An Intelligent CSO-DBNN Based Cyber Intrusion Detection Model for Smart Grid Power System

Mrs. Sabita Nayak[1*], Mr. Amit Kumar[*2]

[*]*Assistant Professor, Department of Electronics and Communication, B.I.T. Sindri, University-JUT, Dhanbad, Jharkhand, India*

Abstract *— Massive proliferation in cyber-attacks has drawn much attention today among researches and network users of different arena sectors. After all these years of research aftereffects against cyber-attack, still we lack in reliable Intrusion Detection System (IDS) which can adjust by itself for bulk amount of data based on the real time situations. In this manuscript, we present an IDS model to classify the different class of cyber-attack scenarios such as short circuit, relay setting change, remote command input, false data injection, line maintenance, and failure detection in SG power-system. Furthermore, a preprocessing, data normalization, feature selection are carried out and finally, after applying Gaussian random distribution the taxonomy here is done by Cat Swarm Optimization (CSO) [21] algorithm trained Deep Belief Neural Network (DBNN) with minimum MSE. At last accuracy, precision, recall, and F1 score metrics are analyzed to show the reliability of our proposed CSO assimilated Machine learning based intrusion detection systems in a SG power system*

Keywords *— Deep Belief Neural Networks, Cat Swarm Optimization, Intrusion Detection System, Smart Grid (SG) power system*

I. INTRODUCTION

At present internet is the vital gateway to all sector information and at the same time attackers and malicious users sought for the networks with insecure services and Trojan attacked systems [1]. Therefore an alert system is required to notify the administrator or user about the attack and type of attack to ensure the integrity and safety of the system and data [2]. Hence, in recent years Intrusion Detection System (IDS) reveals its promising impacts in monitoring, attack detection and classification in manifold sectors [3]. Although, employing IDS for real time applications still face some crucial challenges even after the introduction of various IDS models by researches [4]. Machine learning algorithms congealed a decent endeavor in overcoming these challenges was proved by the researches but still exactness of attack detection rate may vary based on the feature extraction and classification techniques chosen by them [5].

The IDS system model designed can be of software, hardware or mixture of both and its main objective is to safeguard the system from all kind of threat and malicious activities before they do real damage to the resources [6]. Smart grid (SG) is a next generation electrical grid system to overcome convention system with one way communication, manual restoration, limited control and centralized operation [7]. On the other hand, threats such as Advanced Persistent Threat (APT) Man-in-The-Middle (MiTM), Denial of Service (DoS) and False Data Injection (FDI) attacks interrupt the privacy and reliability of the SG network system [8]. Researchers have come up with many IDS strategies such as IDS relying on a Support Vector Machine (SVM) by A. Patel et al. in [9], signature-based IDS by B. Kang et al.[10], adaptive Artificial Neural Network (ANN) by Nadai et al. in [11], K Nearest Neighborhood (KNN) by Naoum et al in [12], deep belief network by Zhao et.al in [13] etc ,but they results in high level of false positives. Therefore an effectual integration of classifier with heuristic approaches trends today may pave a way to design an efficient IDS system model for Smart Grid Power system.

In this paper, the intelligent intrusion detection system (IDS)based on Cat Swarm Optimization (CSO) algorithm trained Deep Belief Neural Network (DBNN)for Smart Grids (SG) in a power system concept is proposed. Here we present the IDS model and the SG architecture along with the description of suggested CSO and DBNN in training and classifying the attacks. The left over sub division of the manuscript is regulated as follows. In section 2 a comprehensive prose review has been carried out on the various intrusion detection system using neural networks and other related works on IDS. Section 3 addresses about the Preliminaries of CSO and DBNN modules along with the proposed approach and section 4 discuss about the discussion and analysis on the results of the proposed framework by evaluating the performance on various metrics and finally section 5 delivers the concluding remarks

II. RELATED WORK

In this section, among the numerous research works on cyber-attacks and IDS strategies selected contemporary research works were reviewed here in this section.

