IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 February 2024, accepted 16 February 2024, date of publication 20 February 2024, date of current version 11 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3367993

RESEARCH ARTICLE

Optimal Deep Learning Empowered Malicious User Detection for Spectrum Sensing in Cognitive Radio Networks

LATIFAH ALMUQREN[1], MOHAMMED MARAY[2], FAIZ ABDULLAH ALOTAIBI[3], ABDULRAHMAN ALZAHRANI[4], AHMED MAHMUD[5], AND MOHAMMED RIZWANULLAH[6]

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2]Department of Information Systems, College of Computer Science, King Khalid University, Abha, Saudi Arabia
[3]Department of Information Science, College of Humanities and Social Sciences, King Saud University, Riyadh 11437, Saudi Arabia
[4]Department of Computer Science and Engineering, College of Computer Science and Engineering, University of Hafr Al Batin, Hafr Al Batin 31991, Saudi Arabia
[5]Research Center, Future University in Egypt, New Cairo 11835, Egypt
[6]Department of Computer and Self Development, Deanship of Preparatory Year, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding author: Mohammed Rizwanullah (r.mohammed@psau.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 248 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R349), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2024R838), King Saud University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2024/R/1445). This study is partially funded by the Future University in Egypt (FUE).

ABSTRACT Malicious user recognition for spectrum sensing in Cognitive Radio Networks (CRNs) is a serious safety feature to safeguard effective and trustworthy process of these systems. Spectrum sensing permits CRNs to identify and employ accessible spectrum bands. As well as it is available to prospective interference and mischievous actions. To preserve network integrity, recognition of malicious consumers is vital. Deep learning (DL) based malicious consumer classification powers advanced neural network frameworks to recognize and flag possible threats inside a network. By examining numerous amounts of information, DL techniques can distinguish patterns as well as anomalies that are connected with malicious user performance plus system intrusions, scams or irregular action. This technique provides flexibility benefit that permits a network to learn and develop in evolving threats. It also offers an effectual revenue of improving network security in the difficult and active digital landscape. Therefore, this article develops an Optimal Deep Learning Empowered Malicious User Detection for Spectrum Sensing (ODL-MUDSS) in the CRN. The main intention of ODL-MUDSS model focused on automated identification and classification of MUs in CRN. To accomplish this, the ODL-MUDSS model primarily applies deep belief network (DBN) methodology for automated and accurate detection of MUs. In addition, recognition performance of DBN technique can be enhanced by use of sand cat swarm optimization (SCSO) algorithm and thereby improves the detection results. The performance validation of ODL-MUDSS technique is observed under different processes. The comprehensive outcomes stated enhanced performance of ODL-MUDSS model over other existing models with maximum accuracy of 97.75%, precision of 97.75%, recall of 97.75%, and F-score of 97.75%.

INDEX TERMS Cognitive radio networks, communication,spectrum sensing, malicious user detection, deep learning.

The associate editor coordinating the review of this manuscript and approving it for publication was Turgay Celik.

I. INTRODUCTION

Cognitive radio is mainly aimed at effective radio spectrum division employing an extraordinary network in order to recognize and abuse available radio spectrum deprived of intrusions [1]. The refined organization of cognitive radio has been considered as important spectrum-shortage issue in the prospect of wireless communication, where more subscribers rise quickly. In cognitive radio networks (CRNs), hunting a vacant spectrum is executed by employing a spectrum detecting procedure that employs nodes called secondary users (SUs) deprived of authorized licence [2]. To wisdom and verify the work of an elective spectrum utilized by other nodes is called primary users (PUs) with authorized licence. To attain great spectrum detecting acts, distributed and centralized cooperative networks developed a related solution. In initial system, SUs collaborate and part their identifying information with a fusion center (FC) that collects all SUs' sensing notes to grasp an optimum judgment on PUs' spectrum use [3]. In 2nd network, SUs collaborate as well as share sensing data among themselves and create concluding decisions regarding PU spectrum use separately without any interface with FC. Despite of main advantages of cooperative systems, they are liable to latent attacks by malicious users (MUs) that cause unwanted intrusions among SUs and Pus, so decreasing decision exactness of spectrum identifying procedure [4].

Several existing studies assume that secondary consumers constantly tell the truth. But, it is well recognized that wireless networks cooperated below the switch of malicious parties. The secondary user of malicious can send false data and misinform spectrum sensing outcomes to origin crash or ineffective spectrum usage [5]. For instance, few secondary users often report presence of the primary user such that they can conquer spectrum by themselves [6]. Few experimental techniques in CSS will help to lead an optimum global decision [7]. A genetic algorithm (GA) is a class of mathematical techniques driven by growth. This algorithm is effective to find optimum solution by applying enthused techniques to given issues. Machine Learning (ML) is an alternative useful model by learning nearby surroundings [8]. The experiential nature of ML model inspires by utilizing in CRN. Furthermore, these kinds of methods provide good performance in spectrum sensing detection. Deep Learning (DL) is a specified type of ML in the domain of Artificial Intelligence (AI) that relates to deep artificial neural network (ANN) which is also known as deep neural networks (DNNs) [9]. These techniques simulate the procedure of learning by a human brain. The human brain generally comprises cells which are denoted to as neurons in neural systems. At the same time, in a human brain, all cells are linked over axons and dendrites with link areas called as synapses [10]. These links are found in ANN that contain weights to act as influences among nerve cells in the human brain.

This article develops an Optimal Deep Learning Empowered Malicious User Detection for Spectrum Sensing (ODL-MUDSS) in the CRN. The main intention of ODL-MUDSS model focused on automated identification and classification of MUs in CRN. To accomplish this, ODL-MUDSS technique primarily applies deep belief network (DBN) methodology for automated and accurate detection of MUs. In addition, recognition performance of DBN technique can be enhanced by use of sand cat swarm optimization (SCSO) algorithm and thereby improves the detection results. The performance validation of the ODL-MUDSS technique is examined under different measures. In short, the major contributions of the study is listed as follows.

- An intelligent ODL-MUDSS technique comprising of pre-processing, DBN based classification, and SCSO based hyperparameter tuning has been presented. To the best of our knowledge, the ODL-MUDSS model has never presented in the literature.
- Employ DBN model for the identification and classification of MUs in the CRN.
- Hyperparameter optimization of the DBN model using SCSO algorithm using cross-validation helps to boost the predictive outcome of the ODL-MUDSS model for unseen data.

