Vol.67: e24231114, 2024
https://doi.org/10.1590/1678-4324-2024231114
ISSN 1678-4324 Online Edition

BABT
Brazilian Archives of Biology and Technology

Article - Engineering, Technology and Techniques

Enhancing Intrusion Detection Using Binary Arithmetic Optimization with Sparse Auto Encoder for Fog-Assisted Wireless Sensor Networks

Thiruppathi Muthu[1]
https://orcid.org/0000-0001-9880-539X

Vinoth Kumar Kalimuthu[1*]
https://orcid.org/0000-0002-8920-4936

Balakrishnan Srinivasan[1]
https://orcid.org/0000-0002-3836-2926

Rajakani Velumani[2]
https://orcid.org/0009-0006-4767-0329

[1]Vivekanandha College of Engineering for Women, Department of ECE, Tiruchengode, India; [2]Anjalai Ammal Mahalingam Engineering College, Department of ECE, Thiruvarur, India.

Editor-in-Chief: Alexandre Rasi Aoki
Associate Editor: Fabio Alessandro Guerra

Received: 10-Nov-2023; Accepted: 26-Feb-2024.

*Correspondence: vinodkumaran87@gmail.com; (V.K.K.).

HIGHLIGHTS

- Intrusion Detection using BAOA-SAE technique for Fog Assisted WSN
- Broad range of simulated outcome was performed on benchmark IDS dataset.
- Binary variants of AOA to be suitable for the FS tasks.

Abstract: Intrusion detection in Fog-Assisted Wireless Sensor Networks (Fog-WSNs) is a critical security measure designed to protect the functionality and integrity of these networks. Fog computing extends the abilities of traditional WSNs by introducing edge devices or fog nodes that can process data and provide computational resources. Intrusion detection in Fog-WSNs is vital to maintain the privacy and security of data generated and transmitted by sensors and processed at the fog node. Machine learning (ML) algorithms are widely employed to detect intrusion. These models can be trained on historical data to detect known attack patterns and can adapt to emerging threats. By implementing effective intrusion detection mechanisms, these networks can alleviate risks and ensure the reliable operation of critical applications in different fields namely IoT, smart cities, and industrial automation. This study designs an Intrusion Detection using Binary Arithmetic Optimization with Sparse Auto encoder (BAOA-SAE) technique for Fog Assisted WSN. The major aim of BAOA-SAE method is to recognize and classify the presence of the intrusions in the network. Primarily, the BAOA-SAE method focuses on the election of prominent features in the network data. Next, the SAE model is implemented to categorize the presence of intrusions. To improve the intrusion rate, the BAOA-SAE technique employs bacterial foraging optimization algorithm (BFOA). A broad range of

simulated outcomes were performed on benchmark IDS dataset. The extensive outcomes highlighted the high efficiency of the BAOA-SAE method over other existing techniques.

Keywords: Fog computing; Wireless sensor networks; Machine learning; Intrusion detection; Feature selection.

INTRODUCTION

Due to the huge popularity of wireless IoT devices, the amount of connections and development of mobile computing is growing rapidly [1]. Therefore, the problems of response time and consumption of energy are said to be very critical [2]. For addressing and suggesting good solutions, a fog-assisted system has been developed in order to achieve difficult delay-sensitive following-generation services like one needed by (resource-limited) wireless mechanisms for example; surveillance video cameras, sensors, and mobile phones for evaluating physical variables such as humidity, temperature, pressure and much more) [3]. Allowing this solution, the fog nodes are placed close to where data are created in order to permit more capable computing, networking functions, and storage for resource-limited IoT tools. So that, the discharging of delay-sensitive tasks and also resource-consuming from end IoT devices to a near fog computing node can be proficiently executed [4]. In this paper, a single-cell fog-assisted system is measured where the base station (BS) is prepared with one fog node to aid a quantity of IoT devices [5].

In present scenario, the security of wireless sensor networks (WSN) has become a main anxiety. How to classify numerous system threats is a key point which needs to be cracked [6]. The research of security WSN mainly attention to the following parts such as network routing and security of data fusion; encryption models, key management, and authentication skills; numerous network attack techniques and defense plans [7]; and finally network intrusion detection networks and response methods. The studies of WSN security can be separated into passive as well as active defense [8]. When comparing with the development of passive defense for WSN, there are some studies on active defense. However, passive defense is an extent that is taken in response to the attack's features after the threats have happened. And this is not adequate for the security of WSN [9]. Therefore, it is vital to study active defense tools for detecting mischievous intrusions before attacks happen [10]. In active defense equipment, intrusion detection will perform animportant part in safeguarding the security of WSNs.

This study designs an Intrusion Detection using Binary Arithmetic Optimization with Sparse Auto encoder (BAOA-SAE) technique for Fog Assisted WSN. The main objective of BAOA-SAE method is to recognize and classify the intrusion’s existence in the network. Primarily, the BAOA-SAE algorithm focuses on the election of prominent features in the network data. Next, the SAE system is implemented to categorize the presence of intrusions. To improve the intrusion rate, the BAOA-SAE technique employs bacterial foraging optimization algorithm (BFOA). A wide range of simulations was performed on benchmark IDS dataset.

RELATED WORK

Muthu and Kalimuthu [11] aimed to develop a seagull optimizer-based FS method with optimal ELM (SGOFS-OELM) for resolving intrusion detection in fog-based WSNs. This proposed SGOFS-OELM approach was developed to achieve this objective by devising the SGOFS technique to select the best potential feature subsets. The ELM classification method has been implemented for intrusion detection. Lastly, the political optimizer (PO) could be employed to perform automatic parameter fine-tuning of the ELM algorithm that finally results in improved classification effectiveness. In [12], a fog computing-based smart agricultural architecture was presented, which employs UAVs for collecting information atIoT sensors used in agriculture as well as it offloads in fog locations implemented at the network edge. This architecture accepts the notion of a charging token, at which point accomplishing a trip, UAVs attain tokens from the fog nodes. Subsequently, this tokenis used for charging the UAVs for their following trips.

