks connection from the UNSW-NB15 databases also to report and detect abnormalities like malicious attack.

3 The Proposed Model

In this study, a new CCSOA-OWKELM technique is derived for IDS in the Industry 4.0 environment. The CCSOA-OWKELM technique involves three major processes such as preprocessing, CSSOA based feature selection, and OKELM based classification. The overall working principle of the CCSOA-OWKELM technique and the modules involved in it are discussed in the following.

3.1 Data Pre-Processing

In the data pre-processed, the input data attains pre-processed under three stages: data transformation, class labeling, and data normalization. Primarily, input data in .xls format has been changed as to the .csv format. Second, the class labeling method was carried out in which the instances were allocated to matching classes. Thirdly, the data normalization technique takes place employing min-max dataset as defined as:

$$Min - Max.Norm = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{1}$$

3.2 Design of CCSOA Based Feature Selection Technique

The pre-processed data is fed into the CSSOA based feature selection technique, which inherits the characteristics of the chaotic maps and CSOA.

The CSOA is depending upon the brood parasitism of a few cuckoos' species through laying their eggs in the nest of other host birds. For easiness in representing the basic CSOA, the succeeding 3 rules are utilized: (1) All cuckoos lay single egg once, and dump it in an arbitrarily selected set; (2) the optimal nest with higher quality eggs would be performed on the upcoming generation; (3) the amount of accessible host nest is set, and the eggs laid by a cuckoo are found using the host bird with a likelihood

$p_a \in [0, 1]$. In this instance, the host bird could throw away the eggs or just abandon the nest and construct complicated novel nests. According to the aforementioned rules, the basic CSOA approach is defined in Algorithm 1. Moreover, the approach utilized a balanced integration of a local arbitrary walk also the global explorative arbitrary walk, regulated by a switching variable p_a. The local arbitrary walk could be expressed in the following

$$x_i^{t+1} = x_i^t + \alpha s \otimes H(p_a - \varepsilon) \otimes (x_j^t - x_k^t) \tag{2}$$

whereas x_j^t & x_k^t represents 2 distinct solutions elected arbitrarily by arbitrary permutation, H denotes a Heaviside function, ε indicates an arbitrary amount from a uniform distribution, and s denotes the step size. Fig. 2 illustrates the flowchart of CSOA [20]. Alternatively, the global arbitrary walk is performed with the help of Lévy flights:

$$x_i^{t+1} = x_i^t + \alpha \oplus L\acute{e}vy\ \ (s,\ \lambda) \tag{3}$$

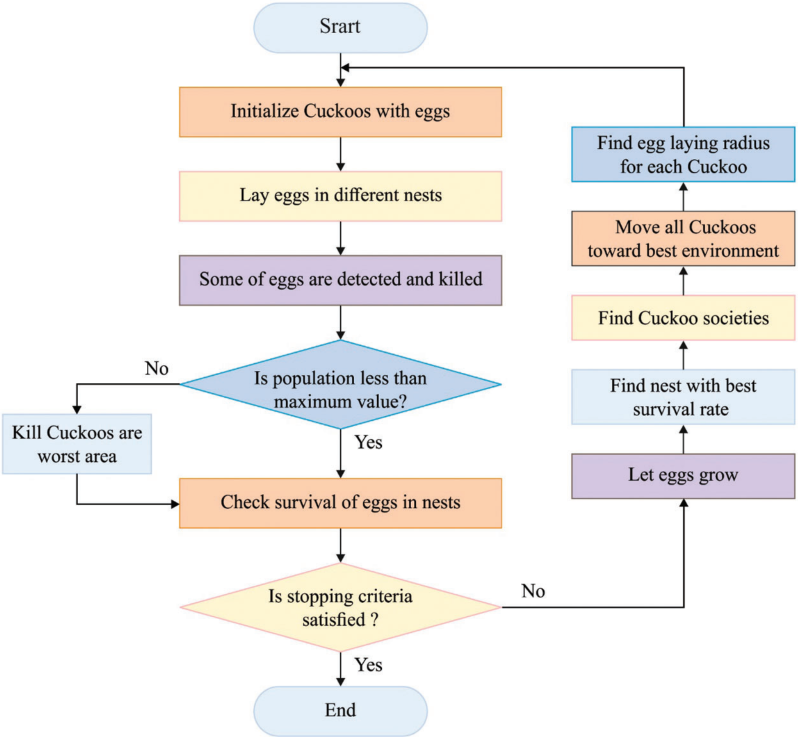
Srart
Initialize Cuckoos with eggs
Lay eggs in different nests
Some of eggs are detected and killed
Is population less than maximum value?
No
Kill Cuckoos are worst area
Yes
Check survival of eggs in nests
Is stopping criteria satisfied ?
No
Yes
End
Let eggs grow
Find nest with best survival rate
Find Cuckoo societies
Move all Cuckoos toward best environment
Find egg laying radius for each Cuckoo