The rest of the paper is organized as follows. Section II provides the related works and section III offers the proposed model. Then, section IV gives the result analysis and section V concludes the paper.

II. LITERATURE REVIEW

In [11], a support vector machine (SVM) learning technique is mainly developed to learn performance of malicious consumers and it categorizes genuine as well as mischievous users. A particle swarm optimization (PSO) model too combined to absorb minimum probable differences malicious consumer's energy report deviance from genuine SUs. The possibility of classification and energy of recognition are used for evaluating influence of developed model. In [12], the author recommended ML-based Adaptive Gaussian Mixture Model (AGMM) for supportive spectrum detecting in cognitive radio systems for design recognition. The author uses secondary consumers energy level in order to form a feature vector in designed technique. The training feature vector for detection is determined through an integration of Gaussian density tasks that attained by employing presented method.

Nie et al. [13] developed a new cluster-based cooperative detecting after-forecast system where a learning and sensing group are together measured for implementing cooperative forecast as well as sensing proficiently. This permits to skipping difficult physical detecting to decrease demands when spectrum accessibility can be just projected utilizing cooperative forecast. Salameh et al. [14] projects a safety-aware routing procedure that reflects jamming attack which interfere with cognitive radio programs. This designed process gives a protected network for every hop inside an IoT basis destination pair to issue of optimization. However, CRNs are more exposed to attacks so an Ensemble-based Jamming Behaviour Detection and Identification (E-JBDI) model is projected as next link of defence.

In [15], Fruit fly optimisation algorithm (FOA) and DBN used. DBN has 4 constraints on training stage such as penalty parameter, weight decay, learning rate and amount of hidden units. These constraints must be correctly chosen for suitable operation of DBN. Modification of these limits occupied into an optimisation problem and it is considered by FOA. Tangsen et al. [16] projects Node Evaluation and Scheduling (NES) and Secure Spectrum Sensing based on Blockchain (SSSB) model that estimates consistency of detecting nodes in actual period and attains faith value of a node. The node's data kept in Blockchain (BC) administration centre. BC converts node data to safeguard because a node resembles to individual trust value deprived of any confusion.

In [17], an enhanced ANN-based aggressor detection technique is developed. The act of ANN upgraded by employing Immune plasma optimization (IPO) model that is stimulated by human immune method for a disease of COVID-19. In [8], BC-based safety improvement as well as spectrum sensing model projected for dealing with spectrum and recognising mischievous user in CRN. Spectrum sensing is a vital need for one that is affected by mischievous consumers in CRN. The mischievous consumer attacks common signal recognition of system and interrupts accurateness of network act. The event of a mischievous consumer in CRN sends wrong sensing data that reduces system performance. BC-based security as well as spectrum sensing succeeded in CRN system that authorizes system performance.

III. THE PROPOSED MODEL

In this study, we focus on design as well as development of ODL-MUDSS in the CRN. The main intention of ODL-MUDSS technique focused on automated identification and classification of MUs in CRN. Fig. 1 demonstrates workflow of ODL-MUDSS methodology. The figure indicates that the proposed model comprises three major processes namely preprocessing, DBN based MUs detection, and SCSO based hyperparameter tuning process.

A. SYSTEM MODEL

In this proposed model, we supposed CRN system through N normal CRN consumers and M malicious CRN consumers. For evaluating global decisions, every CRN users and malicious CRN consumers, primarily conduct local radio spectrum identifying and then report their detection outcomes to equivalent FC [18]. The developed system technique obtains data from AY malicious CRN consumers might be greater energy level i.e.; suggests active status of PU. Also, received data from malicious CRN consumers might have lower energy levels i.e., suggests inactive status of PU. All CRN consumers containing usual and malicious CRN users are transferring their sensing outcomes to corresponding FC over fading as well as non-fading atmospheres. Then, FC splits regular CRN consumers and malicious CRIoT users depending on developed technique. At FC, it creates a strong worldwide decision depending on radio spectrum sensing outcomes of usual CRN consumers only after splitting regular and mischievous CRN users from CRN system.

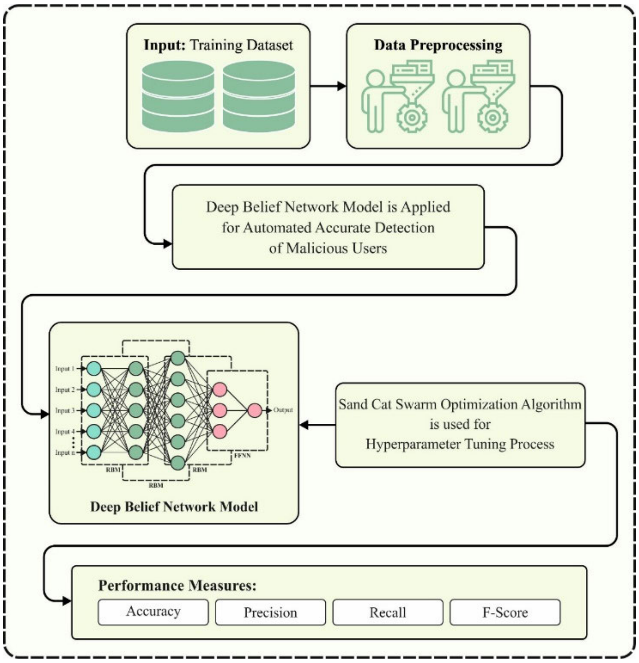
Input: Training Dataset
Data Preprocessing
Deep Belief Network Model is Applied for Automated Accurate Detection of Malicious Users
Input 1
Input 2
Input 3
Input 4
Input n
Output
RBM
RBM
RBM
FFNN
Deep Belief Network Model
Sand Cat Swarm Optimization Algorithm is used for Hyperparameter Tuning Process
Performance Measures:
Accuracy
Precision
Recall
F-Score

FIGURE 1. Workflow of ODL-MUDSS approach.

B. DBN-BASED MU DETECTION MODEL

To accomplish this, the ODL-MUDSS technique applies DBN model for the automated and accurate detection of MUs. DBN overcomes the limitation of backpropagation (BP) via unsupervised learning for generating a layer of feature detector that structures arithmetical model of input information deprived of using any data regarding required output [19]. Then, a high-order feature detector used to grab complex high-level statistical models in input data predicts the label. DBNs are powerful device for DL constructed from RBM. RBM has robust training procedure making it suitable as basic component for DBN. RBM is probabilistic graphical model considered as stochastic neural network that could train distribution prospects over its series of inputs. RBM is one kind of Boltzmann machine, with a constraint that neuron should create a bilateral graph (BG). A BG is a graph whose vertices (V), are split into dual different sets, V_1 (visible unit) and V_2 (hidden unit), and the edge of graph connects V_1 into V_2. Both sets may have symmetrical connectivity between them, and there is no links between nodes within the similar group.