Alzubi and coauthors [13] introduced an Effective Seeker Optimizer model with an ML-enabled IDS (ESOML-IDS) technique for the EC and FC framework. This introduced method develops arecent ESO-based FS methodology for choosing an optimum feature subset for identifying the intrusion event in the FC and EC platforms. Also, the authors implemented a comprehensive learning PSO (CLPSO) with De-noising-AE (DAE) for identifying intrusions. Wei and coauthors [14] projected a K-nearest neighbour (K-NN)-based IDS and developed a protected network model. This method trains IDS employing a feature database to make a standard profile. The IDS exploits the standard profile to execute real-world identification of network traffic data for attaining faster identification by interconnecting numerous devices in the WSNs.

Reddy and coauthors [15] proposed a security mechanism and guarantee candid function of IoT networks with IDS. A network-IDS (NIDS) was developed depending on the perception of the Exact Greedy Boosting ensemble approach for device operation in the fog nodes owing to protective crucial structure from accurate and earlier identification of malicious actions. Pan and coauthors [16] implemented a lightweight IDS for WSNs. Incorporating sine cosine algorithm (SCA) and KNN could be considerably enhanced the classification accurateness and extremely decreased the false alarm rate (FAR) hence, identifying various attacks comprising unknown attacks. To control the system's complexity, the compact mechanism has been employed to SCA (CSCA) for maintaining the computational space and time, and the polymorphic mutation (PM) approach could be utilized to balance for decreasing the optimization accuracy.

THE PROPOSED MODEL

In this work, new designs and implementation of the BAOA-SAE system for Fog-Assisted WSN.The major aim of the BAOA-SAE method is to recognize and classify the intrusion's existence in the network. It involved three major processes namely BA OA-based FS, SAE-based classification, and BFOA-enabled parameter tuning. Figure 1 denotes the workflow of BAOA-SAE model.