Yang et al. in [14] has introduced an effective defense strategy for data integrity attacks in the smart grid system. In addition they designed a model to detect the sparsest attack vector proficiently and system its performance analysis on IEEE standard systems proves its efficiency in attack detection with less complexity. Then, they have proposed a PMU placement strategy to ensure the integrity and scrutinizing of the system against the attacks and the results obtained shows its intolerance with cost.Gunduz et al. in [15] has presented a survey just about the cyber-security threats also defense solutions designed for smart grid applications and studied about the security perspective of research scholars in recent. In the manuscript initially, they deliberate the contextual info about the SG and its components, pros and cons etc. Then they discuss about the recent trends in improving the SG security and highlight its efficiency in SG application and future direction. Efstathopoulos et al. in [16], has introduced operational data based cyber-attack detection by exploiting the correlation in between the data values in SGs. This strategy will improve the efficiency in attack detection and that was analyzed by comparing it with various deep and machine learning techniques. Their proposed anomaly based mechanism will accurately detect the attack and at the same time anomalies may degrade the performance of the grid devices. Hence, as a future direction they suggest to enhance the suggested architecture with more improved DNN's based LSTM layers for multi-dimensional operational data. Binna et al. in [17] has experimented on the machine learning algorithms and observed its proficiency in attack classification and challenge in detecting the subset level attacks. So that they suggest making use of RNNs to detect the subset level attacks in future and studied about the sparse and replay attacks by varying 'A' values to generate additional data with ease. In addition they have studied about the performance of ML algorithms with large dataset and 118-bus system on detecting the subset level attacks on state estimation. Finally they discussed about the future search area and its gateway to AC state estimation. Aljarah et al. in [18] has proposed the Whale Optimization Algorithm (WOA) to overcome the convergence and local optima problem in training the MLP network. In the paper the main objective of WOA was to optimize the bias, weights and to minimize the MSE. The performance evaluation of the proposed approach was analyzed by using 20 test functions with diverse features. The effectiveness of the proposed strategy was shown by comparing it with the conventional evolutionary and swarm intelligent training algorithms. Finally they depicts that the suggested algorithm proves its efficiency in accuracy, local optima avoidance, high convergence speed and training reliability even with the different levels of difficulty. Hassib et al. in [19] has proposed a classification framework based on WOA-BRNN with three phases (i) determination of optimal features by WOA (ii) preprocessing by SMOTE algorithm and LSH-SMOTE (iii) Classification by WOA-BRNN. The approach was validated based on two trials: (i) WOA-BRNN against five classifiers for imbalanced dataset (ii) WOA-BRNN against GWO-MLP, PSO, GA, ACO, ES, and PBIL over Balloon, Breast cancer, Iris, and Heart datasets. Finally they concluded that the proposed approach is capable to handle the imbalanced big data by avoiding local optima and achieves a precise classification outcome with a drawback of extended running time. Genge et al. in [20] has designed two IDS model for SGs can be applied for shortest path routing and budgetary limitations with resilient infrastructure. Path selection, device distribution and less computation time can be achieved by using a heuristic approach and the proposed design was analyzed in two scenarios. Finally, the performance of the proposed design was evaluated based on the computational time and its applicability to huge problems.

III. PROPOSED METHODOLOGY

A. Overview

The entire document should be in Times New Our suggested DBNN approach is forged from the well-organized weighted Restricted Boltzmann Machines (RBMs) and trained by learning algorithm based on the desire vogue i.e while learning RBM, some layers are not considered. Figure 1 shows the architecture of DBNN. It is illustrated that it has N number of layers, weighted matrix Wk at layer k and its hidden units will be the input to the next layer k+1.The gradient descent and back-propagation algorithm is utilized here to train the learning algorithm and to adjust the weight (wk) parameters. Our suggested swarm intelligence algorithm (CSO) aims at minimizing the MSE and to overcome the local minima deception based on the consequence of the output layer and sometimes the weights may upsurge in the course of convergence progression. Our main objective in this paper to model the smart grid cyber intrusion detection system, in which the CSO will train the DBNN and the optimal weight obtained by CSO will the used in the DBNN and to conclude proposed model performance where analyzed based on some metrics to deliberate the efficiency.