A typical RBM accept binary value for the hidden and visible states. This sort of RBM is called Bernoulli-Bernoulli RBM viz., separate distribution with two potential results labelled by $n = 0$ and $n = 1$. When $n = 1$ it implies that true value takes place with P possibility and If $n = 0$ it implies the wrong case takes place with possibility $q = 1 - p$, whereas $0 < p < 1$.

RBM is an energy-based mechanism, it includes m hidden states and n visible states, the hidden and visible states are v and h vectors are correspondingly. Assume a series of states (v, h), the RBM energy is described below:

$$E\left(v,h\right)=-\sum_{i=1}^{n}a_iv_i-\sum_{j=1}^{m}b_jh_j-\sum_{i=1}^{n}\sum_{j=1}^{m}v_jW_{ij}h_j, \quad (1)$$

In Eq. (1), the state of i^{th} visible state is v_j, and the state of j^{th} hidden state is h_j. W_{ij} is the connection weight of hidden and visible states. Also, there is offsets (bias weight) a_i for the visible unit and b_j for the hidden state.

We can discover joint likelihood distribution of (v, h) for energy function once the parameter is determined as follows:

$$P\left(v,h\right)=\frac{1}{Z}e^{-E(v,h)} \quad (2)$$

$$Z=\sum_{v,h}e^{-E(v,h)}, \quad (3)$$

Here a normalization constant is Z. The activation of hidden state is conditionally independent once the visible state is given. Then, the activation probability of j^{th} hidden state is:

$$P\left(h_j=1\,|\,v\right)=\sigma\left(b_j+\sum_{iv_i}W_{i_j}\right), \quad (4)$$

where a logistics sigmoid activation function is represented as $\sigma(x) = 1/\left(1+e^{(-x)}\right)$. Likewise, activation of visible state is conditionally independent once hidden state, h given and probability of i^{th} noticeable states of v given h is attained as follows:

$$P\left(v_i=1\,|\,h\right)=\sigma\left(a_i+\sum_{jh_j}W_{i_j}\right). \quad (5)$$

The log-log-probability of training dataset is differentiated about W is calculated by the following expression:

$$\frac{\partial logp(v)}{\partial 1W_{i_j}}=\langle v_{ih_j}\rangle_{daia}-\langle v_{ih_j}\rangle_{model}, \quad (6)$$

In Eq. (6), $\langle . \rangle_{data}$ and $\langle . \rangle_{model}$ are predictable values in model or data distribution. The learning rules for system weight in log-probability-based training dataset are attained as follows:

$$\Delta W_{i_j}=\epsilon(\langle v_{ih_j}\rangle_{daia}-\langle v_{ih_j}\rangle_{model}, \quad (7)$$

In Eq. (7), the learning rate is e. Meanwhile, there is no straight connection in the HL of RBM, we can easily obtain an unbiased sample of $\langle v_ih_j\rangle_{daia}$. Unfortunately, it is challenging to calculate unbiased samples of $\langle v_ih_j\rangle_{model}$ meanwhile it needs exponential time. To overcome these problems, a quick training model named Contrastive Divergence (CD) is introduced. When the state is selected for hidden unit, a "reconstruction" is generated by setting v_i to 1 with possibility shown as follows:

$$\Delta W_{i_j}=\epsilon(\langle v_{ih_j}\rangle_{data}-\langle v_ih_j\rangle_{recon}. \quad (8)$$

where average value over reconstruction and input data are $\langle v_ih_j\rangle_{recon}$ and $\langle v_ih_j\rangle_{data}$, it is deliberated as a better approximation to $\langle v_jh_j\rangle_{model}$.

DBN is a NN made up of multiple layers of RBM that form stacked RBM. Thereby, we can learn a high-order representation of input dataset. Hinton et al., newly established a DBN together with unsupervised greedy learning model to construct the network consecutively. ANN with system topology constructed from layer of neuron method but with deep structure and learning mechanics.

In real-time, the DBN training frequently comprises of two stages: (1) finetuning and (2) greedy layer-wise pertaining. Layer-wise relating includes training technique parameter layer-wise through CD algorithm and unsupervised training. Firstly, the training begins with the low-level RBM that receives DBN input and moves slowly in a hierarchy. Lastly, RBM in top layer comprising DBN output is learned. Thus, learned feature or output of prior layer is utilized as an input of succeeding RBM layer.

As a final step, in finetuning, the network is trained in a supervised way after the training of RBM using BP model to "finetune" the weight. This greedy learning problem-solving method of DBN is rapid as well as effective. It includes generating optimum superior at every layer in stacked RBM, which finds a global optimal value.

C. HYPERPARAMETER TUNING USING SCSO MODEL

Eventually, classification performance of DBN method can be enhanced by the use of SCSO algorithm. SCSO is a new and effective swarm optimization approach based on the hunting behaviors of sand cat herd that has tremendous strength to dig for prey and could identify lower frequencies lower than 2 KHz [20]. Global search and attack prey are two foraging behavior of sand cats in SCSO. The Bi-GRU hyperparameter is considered as the prey. At the initialization phase, the population was randomly initialized which increases issue of unequal distribution that affects quality of optimum solution. Singer mapping is adopted to an early populace of sand cat enables to attain regular distribution probability, which increases possibility of attaining optimum expression as follows:

$$z_{k+1}=\mu\left(7.86z_k-23.31z_k^2+28.75z_k^3-13.302875z_k^4\right) \quad (9)$$

In Eq. (9), control parameter within *the* [0, 1] interval is z_k. If $\mu\in$ [0.9, 1.08], then Singer mapping has chaotic behavior.