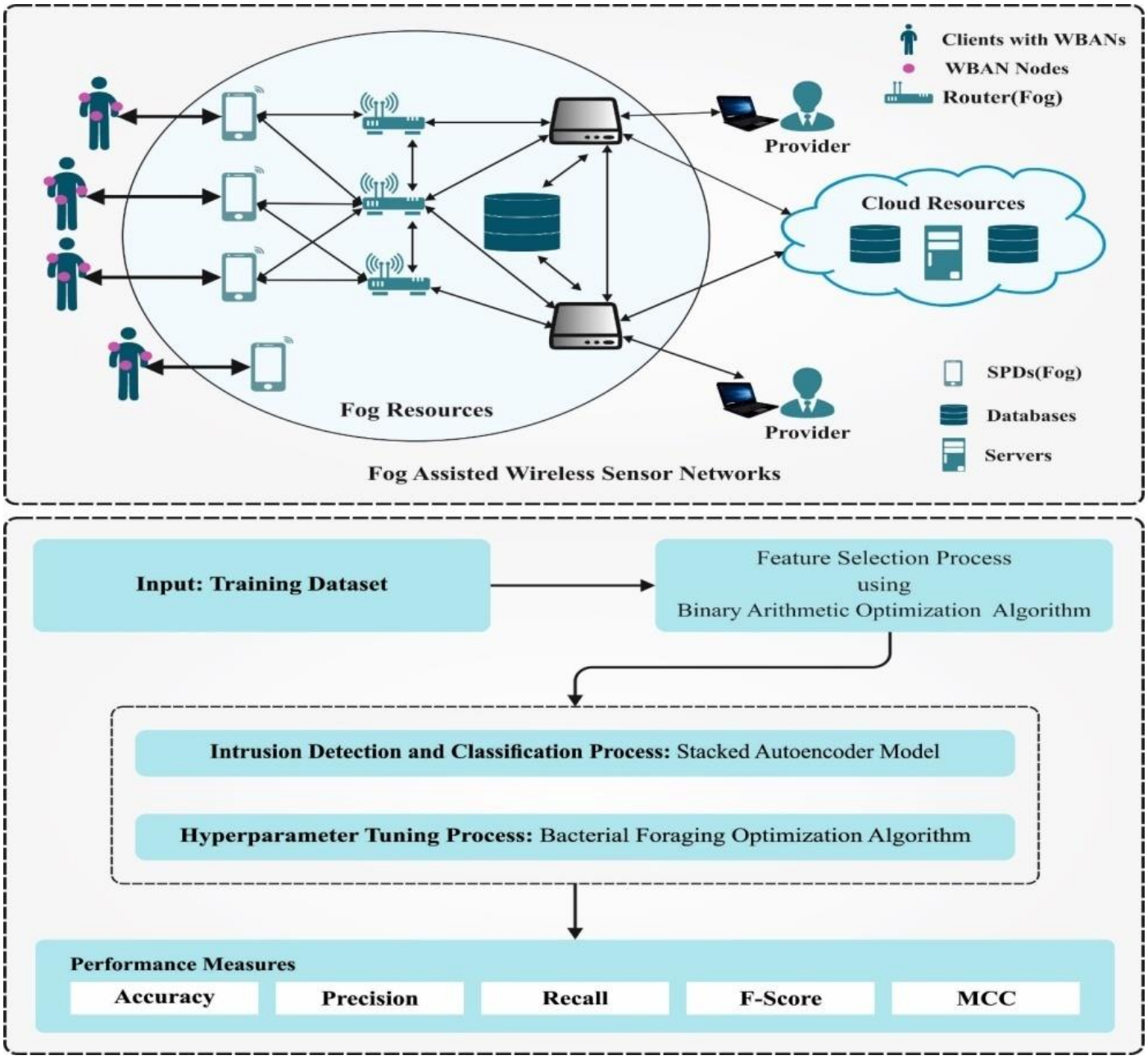


Figure 1. Workflow of BAOA-SAE algorithm

Feature selection using AOA model

Primarily, the BAOA-SAE technique focuses on the election of prominent features in the network data. Naturally, Feature selection (FS) is a binary (Discrete) problem. Therefore, to address these challenges, the original AOA was introduced [17]. The study presents the binary variants of AOA to be suitable for the FS tasks. In the original AOA, candidate continuously explores the search range because the position vector has continuous real values. This can be appropriate for candidate to work with binary data, as given below:

$$B_1\left(x_{i,j}(t+1)\right)=\begin{cases}1 & \text{if sigmoid otherwise } \left(x_{i,j}(t+1)\right)\geq \text{rand}_i\\ 0 & \text{otherwise}\end{cases} \quad (1)$$

In Eq. (1), the original exploration stage is $x_{i,j}(t+1)$, an updated binary location of exploration stage at t^{th} iterationsare$B_1\left(x_{i,j}(t+1)\right)$, a $rand$ is a randomly generated value from the uniform distribution ∈ [1,0], and sigmoid (x). Binary transfer function is used to convert the continuous search space to binary. A few of input values can be mathematically converted into output in the range of [0,1] using the sigmoid function. For machine learning and neural networks, the S curve creates it proper activation function. The output is nearer 1 then input hastremendously positive and 0refers to input is highly negative. Due to these characteristics, the sigmoid function can be suitable for processes such as binary classifiers, where we predict the possibility of event occurring or not. It can be mathematically modelled as follows:

$$\text{sigmoid }(x)=\frac{1}{1+e^{-10(x-0.5)}} \quad (2)$$

Likewise, the updating location of exploitation stage in Eq. (4) is modified as:

$$B_2\left(x_{i,j}(t+1)\right)=\begin{cases}1 & \text{if sigmoid otherwise } \left(x_{i,j}(t+1)\right)\geq \text{rand}\\ 0 & \text{otherwise}\end{cases} \quad (3)$$

In Eq. (3), the original exploitation stage is represented by $x_{i,j}(t+1)$ in Eq. (4) and a modified binary location of exploitation stage at t^{th}iterations are$B_2\left(x_{i,j}(t+1)\right)$, a uniformly distributed random number ∈ [1, 0] is $rand$, and sigmoid (x) is evaluated as in Eq. (2).

In this study, the solution representation is given in vector with 1D. The vector length denotes the number of features. These values of 0 and 1 binary vectors are given in the following: if the value is 1: then the feature is selected and vice versa otherwise not. The FS problem is a bi-objective complexity with a 2 objectives, one has to attain the least number of possible features, and next can be to enhance accurateness of the classification. The FF is utilized to consider both goals, whereas the SAE is used:

$$\text{fitness}=\alpha\rho_R(Y)+\beta\frac{|K|}{|N|} \quad (4)$$

In Eq. (4), the error rate of SAE classifier is$\rho_R(Y)$, $\alpha=[0,1]$ and $\beta=(1-\alpha)$ they are original amount of features is $|N|$, parameters and the amount of selected features is $|K|$.

Next, the SAE model is applied to categorize the presence of intrusions. SAE can learn features automatically from the unlabelled dataset and when compared to original data, gives a better characterization [18]. In real-time, the feature found by SAE replaces the original data, which commonly results in improved performance.

The SAE is a NN which contains output, hidden, and input layers, trained to regenerate its inputs. Usually, the AE obtains a vector input, which encodes latent layer, and decodes into regeneration y. For example, when training data is $\{x_1, x_2, x_3, \ldots x_n\}$, and input x_i is encoded first into a hidden representation $h(x_i)$ based on (5), later hidden representation $h(x_i)$ is decoded into reconstruction $y(x_i)$ based on (6).

$$h(x)=g_h(W_{sh}*x+b_{sh}) \quad (5)$$

$$y(x)=g_o(W_{so}*h(x)+b_{so}) \quad (6)$$

Here the activation of hidden and output layers are $g_h(\cdot)$ and $g_o(\cdot)$ correspondingly; the encoding and decoding matrices are W_{sh} and W_{so} and the encoded and decoded bias vectors are b_{sh} and b_{so} correspondingly. The squared loss function $L(x,y)$is used for measuring the reconstructed error. We can attain the model parameter represented as θ by minimalizing the difference between the reconstruction y and the input x, as follows:

$$\theta=\arg\min_{\theta} L(x,y)= \arg\min_{\theta} 2\sum_{i=1}^{n}\|x_i-y(x_i)\|^2 \quad (7)$$

The AE with multiple hidden units than input could yield suitable representation once it is trained by using SGD model. But if the latent layer is larger than the input layer or the same size, then AE can learn identity function and becomes useless. By constraining the encoder through other restrictions namely sparsity constraint, the current practice specifies that the abovementioned problem can be prevented. The hidden unit is limited by sparseness. For the sigmoid activation function, if the output of neuron is 1 then it is considered active, otherwise inactive if 0. The sparseness implies the maximum neurons of latent layer can be inactive. To accomplish such an average activation of neuron shave been closer to ρ and ρrepresents a sparsity parameter, a smaller value closer to $0(\rho = 0.05$. The average activation $\hat{\rho}_j$ of the j^{th} hidden neuronsare evaluated by:

$$\hat{\rho}_j=\frac{1}{l}\sum_{i=1}^{l}[h_j(x_i)] \quad (8)$$

$$\hat{\rho}=\rho \quad (9)$$

Where x_i represents the input, the scale of the trained dataset is$l$, and $h_j(\cdot)$ indicates the function to evaluate the activation. Figure 2 demonstrates the architecture of SAE.