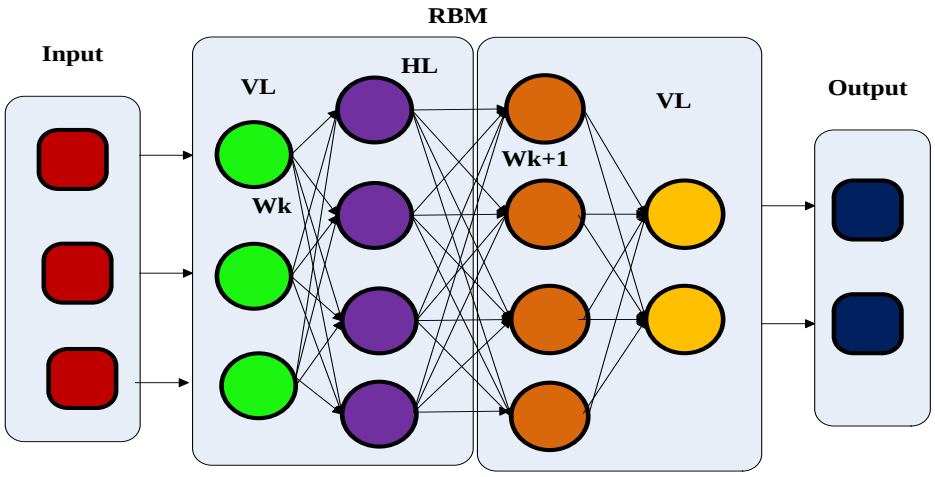

Fig. 1 Architecture of DBNN

1) Deep Belief Neural Network: Our DBNN is a multiplicative model which integrates RBM (multilayer unsupervised learning networks) and Back Propagation (supervised learning network) by means of independent layers. In which the parameters of the RBM will be optimized based on stochastic gradient ascent on the log-likelihood of training patterns, then the training data sample will be given to the visible layer and the probability will be evaluated in the hidden layers by using the below equation.

$$p(v) = \sum_{h} e^{-E(v,\square)} \Big/ \sum_{v,\square} e^{-E(h,v)} \quad (1)$$

Here, we assume that *v and h* as the visible *v* and hidden $h \in \{0, 1\}$ layers respectively and $E\,(h_j v_i)^{\text{data}}$ and $e^{-E(h,v)}$ has been computed by using the following equations (2-6). The sampled *v* and *h* variables are sampled to pre train the DBNN in the first level, and then based on the optimization algorithm optimal value of *v* and *h* are the input vectors to the next level in the DBNN and this will be continued until the last hidden and visible layer of the network.

$$E(hv)^{data} = p\left[{}^{h}/_{v}\right]v^{T} \quad (2)$$

Where, *p*[*h*/*v*] represents the probability of attaining *h* by means of the training data *v*. i.e the hidden vector is deliberated as shown in figure (6).

$$p\left[h_j = 1/v\right] = \sigma\left(\sum_{i=1}^{m} w_{ij} v_i + a_j\right) \quad (3)$$

$$p\left(h_j = 0/v\right) = 1 - p\left(h_j = 1/v\right) \quad (4)$$

Similarly the visible vector probability can be deliberated as follows

$$p\left[v_j = {}^{1}/_{h}\right] = \sigma\left(\sum_{i=1}^{m} w_{ij} h_i + b_j\right) \quad (5)$$

$$p\left(v_j = 0/h\right) = 1 - p\left(v_j = 1/h\right) \quad (6)$$

Where,

$$\sigma(y) = 1/1 + e^{-y}\,; Logistic\ Sigmoid\ functio \quad (7)$$

Here, we assume that the *h* and *v* are the binary stochastic units and its energy can be illustrated as follows,

$$Energy(v, \square, \theta) = -v^{T} wh - b^{T} v - a^{T} h \quad (8)$$

Where *w*- is the weight vector between the *h* and *v* a and b - are the variable bias of *h* and *v*
$\Theta = \{w,a,b\}$.

For any particular configuration, the probability of *h* and *v* can be expressed as follows:

$$Energy(v, \square, \theta) = e^{-energy(v,\square,\theta)} \quad (9)$$

Then, the weight updation can be succeeded by evaluating the impending derivatives below:

$$\partial \log p(v, \square; \theta)/\partial \theta_{ij} = E\left(h_j v_i\right)^{data} - E\left(h_j v_i\right)^{model} \quad (10)$$

$$\partial \log p(v)/\partial a_i = v_i - E(v_i)^{model} \quad (11)$$

$$\partial \log p(v)/\partial b_j = E(h_i)^{data} - E\left(h_j\right)^{model} \quad (12)$$

Where,

E(.)- Probability operators

$E(.)^{\text{data}}$ - $E(.)^{\text{model}}$ -Probability of constructed and reconstructed data driven

The contrastive divergence for the parameter model, $\Theta = \{w,a,b\}$ is exposed in equation (13).

$$\theta^{n+1} = \theta^{n} + \in \left(\left(v_i^0 h_j^0 \right) - \left(v_i^n h_i^n \right) \right) \quad (13)$$

In any case the reconstructed data will be similar to that of the model data then the updating will be carried out by using the equation (14).