The prey-exploration formula is defined below:

$$\vec{X}\left(t+1\right)=\vec{r}\left(\vec{X}_b\left(t\right)-rand\left(0,1\right)\cdot\vec{X}_c\left(t\right)\right) \quad (10)$$

$$\vec{r}=\vec{r_G}\times rand\left(0,1\right) \quad (11)$$

$$\vec{r_G}=s_M-\left(\frac{s_M\times iter_c}{iter_{\max}}\right) \quad (12)$$

Here the location vector search agent is $\vec{X}$, amount of iterations for existing iteration is represented as t, the optimum location of a candidate is $\vec{X}_b$, the existing location of search agent is $\vec{X}_c$, the sensitivity range of sand cat to lower frequency noise is $\vec{r}$, range of sensitivity that linearly dropped from 2 to 0 is $\vec{r}_G$, existing iteration is $iter_c$, and greatest amount of iterations is $iter_{max}$.

The reduction factor $\vec{r}_G$ in SCSO linearly decreased, which causes them to slowly converge in later iteration and thereby descent into local optima. For these reasons, a messy reduction factor is proposed to prevent potential solutions from getting trapped in local optima:

$$\begin{cases} \vec{r}_G = s_M - s_M\left(\frac{iter_c}{iter_{max}}\right)^{0.25} + |h_i|\left(\frac{iter_c}{iter_{max}}\right)^{0.25} \\ \qquad - \left(\frac{iter_c}{iter_{max}}\right)^{0.25} \\ h_i = 1-2(h_{i-1})^2, \quad h_{i-1} \in [0,1] \end{cases} \tag{13}$$

Furthermore, a sand cat can sense frequency lower than $2\ kHz$, S_M take the value of 2. The sand cat attacks the prey, and the prey attack strategy for population is shown as follows:

$$\vec{X}_{\text{rnd}} = \left|rand\ (0, 1) \cdot \vec{X}_{\text{b}}\ (t) - \vec{X}_{\text{c}}\ (t)\right| \tag{14}$$

$$\vec{X}\ (t+1) = \vec{X}_{\text{b}}\ (t) - \vec{r} \cdot \vec{X}_{rnd} \cdot cos\ (\theta) \tag{15}$$

Now a random angle between 0 and 360 is represented as θ, and a random location produced from the optimum and the existing location is $\vec{X}_{rnd}$. All the members of population are capable of moving in a circumferential direction Using this method. Every sand cat selects a random angle. The sand cat can prevent local optima as it gets closer towards the prey location. SCSO is used to balance the exploitation and exploration stages by an adaptive factor, $\vec{R}R = 2 \times \vec{r}_G \times rand(0, 1) - \vec{r}_G$, which is the total search stage if I $c > 1$ and attack stage if I $|R| < 1$.

The adaptive t-distribution is proposed for mutating adaptive t-distribution for existing optimum global solutions and upgrading optimum solution to improve populace diversity at later iterations and enhance global search ability. The t-distribution probability density function is shown below:

$$P_t\ (x) = \frac{\Gamma\left(\frac{n+1}{2}\right)}{\sqrt{n\pi}\,\Gamma\left(\frac{n}{2}\right)}\left(1+\frac{x^2}{n}\right)^{-\frac{n+1}{2}}, \quad -\infty < x < +\infty \tag{16}$$

In Eq. (16), the degree of freedom is n. At the initial iteration, the t-distribution tends to be Cauchy distribution that improves population range and increases the global search capability due to the comparably small amount of iterations. At the later iteration, the t-distribution tends to be Gaussian distribution, which is helpful to search a smaller range and improves the local convergence capability due to the amount of iterations being comparatively large. The adaptive parameter ω is introduced to improve populace diversity at an initial iteration and enhance local exploitation capability at a later iteration:

$$\omega = \left(1 - \frac{t-1}{T-1}\right) \times \frac{T-t}{T} \tag{17}$$

In the equation, ω the adaptive parameter is comparatively larger at the initial iteration which implies t-distribution can be used to improve populace diversity. Fig. 2 illustrates the steps involved in SCSO. In a later iteration, ω adaptive parameter is slowly decreased to minimize the impact of t-distribution on the individual position for retaining the optimal individual. The variation probability is set to 0.5 and when the randomly generated value [0, 1] is lesser than the variation probability perform the t-distribution change strategy as follows:

$$X_i^t = X_i + X_i \times \omega \times t\ (t) \tag{18}$$

In Eq. (18), the location of i^{th} individuals after the update of t-distribution is $X_i^t \cdot$ the t-distribution with a degree of freedom t is $t(t)$ and the existing amount of iterations is t.

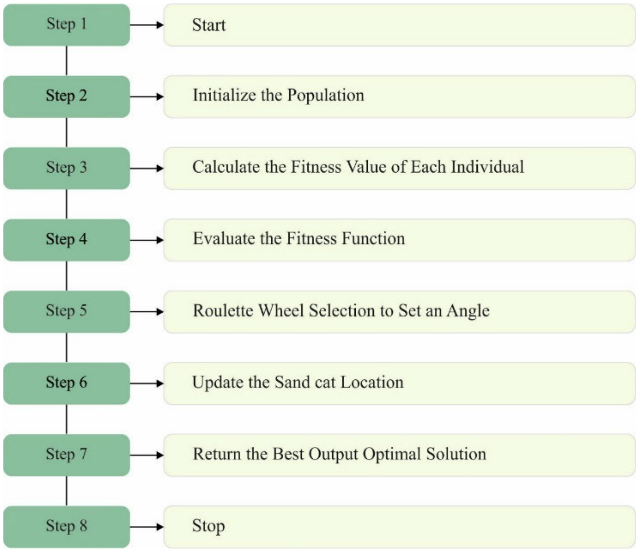
Step 1
Start
Step 2
Initialize the Population
Step 3
Calculate the Fitness Value of Each Individual
Step 4
Evaluate the Fitness Function
Step 5
Roulette Wheel Selection to Set an Angle
Step 6
Update the Sand cat Location
Step 7
Return the Best Output Optimal Solution
Step 8
Stop

FIGURE 2. Steps involved in SCSO algorithm.

The fitness selection is a significant factor influencing performance of SCSO technique. The hyperparameter selection procedure involves solution encoding model to calculate efficiency of candidate solution. In this research, SCSO model reflects accuracy as main principle for designing fitness functions that is expressed below.

$$Fitness = \max\ (P) \tag{19}$$

$$P = \frac{TP}{TP + FP} \tag{20}$$

From the above equation, TP represents true positive and FP denotes false positive value.

IV. RESULTS AND DISCUSSION

The MU detection outcomes of ODL-MUDSS technique can be investigated employing a dataset comprising 4000 samples. The dataset includes two classes as represented in Table 1.

Fig. 3 exhibits confusion matrices created by ODL-MUDSS model under 80:20 and 70:30 of TRPH/TSPH.