Figure 2: Flowchart of CSOA

Now, $\alpha > 0$ denotes the step size scaling factor; Lévy $(s,\ \lambda)$ represents the step length i.e., distributed based on the succeeding likelihood distribution as given in (4) that contains an infinite variance using an infinite mean:

$$L\acute{e}vy\ (s,\ \lambda) = \frac{\lambda\Gamma(\lambda)\ \sin\ (\pi\lambda/2)}{\pi}\frac{1}{s^{1+\lambda}} \tag{4}$$

Searching for an optimum solution in chaotic ways amongst the local minimal via regularity, semi-stochastic, and ergodicity properties leads to a higher possible global optimum solution. The chaos parameters are caused using Gauss or mouse map in the CCSO approach are discussed. But, chaos parameters are currently supposed to be made through an arbitrary 1D map that allows to alter in the range of (0.1) or scale them in this range. The first value for Gauss or mouse chaotic function is an arbitrary number then the series value is evaluated using Eq. (5):

$$x_0 = rand$$

$$x_{i+1} = \begin{cases} 1 & x_i = 0 \\ \dfrac{1}{mod(x_i,\ 1)} & otherwise \end{cases} \tag{5}$$

For finding habitat in the upcoming generation, cuckoos' must search everywhere to detect an optimal one. As the continuous space of feature should be converted to the respective binary spaces, a novel location of the habitat is utilized in the following equation where $y^{j,t+1}$ represents the cuckoos with j index afterward t iteration [21]:

$$y^{j,t+1} = f(x) = \begin{cases} 1 & if \quad (w(x^{j,t+1}) \geq rand) \\ 0 & \quad otherwise \end{cases} \tag{6}$$

$w(x^{j,t+1})$ is computed by Eq. (7).

$$w(a) = \frac{1}{1 + e^{10(a-0.5)}} 1 \tag{7}$$

In order to resolve the FS problem, the continuous space (free location) should be converted to their respective binary solution. E.g., when the value of a bit is equal to 1, its respective features are elected in the feature subsets, whereas 0 specifies nothing. It implies that the 2nd and 4th feature is selected for the feature subsets. The FF defined in Eq. (8):

$$fitness_t = \max\left((1-b) \times ACC + b \times \left(1 - \frac{m}{n}\right)\right) \tag{8}$$

where n represents the overall amount of features, m denotes the elected feature subset length, and b indicates a variable respective to make a balance among the feature reduction and classification accuracy could be in zero and one. It is shown in the experiment that b = 0.2. The ACC parameters are the classification accuracy rate created using rapid classifiers like WKELM for evaluating the feature set and make the accuracy value. In all iterations, fitness value is allocated to cuckoo's habitat in the search space. This position is calculated on all iterations, and the optimal positions are elected as the optimal solution.

3.3 Design of OKELM Based Classification Technique

During data classification, the chosen features are fed to the WKELM method for allotting suitable class labels. Generally, NN is used in regression problems and pattern identification. The BP and gradient based learning methods are the most popular methods used for NN. Additionally, this technique has some drawbacks such as complex set of learning variables, training losses, convergences, and slow learning. Because of this shortcoming of gradient based learning and traditional BPNN, the ELM approach was proposed [22]. In ELM method, the output weight of an SLFN is analytically calculated using MP generalized inverse instead of iterative learning scheme. The framework of SLFN uses ELM approach is given in the following. Here, $l_{1m},\ l_{2m}$ and l_{rm} denotes weight vector associated with input neuron and kth hidden, w represents weight vector associated with output, neuron and kth hidden $f(\cdot)$ signifies activation function. The main characteristics of ELM are given in the following:

i) In ELM framework, the learning speed is rapid. Owing to this, the SLFN is trained with ELM. Hence, an ELM technique is quicker compared to other conventional learning methods.

ii) The less training error and some kinds of weight are depending on ELM because it has improved performance for NN.
iii) In the architecture of SLFN, the ELM technique exploits non- differentiable activation functions.
iv) The easy solution is to try to get the ELM framework.

The ELM output using *m* neuron and *f* activation function is represented by:

$$o_{\mathrm{j}} = \sum_{\mathrm{i}=1}^{m} \beta_{\mathrm{i}} f(l_{\mathrm{i}} \mathrm{x}_r + b_{\mathrm{i}}) \tag{9}$$

The ELM method has a quicker learning speed compared to conventional NN. Furthermore, it has an optimal generalization efficacy. In ELM learning technique, the main parameter of hidden layer needn't be tuned. In ELM approach, each non-linear succeeding continuous function is utilized as hidden neuron. Fig. 3 shows the framework of WELM. Therefore, for M optional several instances $(r_{\mathrm{j}},\ m_{\mathrm{j}})|r_{\mathrm{j}} \in \mathrm{Q}^{l},\ m_{\mathrm{j}} \in \mathrm{Q}^{k},\ \mathrm{j} = 1,\ \cdots,\ M$, the output function in ELM uses K hidden neuron is represented by:

$$u_{\mathrm{K}}(r) = \sum_{j=1}^{\mathrm{K}} S_j v_j(r) = v(r)S \tag{10}$$

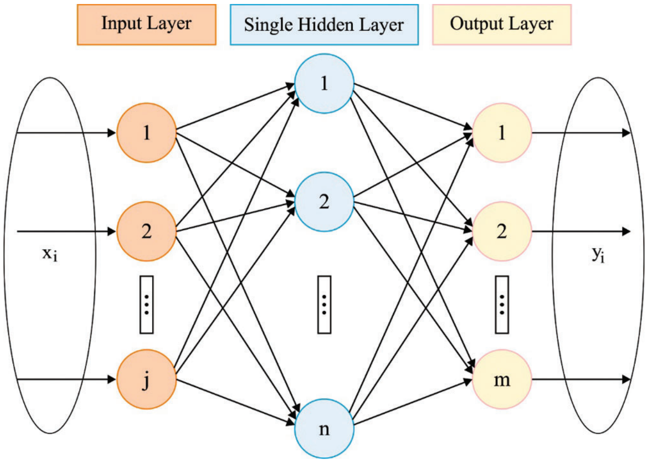

Figure 3: Structure of WELM

In which $v = [v_1(\mathrm{r}),\ v_2(\mathrm{r}), \ldots,\ v_{\mathrm{K}}(\mathrm{r})]$ indicates the output vector of hidden layer about input r. $S = [S_1,\ S_2,\ \ldots,\ S_{\mathrm{K}}]$ represent the vector of output weight amongst output neurons and hidden layers of K. V vector modifies the data from input space for ELM feature space. The output weight and trained error should be simultaneously minimalized to reduce the trained error in ELM method. Therefore, the generalization efficacy of NN is improved as follows:

$$minimize\ \|AS - C\| \tag{11}$$

Here, (11) is solved using

$$S = A^T \left(\frac{1}{E} + AA^T \right)^{-1} C \tag{12}$$

Whereas E denotes the regulation coefficient, A indicates hidden layer output matrix, and C represents foreseeable output matrix of instance, respectively. Therefore, the output function of ELM method is determined by:

$$u(r) = v(r)A^T\left(\frac{1}{E} + AA^T\right)^{-1}C \tag{13}$$

When the feature vector v(r) isn't known, the kernel matrix of ELM is depending upon Mercer condition evaluated by:

$$D = AA^T: \ k_{\mathrm{jz}} = v(r_{\mathrm{j}})v(\mathrm{r_z}) = b(r_{\mathrm{j}},\ \mathrm{r_z}) \tag{14}$$

In this manner, the output function $u(r)$ of WKELM is determined as follows:

$$u(r) = [b(r,\ r_1),\ \cdots,\ b(r,\ r_M)]\left(\frac{1}{E} + D\right)^{-1}C \tag{15}$$

Whereas, $D = AA^T$ and $b(r,$ g) represents kernel function of ELM. Numerous kernel functions include Gaussian, exponential, polynomial, and linear kernels i.e., appropriate for Mercer's condition in ELM study. In this work, WK functioning is utilized to performance and simulation analyses of WKELM:

$$b(r,\ \mathrm{g}) = \cos\left(w\frac{\|r-\mathrm{g}\|}{x}\right)\exp\left(-\frac{\|r-\mathrm{g}\|^2}{y}\right) \tag{16}$$

The result of this application was examined to train and test the efficacy of WK functioning proposed in (16) i.e., optimal than the efficacy of Gaussian, polynomial, linear, and exponential kernels, respectively. The values of adoptable parameter w, x, and y are needed to train the efficacy of ELM. Because of this variable, it should be considerately tuned to resolve the problems. But, the hidden layer feature mapping needn't be well known and several hidden neurons needn't be elected in WKELM method. Furthermore, the WKELM technique has an optimal generalization efficacy than conventional ELM method. At the same time, it is introduced that WKELM is very stable than traditional ELM and faster than SVM.

In order to tune the parameters involved in the WKELM model, the SFO algorithm is employed to optimally modify them. Yang [23] proposed the SFO approach inspired by the flower pollination procedure of flowering plants with the consideration of the biological reproductive procedure. Now, the stimulating nature of sunflower is to consider as searching procedure of optimum direction towards the sun. Under real world conditions, each single flower path sufficiently releases many pollen gametes. In the event of simplicity, each sunflower is taken into account for producing an individual pollen gamete and reproduced in an individual manner. One more essential nature based optimization existing on the inverse square law radiation. The law state that the number of radiations is inverse proportion to square of distance, e.g., the amount (intensity) of radiation decreases in proportional to the square of enhancing the distance. When the distance gets double, an intensity decreased by the factor 4, triples, and minimizes to the factor 9, etc. In this instance, the minimal distance from the plant to sun, a superior intensity of radiation attained, and it tends to stabilize in this vicinity. Similarly, the additional distances of the plant in the sun, the less intensity of heat attained it, hence it takes high step to get as near feasible to global optimal (sun) [24].