$$\theta^{n} = \theta^{n-1} + \in \left(\left(v^0 h^0 \right) - \left(v^1 h^1 \right) \right) \quad (14)$$

2) Cat Swarm Optimization Algorithm(CSO): Cat Swarm Optimization algorithm have being renovated based on swarming behaviour of cats which spends its time by relaxing and surveying its presents environment to a certain extent satisfactorily with no waste of energy resources by chasing onto something. Based on this behavioural characteristics of cats, the CSO algorithm is classified into two phases namely (i) seeking and (ii) Tracing i.e by means of target chasing and relaxing & surveying characteristics.The important factors of seeking phase by Chu et al. [7-8] are as follows:

- Seeking Memory Pool (SMP)
- Seeking Range of the selected Dimension (SRD)
- Counts of Dimension to Change (CDC)
- SelfPosition Consideration (SPC)

Phase 1: Seeking

It includes subsequent steps as follows:

Step 1: Create replicas(*j*) of current cat position(*k*) and check *j*=SMP; SPC=true;*J*=SMP-1, then the current position is retained as one of the candidate.

Step 2: Then based on CDC of each and every replica we randomly add or subtract the SRD to the current value and then replace it with the new one.

Step 3: Evaluate the fitness value (FS) of all the candidate solutions

For Minnimum Solution $FS_b = FS_{max}$

For Maximum Solution $FS_b = FS_{min}$

Step 4: Set the probability of each candidate solution to 'one' or else evaluate it by using the following equation (14)

Step 5: From among the available candidate points chose a point randomly to replavce the cat 'k' position.

$$p_i = {[FS_i - FS_b]}/{FS_{max} - FS_{min};\ 0 < i < j} \quad (14)$$

Phase II: Tracing

After completeing the phase I i.e seeking, when the cats enters the Phase II i.e tracing, they moves based on their velocity in each dimensions. It includes subsequent steps as follows:

Step 1: For each and evry dimension, the velocity was updated using the equation(15).

$$v_{k,d} = v_{k,d} + r_1 \times c_1 \times \left[x_{best,d} - x_{k,d} \right]; d = 1,2,3, \ldots\ldots M \quad (15)$$

Where, $x_{best,\ d}$- Best cats position with best fitness value $x_{k,d}$ - Cat Position, c_1 and r_1 =constant and random value (0,1) respectively

Step 2: Make sure that the velocity is within in the range or not, if it exceeds make the value equal to the range

Step 3: Update the position of the cat by using the following equation (16).

$$x_{k,d} = x_{k,d} + v_{k,d} \quad (16)$$

To solve the optimization problem, initially we have to make the decision on total number of cats or individuals and its position with M dimensions and its velocities, fitness function and a flag to known its current phase (seeking or tracing). Following are the standard steps in CSO for solving optimization problems.

Step 1 : Generate a set of cats (N) for the upcoming process.

Step 2: Intersperse the cats randomly into the solution space with M dimension and it should be in the range of desired max.velocity for every cats in the solution space. Then based on the mixture ratio (MR) value (we set minimum) we chose any one of the cat among the population to phase I.

Step 3: Fitness evaluation based on our objective and not edown the best cat positions so far.

Step 4: Cat movement were done based on the flags (Phase I/Phase II)

Step 5: Again randomly chose the set of cats in phase II by considering the MR value and the left over cats will be siigned to phase I.

Step 6: Terminate, if the stopping criteria is satisfied or else repeat from step 3-5.

3) Proposed CSO-DBNN based IDS Prototype: In this section, our proposed CSO-DBNN is employed to train the DBNN to categorize the cyber threats in the SG power system based on the normal events. In our proposed CSO-DBNN framework, cats (search agents) are initialized to optimize the deep belief network with hidden and visible lyers, bias and weight vectors. Each cats are evaluated by means of Mean Square error (MSE) and our CSO trained DBNN will simulateoulsly evaluate the optimal set of weights and its resultant

network configuration.We assume that the MSE of the network is taken as the Fitness function to the cats (search agents) to evaluate difference in the desired and forecasted results and it is shown in equation (17).

$$MSE = \sum_{I=1}^{N} \left(C_I - \hat{C}_I\right)^2 / N \quad (17)$$

The range of training and testing data will be of various ranges so normalization is required Where, $\acute{v}$ is the normalization value within the range of (0, 1) and this can be obtained by the following equation (18).

$$\acute{v} = {}^{v - v_{min}}/_{v_{max} - v_{min}} \quad (18)$$

In figure 2, the flow of our proposed strategy is deliberated, after processing and normalization, feature selection (dimension reduction) was carried out which is combined with the classifier to ease the classification of attack with high accuracy. Based on Gaussian distribution, the dataset was sub classified into training and testing data. At last the, CSO-DBNN prototype with optimal bias and weights achieved even though training is provided for testing to evaluate the efficiency of the IDS system model for Smart Grids. Our suggested CSO algorithm has the greater ability in disabling the local optima problem mostly seen in other optimization algorithms and this boost up the efficiency in obtaining the optimal bias and weights for our suggested IDS system model.