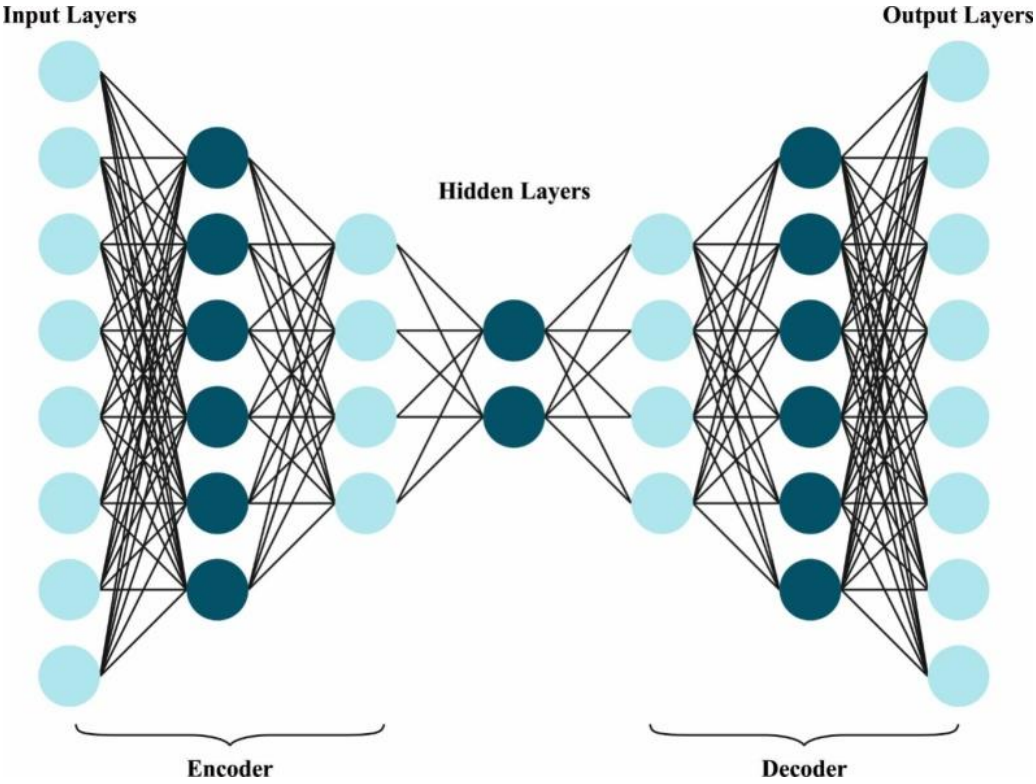


Figure 2. SAE architecture

A penalty term could bein cluded into cost function for achieving the sparseness constraint. This will penalize these conditions where $\hat{\rho}_j$ and ρ are considerably diverse such that the average activation of the hidden neurons could be retained in a smaller value. Based on the KL divergence, the penalty term has been more commonly used as follows:

$$\sum_{j=1}^{m} KL\left(\rho \,\middle\|\, \hat{\rho}_j\right)=\sum_{j=1}^{m}\rho\log\frac{\rho}{\hat{\rho}_j}+(1-\rho)\log\frac{1-\rho}{1-\hat{\rho}_j} \quad (10)$$

From Eq. (10), the number of latent neurons is m.

The BP model performs the AE, and cost function (reconstructed error in sparsity restriction) can be given below

$$L_S(x,y)=L(x,y)+\alpha \sum_{j=1}^{m} KL\left(\rho \left\| \hat{\rho}_j \right.\right) \quad (11)$$

Where the weight of sparsity term isα.

Parameter tuning using BFOA algorithm

To improve the intrusion rate, the BAOA-SAE technique employs BFOA method. E. coli (Escherichia coli) bacteria is based on the chemotactic and foraging behaviors. Through smooth flow and tumbling, the bacteria could be moved in both directions from the toxic region to the nutritional region [19]. The four mechanisms of BFOA are chemotaxis, reproduction, elution-dispersal, and swimming.

During the chemotactic step, if the bacterium determines a novel point where the nutritional medium is high when compared to the existing location, then bacteria move one step forward in that direction. This procedure is reiterated until the worst nutrient is obtained. Based on the nutrient content they picked up at chemotaxis, the bacteria are organized for descending sequence at the reproduction stage. Every bacteria gaps into two, sufficient nutrition reproducing and slowly passing out, its existence in the population has removed but, retaining the original population. As the environment changes, the behaviour and population of bacteria also change; a dispersal and elimination phase is used. Every individual bacteria provided a random integer within [0,1]. If the random value is smaller than predefined parameter value, then it survives; or else, it is eliminated. The BFOA equation and the fitness function are given below.

$$[\theta]^i[j+1,k,l]=[\theta]^j[j,k,l]+c[i]\frac{\Delta[i]}{\sqrt{\Delta^i[i].\Delta[i]}} \quad (12)$$