Next, the intensity quantity of heat Q attained with each plant as follows:

$$Q_i = \frac{P}{4\pi r_i^2} \tag{17}$$

whereas P denotes the power of source and r_i indicate the distances amongst the present optimal and plant i.

The direction of sunflower to the sun is given as follows:

$$\overrightarrow{s_i} = \frac{X^* - X_i}{||X* - X_i||},\ i = 1,\ 2,\ \ldots,\ n_p \tag{18}$$

In the steps of sunflower, s could be calculated by:

$$d_i = \lambda \times P_i(||X_i + X_{i-1}||) \times ||X_i + X_{i-1}|| \tag{19}$$

whereas λ signifies the constant value which defines the "inertial" displacement of plant, $P_i(||X_i + X_{i-1}||)$ means the likelihood of pollination, e.g., the sunflower i pollinates with their nearby neighbors $i-1$ generating the novel individual from the arbitrary position that varies according to the distances between the flowers. Especially, individual nearer to the sun is considered deceased step in search of local refinement as additional distant individuals are usually moving. Also, It could be important for restricting the maximal step provided by all individuals, appropriate not to skip regions prone to be global minimal candidates. It defined the maximum step by:

$$d_{\max} = \frac{||X_{\max} - X_{\min}||}{2 \times N_{\text{pop}}} \tag{20}$$

whereas $X_{\max}$ & $X_{\min}$ signifies the upper bound and lower bound and $\mathrm{N_{pop}}$ denotes the amount of plants of the whole population. The novel plantation is given by:

$$\overrightarrow{X}_{t+1} = \overrightarrow{X}_i + d_i \times \overrightarrow{s_i} \tag{21}$$

4 Performance Validations

This section validates the IDS performance of the CCSOA-OWKELM technique on two benchmark datasets namely NSL-KDD Dataset and CICIDS2017 dataset. The first dataset holds 42 features with 125973 instances. Besides, the second dataset includes 79 features with 225, 745 instances.

Fig. 4 illustrates the set of confusion matrices produced by the CCSOA-OWKELM technique on the NSLKDD-99 dataset with five different runs of execution. The figure has shown that the CCSOA-OWKELM technique has effectively classified the instances into two classes namely Normal and Abnormal. For instance, with run-5, the CCSOA-OWKELM technique has identified a set of 67325 instances into 'Normal' and 58615 instances into 'Intrusion'.

Fig. 5 showcases the set of confusion matrices formed by the CCSOA-OWKELM approach on the CICIDS2017 dataset with 5 distinct runs of execution. The figure demonstrated that the CCSOA-OWKELM manner has effectually classified the instances as to 2 classes namely Normal and Abnormal. For sample, with run-5, the CCSOA-OWKELM method has recognized a set of 97628 instances into 'Normal' and 127949 instances into 'Intrusion'.

Tab. 1 demonstrates the detection performance of the CCSOA-OWKELM technique on the applied dataset. The table values depicted that the CCSOA-OWKELM technique has accomplished maximum classification outcomes on the applied two datasets. For instance, with the NSL-KDD dataset, the CCSOA-OWKELM technique has resulted in a higher average precision of 0.9998, recall of 0.9997, accuracy of 0.9997, and F-score of 0.9997. Also, with the CICIDS2017 dataset, the CCSOA-OWKELM method has resulted in a maximum average precision of 0.9991, recall of 0.9991, accuracy of 0.9992, and F-score of 0.9991.