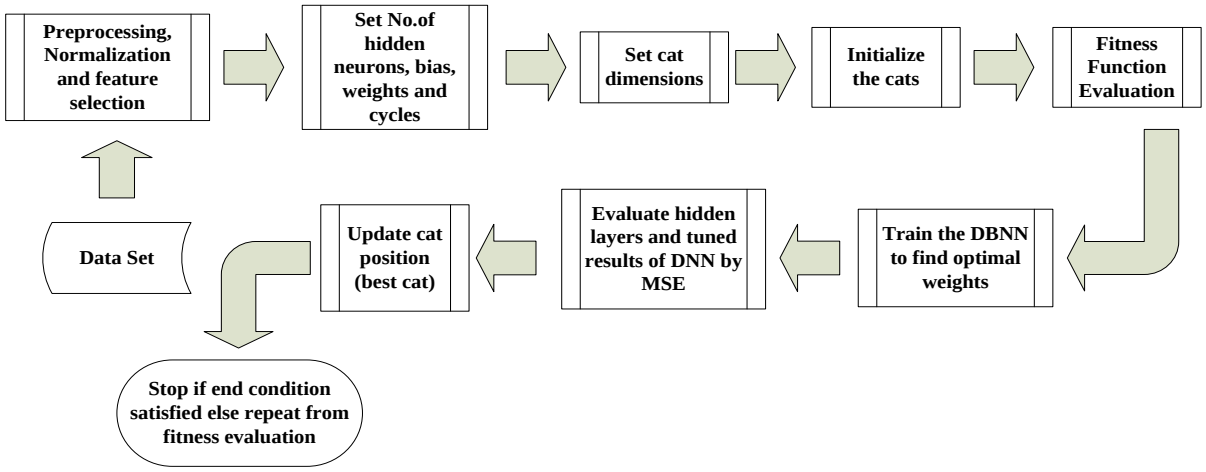

Fig. 2 Working Flow of our Proposed System Model

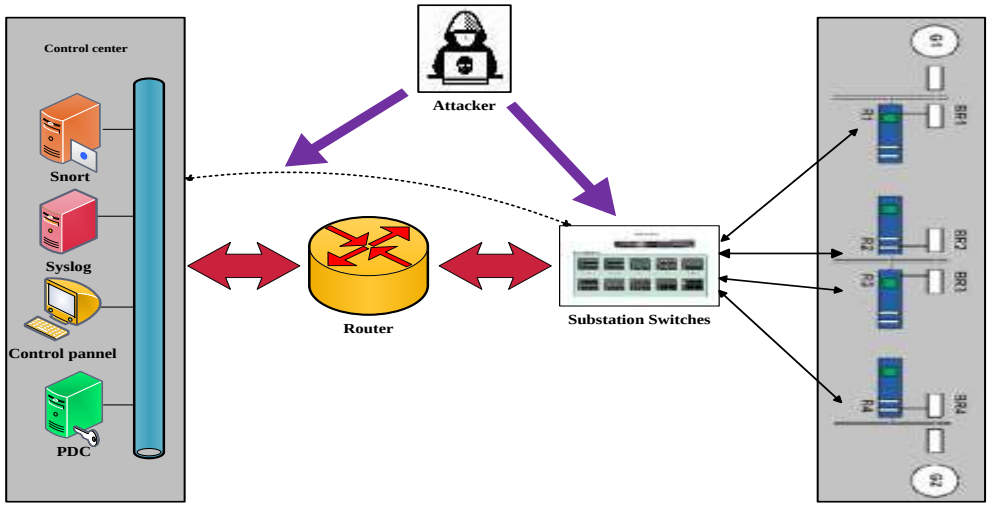

Fig. 3 SG-Power System Architecture

Figure 3 shows SG power system architecture with generators, transmission lines, relays, bus bars, circuit breakers and a control center with snort, syslog, control panel and PDC to control over the network. The relays in the architecture are used as a communicator in between the Substation switch and the router and trip the breakers either for real and

fake distinguished faults/attack in the system without any validation. In other case user can also manually instruct the relays to trip the breakers. The power distribution center (PDC) will take control over all the electrical equipment and power distributions.