In Eq. (12), $\theta^i[j,k,l]$ is the chemotactic stage j, reproduction step k, and elimination step i. This leads to step of size $c[i]$ in the bacterium, and vector at the random direction whose element lies from the interval $[-1,1]$ is Δ:

$$J_{CC}\left[\theta,P[j,k,l]\right]=\sum_{i=1}^{S} J_{CC}\left[\theta,\theta^i[j,k,l]\right] \quad (13)$$

In Eq. (13),$J_{cc}\left[,P[j,k,l]\right]$ is the objective function value that needs to be additionof the real objective function for obtaining time-varying objective function, the overall amount of bacteria is S, and the number of parameters is p.

$$\theta=\left[\theta_1,\theta_2,\theta_3\ldots\theta_p\right] \quad (14)$$

$$J[i,j,k,l]=J[i,j,k,l]+J_{cc}\left[\theta^j[i,k,l],P[j,k,l]\right] \quad (15)$$

$$\text{Fitness}=\frac{1}{1+\sum_{t=1}^{24}[\left[\text{PLoad 1[t]-Objective[t]}\right]^2]} \quad (16)$$

The aforementioned FF is selected for the BFOA to accomplish a last load curve like the desired load curve.

The fitness selection is a considerable factor influencing the performance of the MBES approach. The hyperparameter selection process involves the solution encoding approach to evaluate the efficacy of the candidate solutions. In this work, the MBES algorithm considers accuracy as the major criterion to design the fitness function, which can be formulated as follows.

$$\text{Fitness} = \max(P) \quad (17)$$

$$P=\frac{TP}{TP+FP} \quad (18)$$

Where$TP$and $FP$are the true and false positive values

RESULT ANALYSIS

At this section, the performance validation of the BAOA-SAE system is tested with the KDDCup99 database [20]. It includes 125973 instances and a 2 classes.

Table 1 represents the comparative FS analysis of the BAOA-FS model. The obtained values highlighted that the BAOA-FS model offers optimal best cost (BC) of 0.000854. On the other hand, the TLBO-FS, GA-FS, BGOA-S, BGOA-V, and BGOA models have reported increased BC values.

Table 1. Feature selection analysis of BAOA-FS system

Methods	Best Cost	Selected Features
BAOA-FS	0.000854	3,6,7,9,10,12,14,16,18,19,21,23,27,28,30,31,33
TLBO-FS	0.001108	2,4,5,6,8,9,11,13,14,16,18,19,22,24,25,29,30,32,37,39,40
GA-FS	0.001150	21,7,27,32,25,34,1,2,35,3,24,40,28,26,10,5,33,14,16,12,36,23,30,38,22,15,37,9
BGOA-S	0.004176	3,5,8,13,18,20,21,22,30,32,33,34,36,38,40,2,7,19,23,35,27,29
BGOA-V	0.006763	21,27,32,25,34,1,35,3,24,40,28,26,10,5,33,14,16,12,36,23,30,38,22,15,37,9
BGOA	0.006530	23,34,35,36,23,29,21,37,2,1,6,7,9,11,15,19,20,22,27,39,40,3,5

Figure 3 represents the classifier analysis of the BAOA-SAE system with test database. Figures. 3a-3b illustrates the confusion matrices given by the BAOA-SAE system with 70:30 of TRPhase / TSPhase. The outcome indicated that the BAOA-SAE approach is properly recognized and classified in all four classes. Additionally, Figure 3c shows the PR performance of the BAOA-SAE methodology. This simulation value represents that the BAOA-SAE system achieves excellent PR performance with each class. Besides, Figure 3d represents the ROC analysis of the BAOA-SAE methodology. The simulation value shows that the BAOA-SAE method leads to effectual results with greater ROC values for diverse classes.