TABLE 1. Details on database.

Class	No. of Samples
Normal	2000
Malicious Users	2000
Total Samples	4000

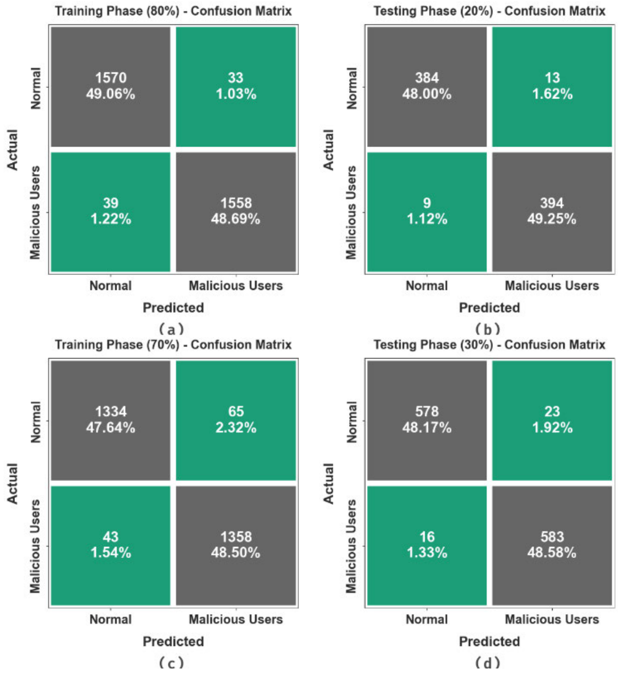

FIGURE 3. Confusion matrices of (a-c) TRPH of 80% and 70% and (b-d) TSPH of 20% and 30%.

TABLE 2. MU detection outcome of ODL-MUDSS algorithm with 80:20 of TRPH/TSPH.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
TRPH (80%)				
Normal	97.94	97.58	97.94	97.76
Malicious Users	97.56	97.93	97.56	97.74
Average	97.75	97.75	97.75	97.75
TSPH (20%)				
Normal	96.73	97.71	96.73	97.22
Malicious Users	97.77	96.81	97.77	97.28
Average	97.25	97.26	97.25	97.25

The effects designate effectual classification of normal and malicious user's samples below all classes.

The MU detection results of the ODL-MUDSS technique on 80:20 of TRPH/TSPH is reported in Table 2 and Fig. 4.

The experimental values highlighted that ODL-MUDSS methodology properly recognized the normal and MU samples. On 80% of TRPH, the ODL-MUDSS model provides average $accu_y$ of 97.75%, $prec_n$ of 97.75%, $reca_l$ of 97.75%, and F_{score} of 97.75%. Besides, on 20% of TSPH, ODL-MUDSS model offers average $accu_y$ of 97.25%, $prec_n$ of 97.26%, $reca_l$ of 97.25%, and F_{score} of 97.25%.

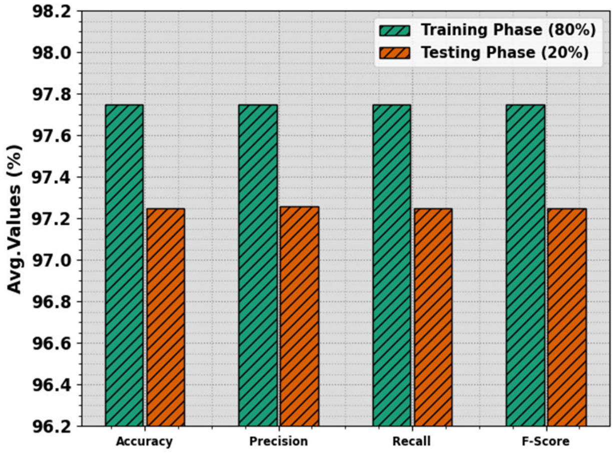

FIGURE 4. Average of ODL-MUDSS algorithm with 80:20 of TRPH/TSPH.

TABLE 3. MU detection outcome of ODL-MUDSS algorithm with 70:30 of TRPH/TSPH.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
TRPH (70%)				
Normal	95.35	96.88	95.35	96.11
Malicious Users	96.93	95.43	96.93	96.18
Average	96.14	96.15	96.14	96.14
TSPH (30%)				
Normal	96.17	97.31	96.17	96.74
Malicious Users	97.33	96.20	97.33	96.76
Average	96.75	96.76	96.75	96.75

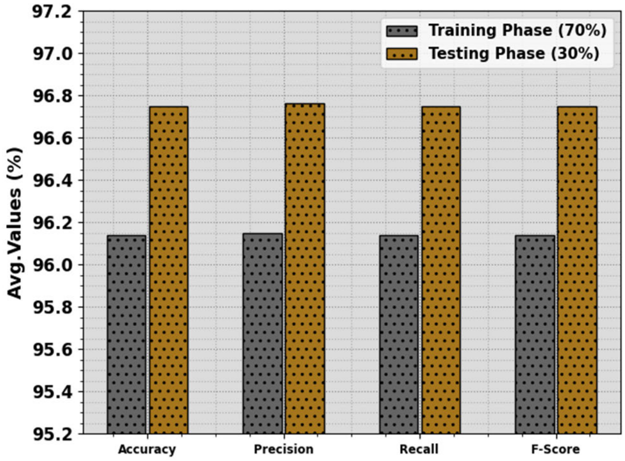

FIGURE 5. Average of ODL-MUDSS algorithm with 70:30 of TRPH/TSPH.

The MU detection outcomes of ODL-MUDSS model on 70:30 of TRPH/TSPH is described in Table 3 and Fig. 5. The experimental values highlighted that ODL-MUDSS approach correctly known normal and MU samples. On 70% of TRPH, ODL-MUDSS method offers average $accu_y$ of 96.14%, $prec_n$ of 96.15%, $reca_l$ of 96.14%, and F_{score} of 96.14%. Also, on 30% of TSPH, ODL-MUDSS method affords average $accu_y$ of 96.75%, $prec_n$ of 96.76%, $reca_l$ of 96.75%, and F_{score} of 96.75%.