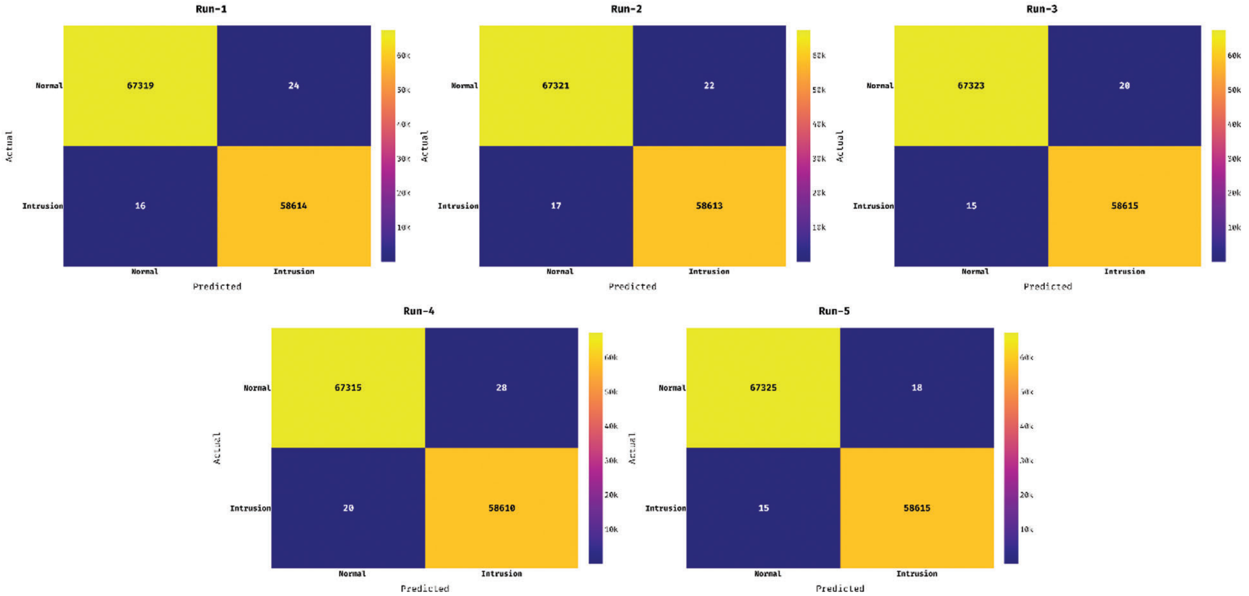

Figure 4: Confusion matrix of NSL-KDD dataset

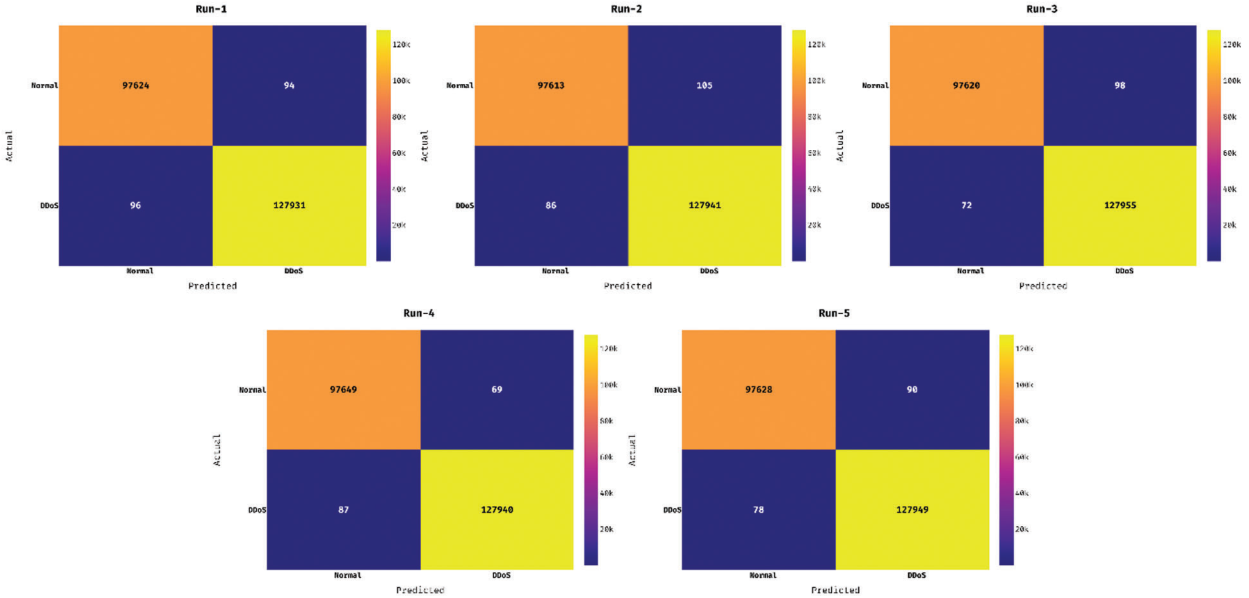

Figure 5: Confusion matrix of CICIDS2017 dataset

In order to verify the betterment of the CCSOA-OWKELM technique on the applied NSL-KDD dataset, a brief comparison study is made in Tab. 2. The results demonstrated that the RF technique has resulted in poor performance with lower accuracy of 0.9595. At the same time, the DT technique has offered slightly increased outcomes by offering an accuracy of 0.9785. Likewise, the SVM and DeepNN techniques have showcased moderately increased accuracy values of 0.9822 and 0.9884 respectively. Moreover, the k-NN and WKELM techniques have accomplished a competitive accuracy of 0.9973 and 0.9993. However, the CCSOA-OWKELM technique has demonstrated superior performance with a maximum accuracy of 0.9997.

Table 1: Results analysis of proposed CCSOA-OWKELM model in terms of various measures

No. of runs	Precision	Recall	Accuracy	F-Score
NSL-KDD Dataset				
Run-1	0.9998	0.9996	0.9997	0.9997
Run-2	0.9997	0.9997	0.9997	0.9997
Run-3	0.9998	0.9997	0.9997	0.9997
Run-4	0.9997	0.9996	0.9996	0.9996
Run-5	0.9998	0.9997	0.9997	0.9998
Average	0.9998	0.9997	0.9997	0.9997
No. of Runs	Precision	Recall	Accuracy	F-Score
CICIDS2017 Dataset				
Run-1	0.9990	0.9990	0.9992	0.9990
Run-2	0.9991	0.9989	0.9992	0.9990
Run-3	0.9993	0.9990	0.9992	0.9991
Run-4	0.9991	0.9993	0.9993	0.9992
Run-5	0.9992	0.9991	0.9993	0.9991
Average	0.9991	0.9991	0.9992	0.9991