During the every iteration cycle, the population of cat was evaluated by using the fitness function until we reach the iteration limit and then we will get a set of optimal features to detect the attack in the power system to classify and to predict the attack with high efficiency. Subsequently after the complete iteration cycle we will get a DBNN with less MSE and optimal weights. Lesser the MSE, the attack classification accuracy will be high with good generalization capability. The performance of the of our IDS system strategy will be evaluated based on accuracy (AC), False Alaram (FA)/Precision and Detection rate (DR)/Recall as per TP (True Positive), TN (True Negative), FP(False Positive) and FN (False Negative) is defined as below equation from (19-21).

$$Ac = {(TP + TN)}/{(TP + TN + FP + FN)} \quad (19)$$

$$DR = {(TP)}/{(TN + FN)} \quad (20)$$

$$FA = {(FP)}/{(TN + FP)} \quad (21)$$

$$F_1Score = 2\left[\frac{Precision(FA) \times Recall(DR)}{FA + DR}\right] \quad (22)$$

Where, True Positive (TP) is the number of SG power system attacksregisteredprecisely classified. True Negative (TN) is the number of standardregisters correctly classified. False Positive (FP) is the number of registered records imprecisely classified. False Negative (FN) is the number of SG attacksregistersimprecisely classified.

IV. RESULT AND DISCUSSION

The proposed technique displayed here contributes security against cyber-attack to the disseminated SG power system framework and the simulation outcome of IDS using CSO-DBNN is described here in this section. Execution of the IDS frameworks is estimated by their accuracy in detecting the attack scenarios. In order to implement the IDS framework on publicly available multiclass dataset, initially data should be pre-processed, normalized and features where selected. Then we have to set the iteration range, number of cats (search agents), dimensions, and visible and hidden layer biases. Finally the steps explained in the above sections were followed to know the presence of cyber-attack or not. Metrics such as accuracy, precision, recall, and F1 score are utilized to evaluate the performance of our proposed IDS model. By considering confusion matrix table 1, accuracy, precision, recall, and F1 are evaluated by using the equations (19-22). The accuracy evaluated will represent the exactness of cyber-attack classification process. The precision evaluated will represent how often the classifier prediction was correctand recall represents the real occurance of attack and its prediction exactness, where F1 score is the integration of both the precision and recall.

TABLE. I CONFUSION MATRIX

		Predicted Class	
		Normal	**Attack**
Actual Class	Normal	TN	FP
	Attack	FN	TP

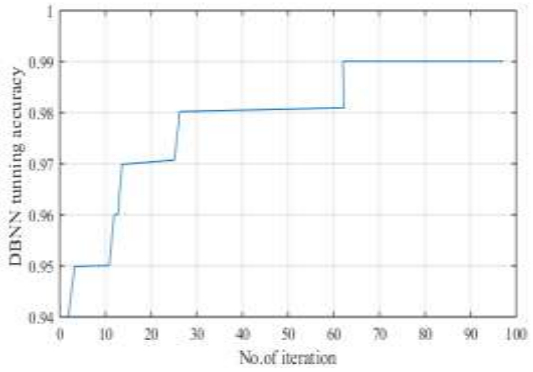

Fig. 4 Convergence curve while tuning

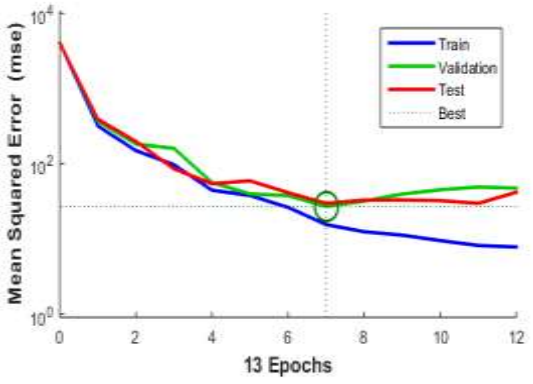

Fig. 5 Mean Square error using CSO-DBNN

Figure 4 illustrates the convergence curve while tuning accuracy of the DBNN by CSO using Dataset 15 Multi classification problems. From the figure it is analyzed that the accuracy curve progressively increases with increase in number of iterations. The curve stabilizes from 63rd iteration and the accuracy stabilizes at about 99%.Figure 5 illustrates the MSE of CSO-DBNN and its Best Validation Performance is 26.9311 at epoch 7.