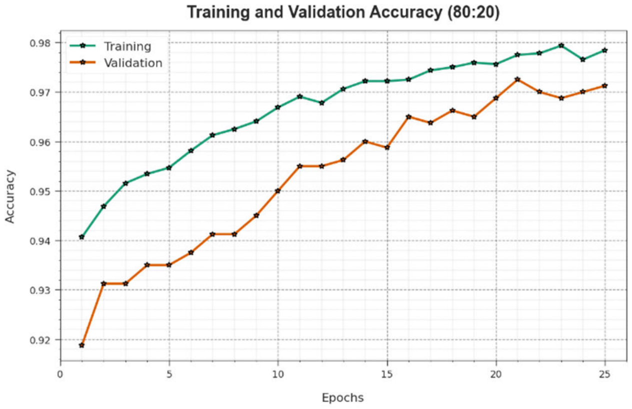

FIGURE 6. $Accu_y$ **curve of ODL-MUDSS algorithm with 80:20 of TRPH/TSPH.**

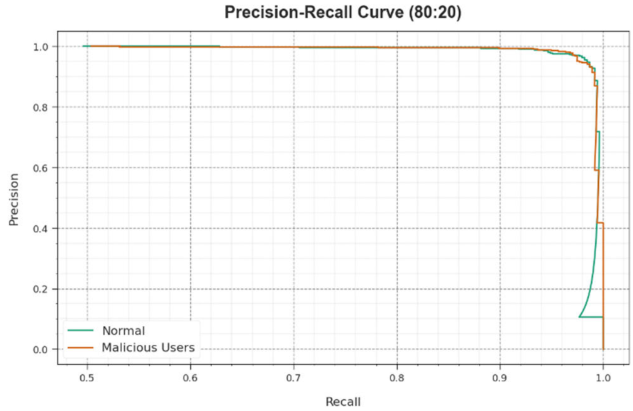

FIGURE 8. **PR curve of ODL-MUDSS algorithm with 80:20 of TRPH/TSPH.**

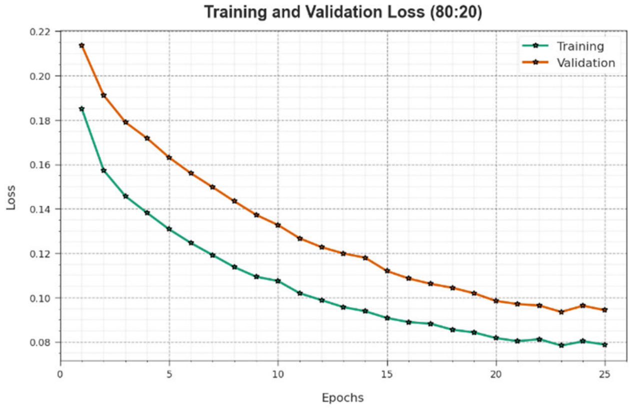

FIGURE 7. **Loss curve of ODL-MUDSS algorithm with 80:20 of TRPH/TSPH.**

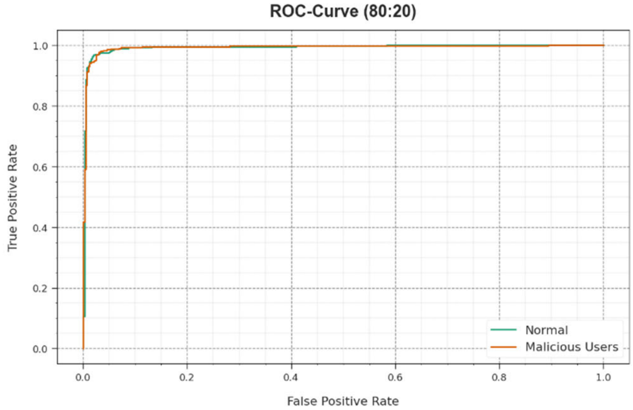

FIGURE 9. **ROC curve of ODL-MUDSS algorithm with 80:20 of TRPH/TSPH.**

To calculate efficiency of ODL-MUDSS technique with 80:20 of TRPH/TSPH, we have created accuracy curves for both TRPH and TSPH, as illustrated in Fig. 6. These curves provide valuable insights into the model's learning progress and its ability to generalize. As we increase the number of epochs, a noticeable improvement in TR and TS accuracy curves becomes evident. This improvement indicates model's capacity to better identify patterns within both TR and TS datasets.

Fig. 7 also offers an outline of ODL-MUDSS approach with 80:20 of TRPH/TSPH, the model's loss values throughout TR process. The decreasing trend in TR loss over epochs indicates that model continually refines its weights to minimize prediction errors on both TR and TS data. This loss curve reflects how well the model fits training data. Particularly, TR and TS loss consistently decrease, representing the model's effective learning of patterns present in both datasets. Moreover, it shows model's adaptation in diminishing discrepancies between predictions and original TR labels.

The precision-recall curve of ODL-MUDSS approach with 80:20 of TRPH/TSPH, we plots precision against recall revealing that our model achieves higher precision-recall values across all classes, as defined in Fig. 8. This graph illustrates the model's ability to recognize various class labels, particularly excelling in correctly identifying positive samples while minimizing false positives.

Fig. 9 also includes ROC curves of ODL-MUDSS technique with 80:20 of TRPH/TSPH, which showcase the model's ability to discriminate between class labels. These curves provide valuable insights into the trade-off among true positive rate (TPR) and false positive rate (FPR) across dissimilar classification thresholds and epochs. They highlight the model's accurate predictive performance across various classes, further emphasizing its classification capabilities.

In Table 4 and Fig. 10, the overall classification performance of ODL-MUDSS technique with recent models are given [21]. The results indicate that the SVM model offers poor performance whereas the LR, NB, and stacking techniques attain slightly boosted outcomes. However, ODL-MUDSS model offers maximum performance with $accu_y$ of 97.75%, $prec_n$ of 97.75%, $reca_l$ of 97.75%, and F_{score} of 97.75%.

The comparative computation time (CT) results of ODL-MUDSS methodology with current approaches are given in Table 5 and Fig. 11. The outcomes demonstrate that ODL-MUDSS method gains better performance with minimal CT of 2.63min. On the other hand, the SVM, LR, NB, and stacking models offer increased CT values. Thus,

TABLE 4. Comparative outcome of ODL-MUDSS algorithm with recent systems.