Table 2: Results analysis of existing with proposed CCSOA-OWKELM model in terms of various measures on NSL-KDD dataset

Methods	Precision	Recall	Accuracy	F-score	Error
Deep NN	0.9915	0.9836	0.9884	0.9875	0.0116
k-NN	0.9971	0.9972	0.9973	0.9971	0.0027
SVM	0.9993	0.9625	0.9822	0.9805	0.0178
Decision Tree	0.9821	0.9714	0.9785	0.9766	0.0215
Random Forest	0.9978	0.9148	0.9595	0.9544	0.0405
WKELM	0.9994	0.9992	0.9993	0.9993	0.0007
CCSOA-OWKELM	0.9998	0.9997	0.9997	0.9997	0.0003

Fig. 6 illustrates the ROC analysis of the CCSOA-OWKELM technique on the applied NSL-KDD dataset. The figure reported that the CCSOA-OWKELM technique has gained effective intrusion detection outcomes with a maximum ROC of 99.9856.

A brief processing time analysis of the CCSOA-OWKELM technique with existing techniques takes place on the NSL-KDD dataset in Tab. 3 and Fig. 7. The results portrayed that the DT and RF techniques have shown ineffective performance with the lower processing time of 80.21 s and 82.76 s respectively. Followed by, the k-NN and SVM techniques have gained slightly improved outcomes with the processing time of 75.09 s and 78.45 s respectively. Next, the WKELM and Deep NN techniques have tried to show moderate processing times of 64.82 s and 56 s respectively. However, the CCSOA-OWKELM technique has outperformed the existing techniques with a minimum processing time of 45.91 s.

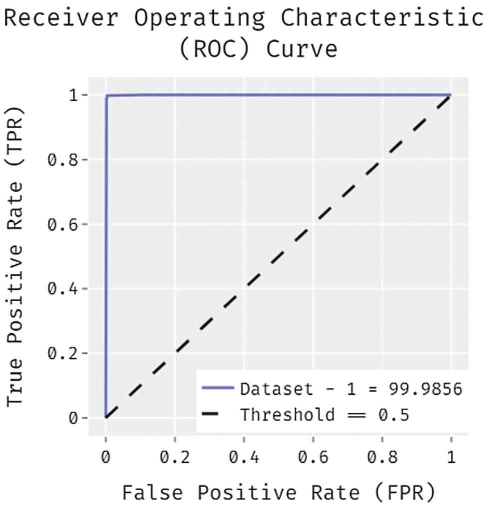

Figure 6: ROC analysis of CCSOA-OWKELM model on NSL-KDD dataset

Table 3: Results analysis of existing with proposed CCSOA-OWKELM model in terms of processing time(s) on NSL-KDD dataset

Methods	Time (s)
Deep NN	56.00
k-NN	75.09
SVM	78.45
Decision Tree	80.21
Random Forest	82.76
WKELM	64.82
CCSOA-OWKELM	45.91

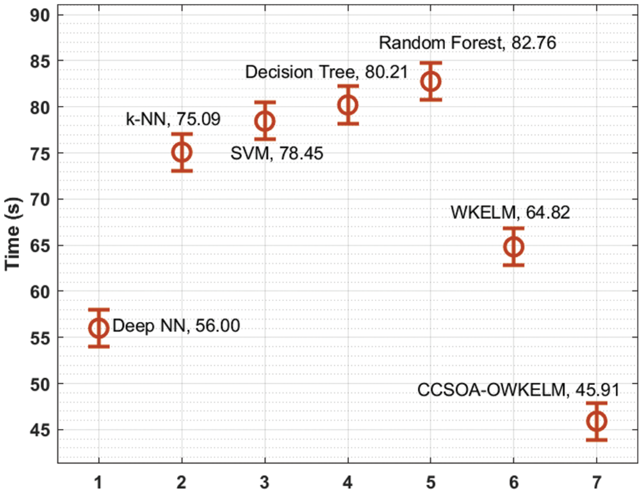

Figure 7: Processing time analysis of CCSOA-OWKELM model on NSL-KDD dataset

For verifying the betterment of the CCSOA-OWKELM manner on the applied CICIDS2017 dataset, a detailed comparative analysis is made in Tab. 4. The outcomes outperformed that the XGBoost method has resulted in a worse efficiency with minimal accuracy of 0.9136. Simultaneously, the ZED-IDS algorithm has accessible somewhat improved results by offering an accuracy of 0.9573. Also, the DeepWindow and DNN-kNN manners have exhibited moderately higher accuracy values of 0.9950 and 0.9963 correspondingly. In addition, the WKELM method has accomplished a competitive accuracy of 0.9982. Eventually, the CCSOA-OWKELM methodology has outperformed higher efficiency with maximal accuracy of 0.9992.