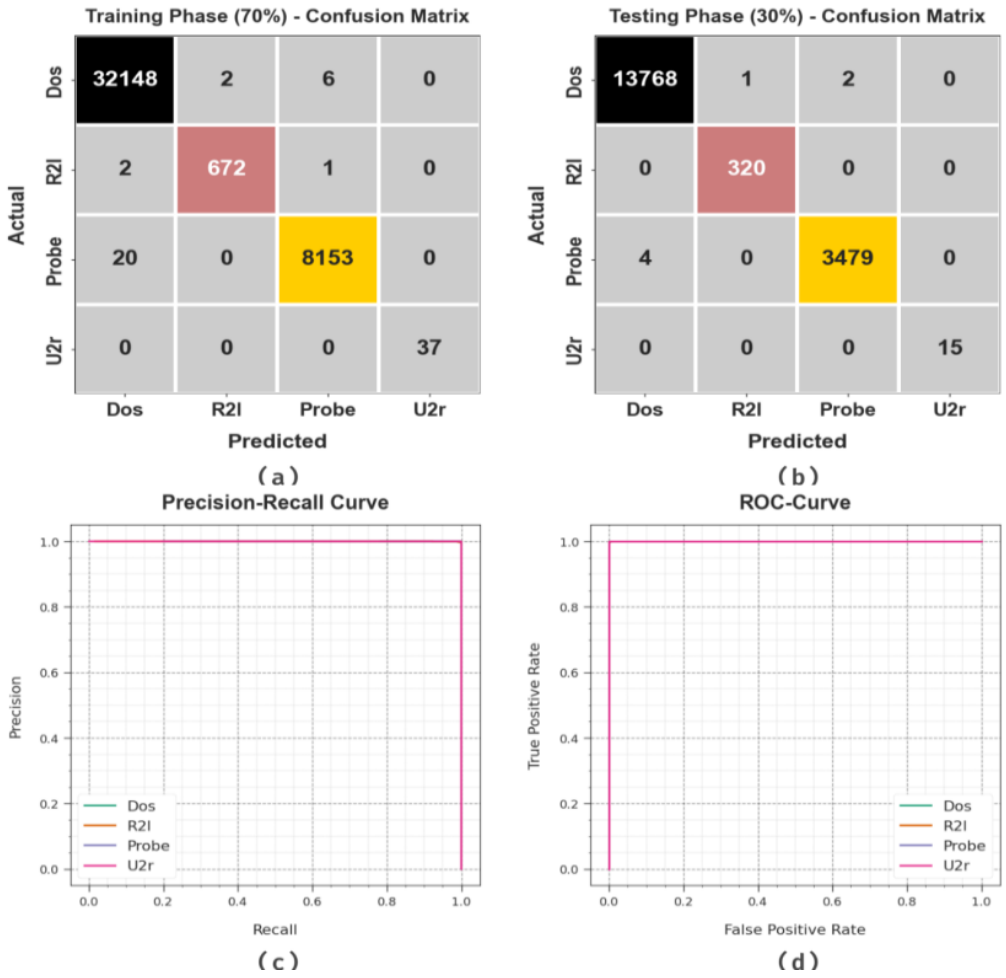


Figure 3. Classifier performance of (a-b) Confusion matrices, (c) PR curve, and (d) ROC

Table 2 and Figure 4 represent the intrusion recognition outcomes of the BAOA-SAE technique. The simulated valuesindicate the effectual ability of the BAOA-SAE method on the intrusion classification process. With 70% of TR Phase, the BAOA-SAE technique offers average $accu_y$, $prec_n$, $reca_l$, F_{score}, and *MCC* of 99.96%, 99.89%, 99.82%, 99.85%, and 99.80% respectively. Also, based on 30% of TS phase, the BAOA-SAE methodology provides average $accu_y$, $prec_n$, $reca_l$, F_{score}, and *MCC*of 99.98%, 99.90%, 99.97%, 99.93%, and 99.90% respectively.

Table 2. Intrusion recognition outcome of BAOA-SAE systemwith 70:30 of TR phase/TS phase

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	*MCC*
		TR Phase (70%)			
Dos	99.93	99.93	99.98	99.95	99.78
R2l	99.99	99.70	99.56	99.63	99.62
Probe	99.93	99.91	99.76	99.83	99.79
U2r	100.00	100.00	100.00	100.00	100.00
Average	99.96	99.89	99.82	99.85	99.80
		TS Phase (30%)			
Dos	99.96	99.97	99.98	99.97	99.88
R2l	99.99	99.69	100.00	99.84	99.84
Probe	99.97	99.94	99.89	99.91	99.89
U2r	100.00	100.00	100.00	100.00	100.00
Average	99.98	99.90	99.97	99.93	99.90