Models	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
SVM Model	70.00	66.00	75.00	91.42
LR Algorithm	93.00	87.00	96.90	90.76
NB Model	94.00	89.00	96.98	95.60
Stacking Model	97.00	96.00	97.00	93.53
ODL-MUDSS	97.75	97.75	97.75	97.75

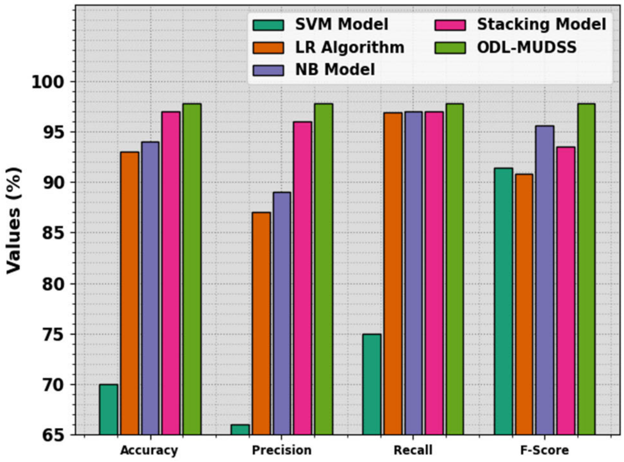

FIGURE 10. Comparative outcome of ODL-MUDSS algorithm with recent systems.

TABLE 5. CT outcome of ODL-MUDSS algorithm with recent systems.

Models	Computational Time (min)
SVM Model	10.42
LR Algorithm	9.62
NB Model	6.20
Stacking Model	7.08
ODL-MUDSS	2.63

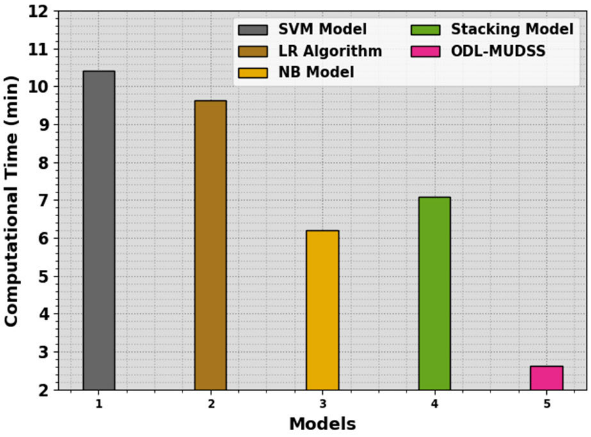

FIGURE 11. CT outcome of ODL-MUDSS algorithm with recent systems.

TABLE 6. AR and IR outcome of ODL-MUDSS algorithm with other methods under varying malicious users.

(%) Percentage of MUs	SVC Model	Logistic Regression	Naïve Bayes	Stacking Model	ODL-MUDSS
Authentication Rate (%)					
10	71.30	95.41	97.79	96.49	99.23
20	73.03	95.92	98.29	97.14	99.08
30	74.61	96.57	98.44	97.43	99.37
40	76.41	97.14	98.72	98.22	99.52
50	77.92	97.57	98.65	98.36	99.44
Intrusion Rate					
10	0.090	0.048	0.100	0.027	0.135
20	0.096	0.064	0.129	0.038	0.147
30	0.102	0.083	0.155	0.046	0.173
40	0.146	0.101	0.164	0.051	0.192
50	0.192	0.119	0.175	0.056	0.198

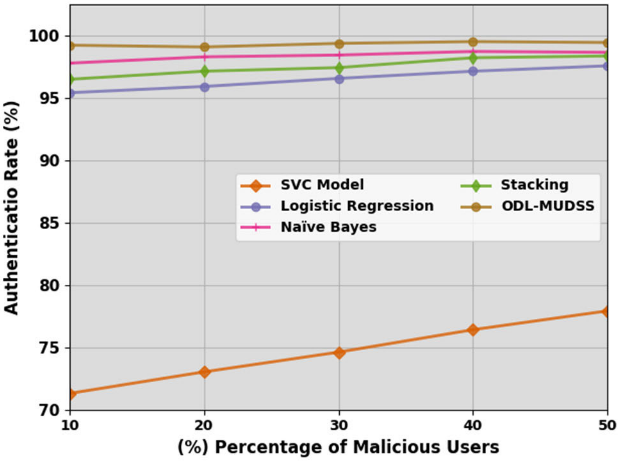

FIGURE 12. AR outcome of ODL-MUDSS approach under varying MUs.

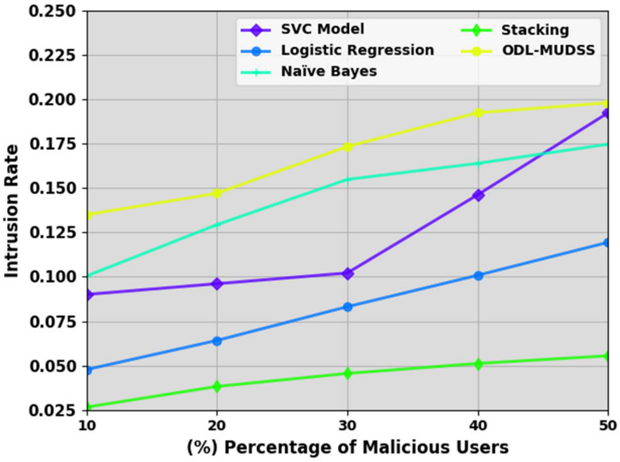

FIGURE 13. IR outcome of ODL-MUDSS approach under varying Mus.

the ODL-MUDSS technique can be employed for automated MU detection process.

Table 6 illustrates comparative outcome of ODL-MUDSS technique with other approaches under varying malicious users in terms of authentication rate (AR) and intrusion rate (IR). Fig. 12 demonstrates the AR outcome of ODL-MUDSS algorithm with recent systems under varying malicious users (MUs). The outcomes stated that the ODL-MUDSS algorithm has gain optimum performances. On 10% of MUs, the ODL-MUDSS algorithm has obtains higher AR of 99.23%, while the SVM, LR, NB, and stacking models offer lesser AR values of 71.30%, 95.41%, 97.79%, and 96.49%, respectively. In addition, on 50% of MUs, ODL-MUDSS techniques has attains greater AR of 99.44%, while SVM, LR, NB, and stacking method provide smaller AR values of 77.92%, 97.57%, 98.65%, and 98.36%, correspondingly.