Table 4: Results analysis of existing with proposed CCSOA-OWKELM model in terms of various measures on CICIDS2017 dataset

Methods	Precision	Recall	Accuracy	F-score	Error
XGBoost	0.9123	0.9740	0.9136	0.9247	0.0864
ZED-IDS	0.9272	0.9583	0.9573	0.9435	0.0427
DeepWindow	0.9910	0.9940	0.9950	0.9890	0.0050
DNN-kNN	0.9929	0.9969	0.9963	0.9949	0.0037
WKELM	0.9950	0.9984	0.9982	0.9967	0.0018
CCSOA-OWKELM	0.9991	0.9991	0.9992	0.9991	0.0008

Fig. 8 depicts the ROC analysis of the CCSOA-OWKELM manner on the applied CICIDS2017 dataset. The figure stated that the CCSOA-OWKELM algorithm has attained effectual intrusion detection results with higher ROC of 99.9914.

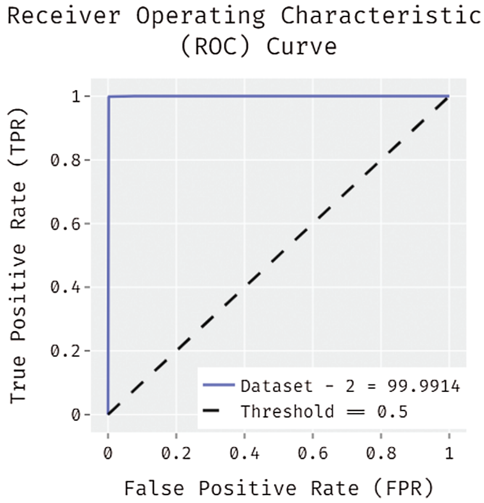

Figure 8: ROC analysis of CCSOA-OWKELM model on CICIDS2017 dataset

A detailed processing time analysis of the CCSOA-OWKELM algorithm with recent manners takes place on the CICIDS2017 dataset in Tab. 5 and Fig. 9. The outcomes exhibited that the XGBoost and ZED-IDS approaches have displayed ineffective performance with the lesser processing time of 98.33 s and 86.48 s correspondingly. In line with, the DeepWindow and DNN-kNN techniques have reached somewhat increased results with the processing time of 76.09 s and 84.67 s correspondingly. Afterward, the WKELM methodology has tried to show moderate processing time of 72.10 s. Lastly, the CCSOA-OWKELM algorithm has showcased the recent methods with lesser processing time of 68.48 s.

Table 5: Results analysis of existing with proposed CCSOA-OWKELM model in terms of processing time (s) on CICIDS2017 dataset

Methods	Time (s)
XGBoost	98.33
ZED-IDS	86.48
DeepWindow	76.09
DNN-kNN	84.67
WKELM	72.10
CCSOA-OWKELM	68.48

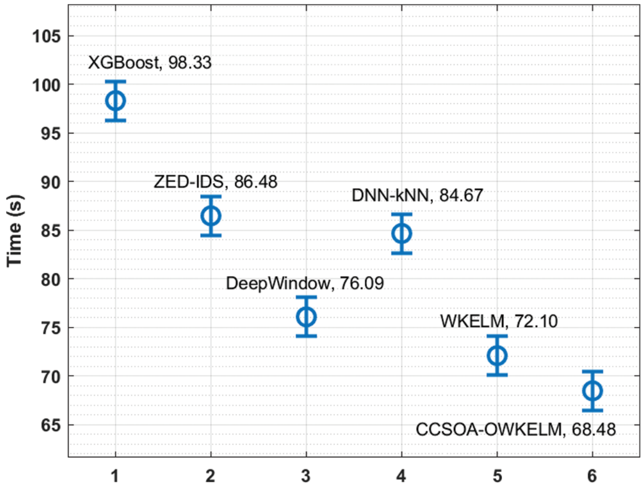

Figure 9: Processing time analysis of CCSOA-OWKELM model on CICIDS2017 dataset

5 Conclusion

In this study, a new CCSOA-OWKELM technique is derived for IDS in the Industry 4.0 environment. The CCSOA-OWKELM technique involves three major processes such as pre-processing, CSSOA based feature selection, and OKELM based classification. The CCSOA-OWKELM technique involves the design of CCSOA based feature selection technique, which incorporates the concepts of chaotic maps with CSOA. Moreover, the use of hyperparameter optimization of the WKELM technique helps to accomplish maximum detection performance. An extensive experimental analysis is carried out on the two benchmark datasets and examined the results interms of different measures. The experimental outcomes demonstrate the promising performance of the CCSOA-OWKELM technique over the recent state of art techniques. As a part of future work, the CCSOA-OWKELM technique can be extended to the design of outlier detection approaches.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under grant number (RGP1/338/40). Princess Nourah bint

Abdulrahman University Researchers Supporting Project number (PNURSP2022R237), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

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

References

[1] N. Moustafa, E. Adi, B. Turnbull and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," *IEEE Access*, vol. 6, pp. 32910–32924, 2018.

[2] H. Kwon, "Dual-targeted textfooler attack on text classification systems," *IEEE Access*, pp. 1, 2021.