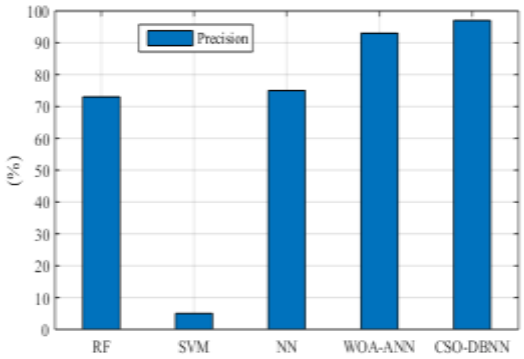

Fig. 6 Precision Comparative analysis

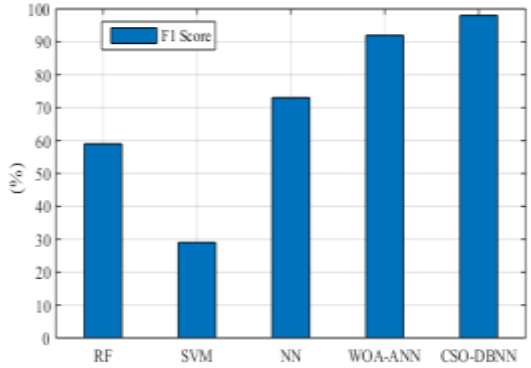

Fig. 7 Recall Comparative analysis

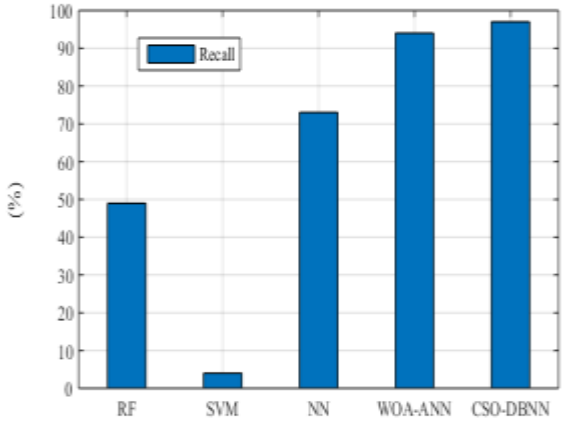

Fig. 8 F1 Score Comparative analysis

Figures 6, 7,8 shows the comparative analysis of Average values of accuracy, precision, recall, and F1 score of the conventional classifiers such as random forest (RF), SVM and NN, WOA-NN and Proposed CSO-DBNN. From the result analysis the figures shows that CSO-DBNN will outperforms the conventional algorithms under study.

V. CONCLUSIONS

A consistent SG power system with cyber infrastructure with IDS should not be dependable and should have the capability to perform efficiently at any kind of suspicious activities. Hence in this paper, the main contribution was to model effective intrusion detection for SG power system by utilizing the classification and optimization algorithms to enhance intrusion detection system performance. The reliability of our proposed CS-DBNN intrusion detection system was measured in terms of accuracy, precision, recall, and F1 score in comparison with the conventional random forest (RF), SVM, NN and WOA-ANN IDS techniques. The experimental outcome depicts the supremacy of the proposed IDS strategy in detecting the attack in the SG power system by preventing the local-optima problem.

REFERENCES

[1] C. h. Rowland, *"Intrusion detection system."* *U.S. Patent 6,405,318*, June 11, 2002.

[2] O. Depren, M. Topallar, E.Anarim, M. K. Ciliz, "*An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks*", *Expert systems with Applications*, Vol.29, No.4, pp.713-722, 2005.

[3] D. Bolzoni, "*Revisiting Anomaly-based Network Intrusion Detection Systems*", University of Twente, Enschede, Netherlands, 2009.

[4] C. A. Catania, and C. G. Garino, "*Automatic network intrusion detection: Current techniques and open issues*." *Computers & Electrical Engineering*, Vol.38, No.5, pp.1062-1072, 2012.

[5] D. P. Vinchurkar, and A. Reshamwala, "*A Review of Intrusion Detection System Using Neural Network and Machine Learning*", *International Journal of Engineering Science and Innovative Technology*, Vol.1, No.2, pp.54-63, 2012.