Fig. 13 exhibits IR result of ODL-MUDSS technique with current systems under varying MUs. The outcomes stated that ODL-MUDSS model has gain optimum performances. On 10% of MUs, ODL-MUDSS method has attains greater IR of 0.135, while SVM, LR, NB, and stacking techniques provide lesser IR values of 0.090, 0.048, 0.100, and 0.027, separately. Moreover, on 50% of MUs, ODL-MUDSS methodology obtains higher IR of 0.198, while SVM, LR, NB, and stacking models offer lesser IR values of 0.192, 0.119, 0.175, and 0.056, correspondingly. Thus, the proposed model can be employed for automated MU detection performance

V. CONCLUSION

In this article, we focus on designs and development of ODL-MUDSS in the CRN. The main intention of the ODL-MUDSS model focused on the automated identification and classification of MUs in CRN. To accomplish this, ODL-MUDSS model primarily applies DBN model for the automated and accurate detection of MUs. In addition, recognize performance of DBN technique can be enhanced by use of SCSO algorithm thereby improving the detection results. The performance validation of ODL-MUDSS approach is studied under different measures. The comprehensive outcomes stated greater performance of ODL-MUDSS approaches over other current methods in terms of distinct metrics. Future work can focus on the design of hybrid metaheuristics and ensemble voting classifier model for enhanced MU detection performance on the CRN.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 248 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R349), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2024R838), King Saud University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2024/R/1445). This study is partially funded by the Future University in Egypt (FUE).

REFERENCES

[1] T. Nawaz and A. Alzahrani, "Machine-learning-assisted cyclostationary spectral analysis for joint signal classification and jammer detection at the physical layer of cognitive radio," *Sensors*, vol. 23, no. 16, p. 7144, Aug. 2023.

[2] M. K. Giri and S. Majumder, "Extreme learning machine based identification of malicious users for secure cooperative spectrum sensing in cognitive radio networks," *Wireless Pers. Commun.*, vol. 130, no. 3, pp. 1993–2012, Jun. 2023.

[3] A. Upadhye, P. Saravanan, S. S. Chandra, and S. Gurugopinath, "A survey on machine learning algorithms for applications in cognitive radio networks," in *Proc. IEEE Int. Conf. Electron., Comput. Commun. Technol. (CONECCT)*, Jul. 2021, pp. 01–06.

[4] S. K. Ram, "Energy-efficient adaptive sensing for cognitive radio sensor network in the presence of primary user emulation attack," *Comput. Electr. Eng.*, vol. 106, Mar. 2023, Art. no. 108619.

[5] H. Jiang, Z. Yu, and J. Yang, "Research on key technology of full duplex cognitive radio network," in *Proc. J. Phys., Conf.*, May 2021, vol. 1920, no. 1, Art. no. 012035.

[6] A. Jain, N. Gupta, and M. Sreenu, "Blockchain based smart contract for cooperative spectrum sensing in cognitive radio networks for sustainable beyond 5G wireless communication," *Green Technol. Sustainability*, vol. 1, no. 2, May 2023, Art. no. 100019.

[7] S. K. Agrawal, A. Samant, and S. K. Yadav, "Spectrum sensing in cognitive radio networks and metacognition for dynamic spectrum sharing between radar and communication system: A review," *Phys. Commun.*, vol. 52, Jun. 2022, Art. no. 101673.

[8] A. Khanna, P. Rani, T. H. Sheikh, D. Gupta, V. Kansal, and J. J. P. C. Rodrigues, "Blockchain-based security enhancement and spectrum sensing in cognitive radio network," *Wireless Pers. Commun.*, vol. 127, no. 3, pp. 1899–1921, Dec. 2022.

[9] M. Arkwazee, M. Ilyas, and A. Dawood Jasim, "Automatic spectrum sensing techniques using support vector machine in cognitive radio network," in *Proc. 2nd Int. Conf. Adv. Electr., Comput., Commun. Sustain. Technol. (ICAECT)*, Apr. 2022, pp. 1–6.

[10] A. Shirolkar and S. V. Sankpal, "Deep learning based performance of cooperative sensing in cognitive radio network," in *Proc. 2nd Global Conf. for Advancement Technol. (GCAT)*, Oct. 2021, pp. 1–4.

[11] K. Arshid, Z. Jianbiao, I. Hussain, G. G. Lema, M. Yaqub, and R. Munir, "Support vector machine approach of malicious user identification in cognitive radio networks," *Wireless Netw.*, 2022.

[12] S. Samala, S. Mishra, and S. S. Singh, "Cooperative spectrum sensing in cognitive radio networks via an adaptive Gaussian mixture model based on machine learning," *J. Commun.*, vol. 17, no. 10, pp. 1–8, 2022.

[13] D. Nie, W. Yu, Q. Ni, H. Pervaiz, and G. Min, "Cluster control and energy consumption minimization for cooperative prediction based spectrum sensing in cognitive radio networks," *IEEE Trans. Commun.*, vol. 71, no. 9, pp. 5580–5594, Sep. 2023.

[14] H. B. Salameh, S. Otoum, M. Aloqaily, R. Derbas, I. Al Ridhawi, and Y. Jararweh, "Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks," *Ad Hoc Netw.*, vol. 98, Mar. 2020, Art. no. 102035.

[15] S. R. Sonti and M. S. G. Prasad, "Deep belief network with FOA-based cooperative spectrum sensing in cognitive radio network," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 27, no. 3, pp. 323–347, 2021.

[16] H. Tangsen, X. Li, and X. Ying, "A blockchain-based node selection algorithm in cognitive wireless networks," *IEEE Access*, vol. 8, pp. 207156–207166, 2020.

[17] V. P. Ajay and M. Nesasudha, "Detection of attackers in cognitive radio network using optimized neural networks," *Intell. Automat. Soft Comput.*, vol. 34, no. 1, 2022.

[18] M. S. Hossain and M. S. Miah, "Machine learning-based malicious user detection for reliable cooperative radio spectrum sensing in cognitive radio-Internet of Things," *Mach. Learn. Appl.*, vol. 5, Sep. 2021, Art. no. 100052.

[19] W. Almanaseer, M. Alshraideh, and O. Alkadi, "A deep belief network classification approach for automatic diacritization of Arabic text," *Appl. Sci.*, vol. 11, no. 11, p. 5228, 2021.

[20] H. Fu and T. Lei, "ISCSO-PTCN-BIGRU prediction model for fracture risk grade of gas-containing coal fracture," *Processes*, vol. 11, no. 10, p. 2925, 2023.

[21] S. Benazzouza, M. Ridouani, F. Salahdine, and A. Hayar, "A novel prediction model for malicious users detection and spectrum sensing based on stacking and deep learning," *Sensors*, vol. 22, no. 17, p. 6477, 2022.