[3] L. Alonso, J. Barbarán, J. Chen, M. Díaz, L. Llopis *et al.,* "Middleware and communication technologies for structural health monitoring of critical infrastructures: A survey," *Computer Standards & Interfaces*, vol. 56, pp. 83–100, 2018.

[4] P. O'Donovan, C. Gallagher, K. Bruton and D. T. J. O'Sullivan, "A fog computing industrial cyber-physical system for embedded low-latency machine learning industry 4.0 applications," *Manufacturing Letters*, vol. 15, pp. 139–142, 2018.

[5] P. Harsha and M. Dahleh, "Optimal management and sizing of energy storage under dynamic pricing for the efficient integration of renewable energy," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1164–1181, 2015.

[6] A. Stăncioiu, "The fourth industrial revolution Industry 4.0," *Fiabilitate Şi Durabilitate*, vol. 1, no. 19, pp. 74–78, 2017.

[7] S. Alem, D. Espes, E. Martin, L. Nana and F. De Lamotte, "A hybrid intrusion detection system in industry 4.0 based on ISA95 standard," in *2019 IEEE/ACS 16th Int. Conf. on Computer Systems and Applications (AICCSA)*, Abu Dhabi, United Arab Emirates, pp. 1–8, 2019.

[8] R. Govindaraju, K. Lukman and D. R. Chandra, "Manufacturing execution system design using ISA-95," *Advanced Materials Research*, vol. 980, pp. 248–252, 2014.

[9] P. Mehra, "A brief study and comparison of snort and bro open source network intrusion detection systems," *Int. Journal of Advanced Research in Computer and Communication Engineering*, vol. 1, no. 6, pp. 383–386, 2012.

[10] J. Lee, H. A. Kao and S. Yang, "Service innovation and smart analytics for Industry 4.0 and big data environment," *Procedia CIRP*, vol. 16, pp. 3–8, 2014.

[11] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "TON_IoT Telemetry Dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

[12] S. Latif, Z. Idrees, Z. Zou and J. Ahmad, "DRaNN: A deep random neural network model for intrusion detection in industrial IoT," in *2020 Int. Conf. on UK-China Emerging Technologies (UCET)*, Glasgow, United Kingdom, pp. 1–4, 2020.

[13] M. A. Basset, V. Chang, H. Hawash, R. K. Chakrabortty and M. Ryan, "Deep-IFS: Intrusion detection approach for industrial internet of things traffic in fog environment," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7704–7715, 2021.

[14] K. N. Qureshi, S. S. Rana, A. Ahmed and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustainable Cities and Society*, vol. 61, pp. 102343, 2020.

[15] V. Priya, I. S. Thaseen, T. R. Gadekallu, M. K. Aboudaif and E. A. Nasr, "Robust attack detection approach for iiot using ensemble classifier," *Computers Materials & Continua*, vol. 66, no. 3, pp. 2457–2470, 2021.

[16] L. Zhou, H. Guo and G. Deng, "A fog computing based approach to DDoS mitigation in IIoT systems," *Computers & Security*, vol. 85, pp. 51–62, 2019.

[17] M. A. Hawawreh, E. Sitnikova and F. d. Hartog, "An efficient intrusion detection model for edge system in brownfield industrial Internet of Things," in *Proc. of the 3rd Int. Conf. on Big Data and Internet of Things*, Australia, pp. 83–87, 2019.

[18] M. M. Hassan, S. Huda, S. Sharmeen, J. Abawajy and G. Fortino, “An adaptive trust boundary protection for IIoT networks using deep-learning feature-extraction-based semisupervised model,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2860–2870, 2021.

[19] H. Qiao, J. O. Blech and H. Chen, “A machine learning based intrusion detection approach for industrial networks,” in *2020 IEEE Int. Conf. on Industrial Technology (ICIT)*, Buenos Aires, Argentina, pp. 265–270, 2020.

[20] R. Rajabioun, “Cuckoo optimization algorithm,” *Applied Soft Computing*, vol. 11, no. 8, pp. 5508–5518, 2011.

[21] J. Hamidzadeh, “Feature selection by using chaotic cuckoo optimization algorithm with levy flight, opposition-based learning and disruption operator,” *Soft Computing*, vol. 25, no. 4, pp. 2911–2933, 2021.

[22] D. Avci, “An automatic diagnosis system for hepatitis diseases based on genetic wavelet kernel extreme learning machine,” *Journal of Electrical Engineering and Technology*, vol. 11, no. 4, pp. 993–1002, 2016.

[23] X. S. Yang, “Flower pollination algorithm for global optimization,” in *Int. Conf. on Unconventional Computing and Natural Computation*, Springer, Berlin, pp. 240–249, 2012.

[24] Z. Yuan, W. Wang, H. Wang and N. Razmjooy, “A new technique for optimal estimation of the circuit-based pemfcs using developed sunflower optimization algorithm,” *Energy Reports*, vol. 6, pp. 662–671, 2020.