[6] M. Crosbie, R. Shepley, B. Kuperman, and L.L. Frayman, "*Computer architecture for an intrusion detection system*", *U.S. Patent 7,007,301*, February 28, 2006.

[7] X. Fang, S. Misra, G. Xue, and D. Yang, "*Smart grid—The new and improved power grid: A survey*", *IEEE communications surveys & tutorials*, Vol.14, No.4, pp.944-980, 2011.

[8] P. I. Radoglou-Grammatikis, and P. G. Sarigiannidis, "*Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems*", *IEEE Access* Vol.7, No. 1, pp.46595-46620, 2019.

[9] Q. Schueller, K. Basu, M. Younas, M. Patel, and F. Ball, "*A hierarchical intrusion detection system using support vector machine for SDN network in cloud data center*", In: Proc. of the International Telecommunication Networks and Applications Conference, Sydney, NSW, Australia, pp. 1-6, 2018

[10] D. H. Kang, B. K. Kim, J. T. Oh, T. Y. Nam, and J. S. Jang, "*FPGA based intrusion detection system against unknown and known attacks*", In: Pacific Rim International Workshop on Multi-Agents, Springer, Berlin, Heidelberg, pp. 801-806, 2006

[11] M. De Nadai, and M. van Someren, "*Short-term anomaly detection in gas consumption through arima and artificial neural network forecast,"* In: IEEE Workshop on Environmental, Energy and Structural Monitoring Systems, Trento, Italy, p. 250255, 2015

[12] R. S. Naoum, and Z, N. Al-Sultani, "*Learning vector quantization (LVQ) and k-nearest neighbor for intrusion classification*", World of Computer Science and Information Technology Journal (WCSIT), Vol.2, No.3, pp.105-109, 2012.

[13] G. Zhao, C. Zhang, and L. Zheng, *"Intrusion detection using deep belief network and probabilistic neural network"*, In: Proc. of the International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing, Guangzhou, China, pp. 639-642, 2017

[14] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "*On optimal PMU placement-based defense against data integrity attacks in smart grid*", IEEE Transactions on Information Forensics and Security, Vol.12, No.7, pp. 1735-1750, 2017.

[15] M. Z. Gunduz, and R. C. Das, "*Cyber-security on smart grid: Threats and potential solutions*." Computer Networks, Vol.169, No.8, pp. 107094, 2020.

[16] G. Efstathopoulos, P. R. Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. K. Angelopoulos, and S.K. Athanasopoulos, In: Proc. of the International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, Limassol, Cyprus, Cyprus, pp. 1-6, 2019

[17] S. Binna, S. R. Kuppannagari, D. Engel, and V. K. Prasanna, "*Subset Level Detection of False Data Injection Attacks in Smart Grids*", In: Proc. of the IEEE Conference on Technologies for Sustainability, Long Beach, CA, USA, USA, pp. 1-7, 2018

[18] I. Aljarah, H. Faris, and S. Mirjalili, "*Optimizing connection weights in neural networks using the whale optimization algorithm", Soft Computing*, Vol.22, No.1, pp.1-15, 2018.

[19] E. M. Hassib, A. I. El-Desouky, L. M. Labib, and E. S. El-kenawy, "*WOA+ BRNN: An imbalanced big data classification framework using Whale optimization and deep neural network*", Soft Computing, Vol.24, No.1, pp. 5573–5592, 2020.

[20] B. Genge, P. Haller, C. D. Dumitru, and C. Enăchescu, "*Designing optimal and resilient intrusion detection architectures for smart grids*", IEEE Transactions on Smart Grid, Vol.8, No.5, pp.2440-2451, 2017.

[21] D, Rodrigues, X. S. Yang, and J. P. Papa, "*Fine-tuning deep belief networks using cuckoo search*, *Bio-Inspired Computation and Applications in Image Processing"*, Chapter 3, pp. 47-59, Academic Press, 2016.

[22] S. C. Chu, P. W. Tsai PW, and J.S. Pan, "*Cat swarm optimization*", In: Proc. of Pacific Rim International Conference on Artificial Intelligence, Springer, Berlin, Heidelberg, pp. 854-858, 2006

[23] M. Z. Alom , V. Bontupalli, and T. M. Taha "*Intrusion detection using deep belief networks*", In: Proc. of International Conference on National Aerospace and Electronics, Dayton, OH, USA, pp. 339-344, 2015