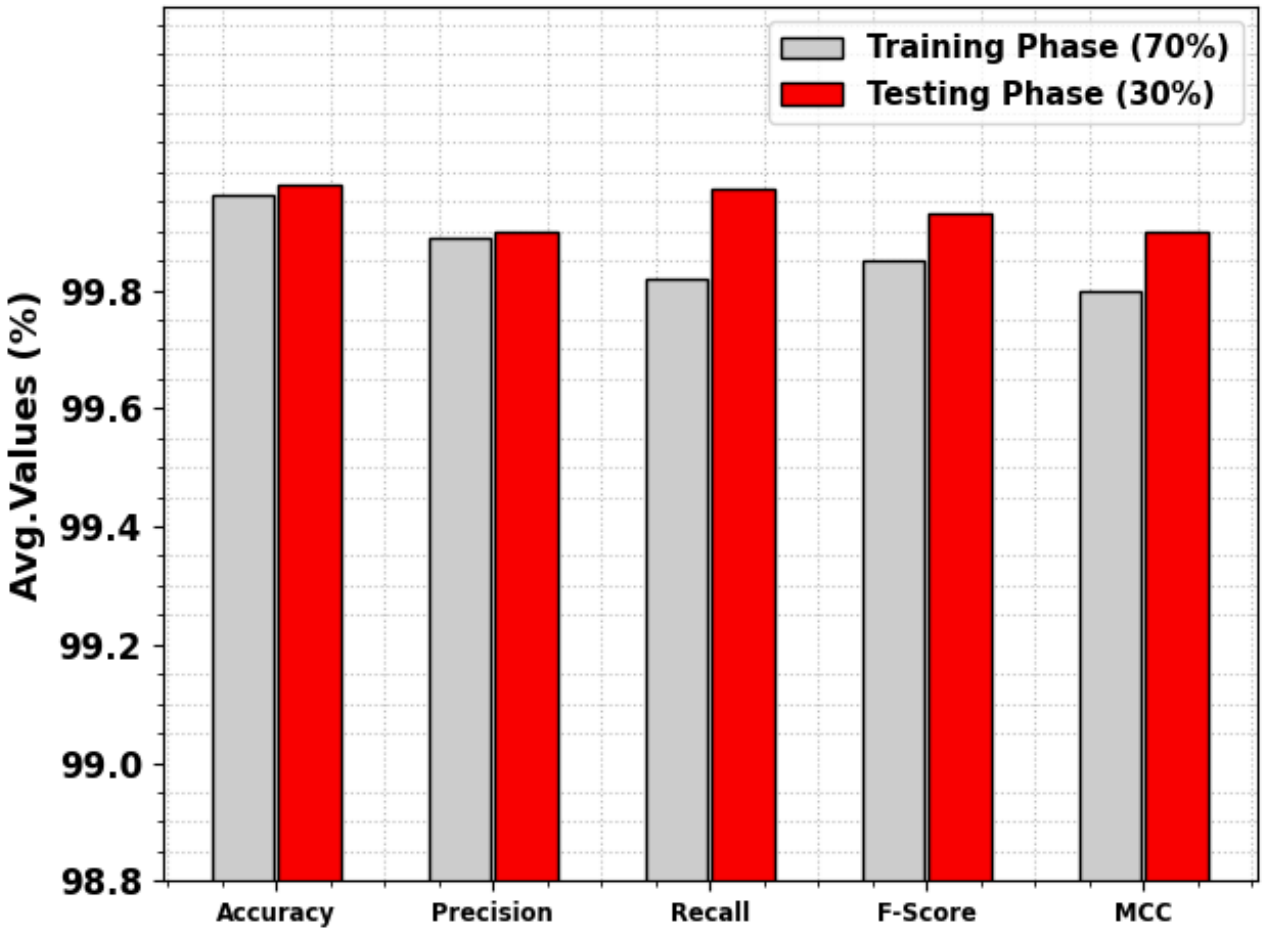


Figure 4. Average of BAOA-SAE technique on 70:30 of TR phase/TS phase

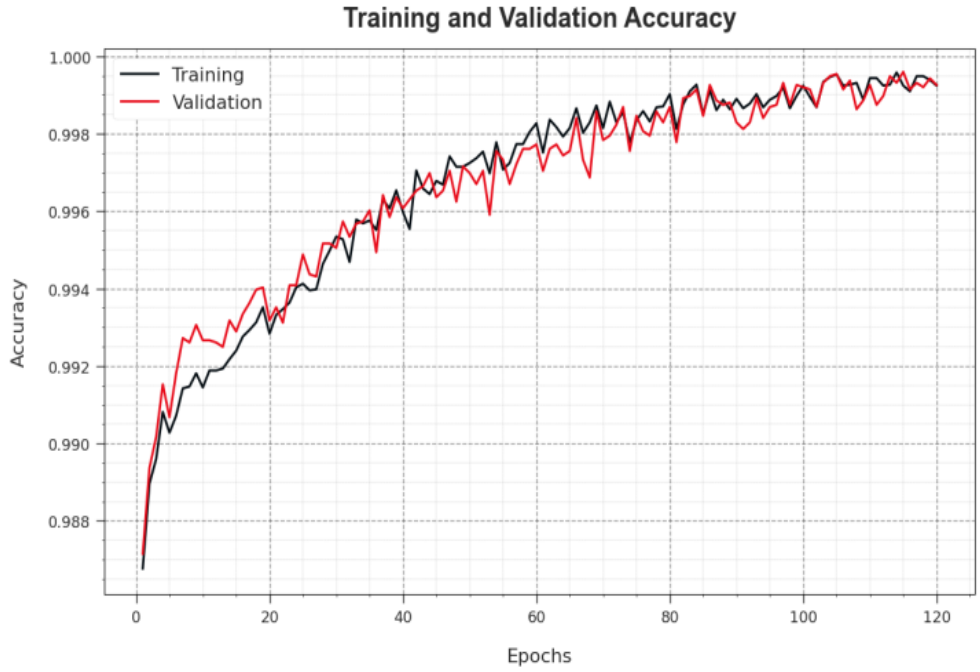


Figure 5. $\mathbf{Accu_y}$curve of the BAOA-SAE technique

To evaluate the effectiveness of the BAOA-SAE method, we have produced accuracy curves for both the training (TR) and testing (TS) phases, as exhibited in Figure 5. These curves deliver valuable insights into the learning development and capability of model to generalize. As we raise the count of epochs, an obvious enlargement in both TR and TS accuracy curves becomes apparent. This improvement shows the model's capacity to effectively recognize patterns in both the TR and TS databases.

Figure 6 also exhibited an overview of BAOA-SAE method loss values across the training progression. The minimizing trend in TR loss over epochs specifies that the model continuously enhances its weights to reduce predicted errors with both TR and TS data. This loss curve considers how much the model fits the training datasets. Remarkably, the TR and TS loss steadily reduced, representing the model's efficient learning of patterns existing in both databases. Besides, it illustrates the model's adaptation in diminishing differences between predicted and actual training labels.

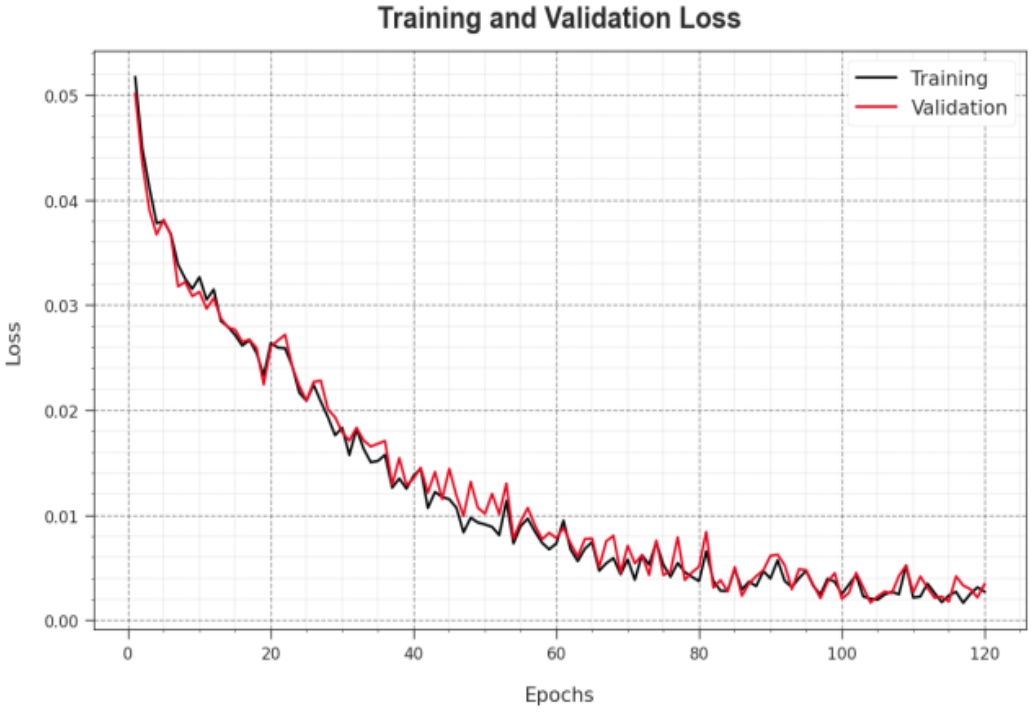


Figure 6. Loss curveof the BAOA-SAE technique

The comparative results of the BAOA-SAE method with recent models are achieved in Table 3 and Figure 7 [21-26]. The outcome values inferred that the BAOA-SAE system accomplishes higher $accu_y$ of 99.98%. At the same time, the DBN, MLIDS, CS-PSO, PSO-SVM, behaviour-IDS, COA-IDS, and DNN+SVM models have reported reduced $accu_y$ values. These simulated outcomes confirmed the excellent performance of the BAOA-SAE algorithms over other models.

Table 3. $\mathrm{Accu_y}$ outcome ofBAOA-SAE methodwith other approaches

Methods	Accuracy
BAOA-SAE	99.98
DBN Technique	99.96
MLIDS Algorithm	99.93
CS-PSO	75.51
PSO-SVM	99.1
Behaviour-IDS	98.89
COA-IDS	96.88
DNN+SVM	92.03

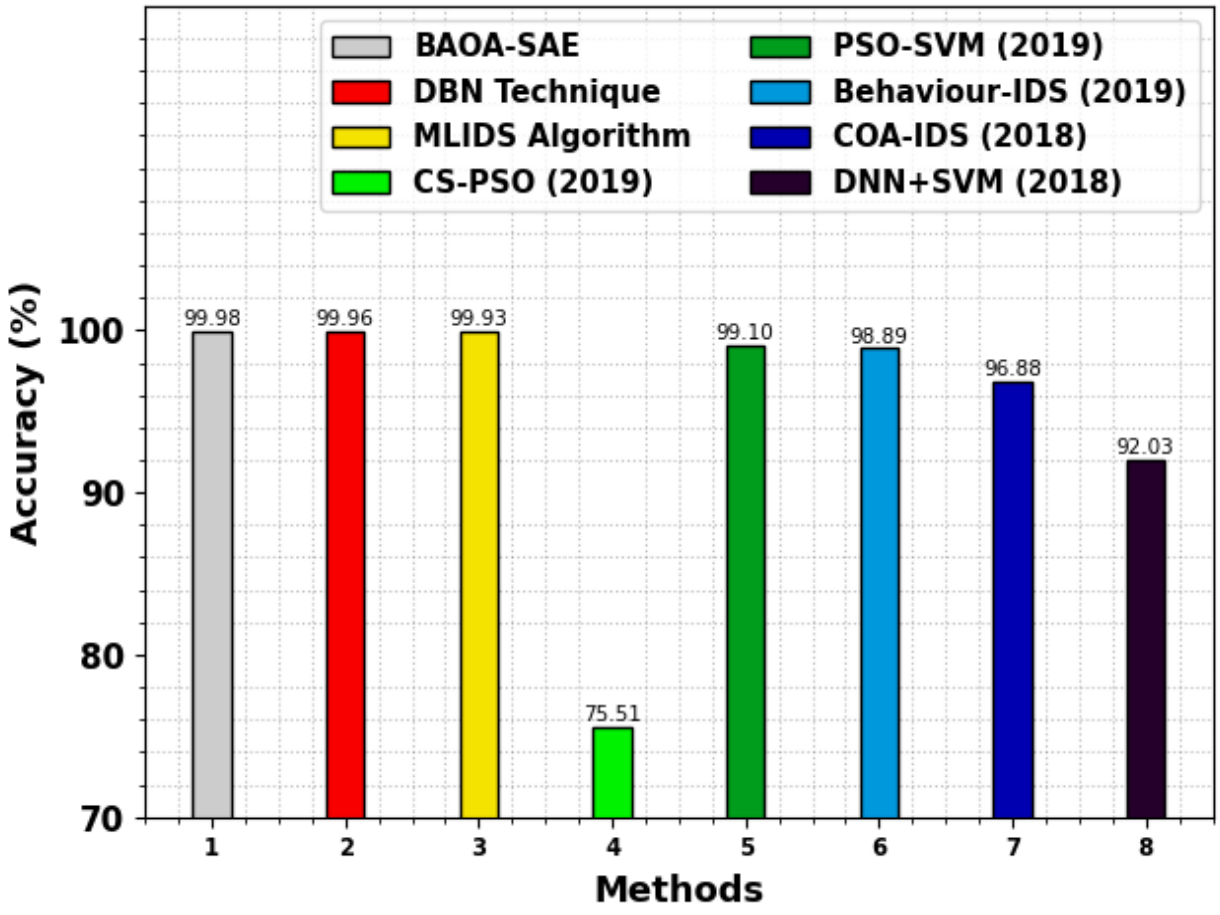


Figure 7. $Accu_y$outcome ofBAOA-SAE method with other approaches

CONCLUSION

This study designs a BAOA-SAE technique for fog-assisted WSNs. The main objective of BAOA-SAE method is to recognize and classify the intrusion's existence in the network. Primarily, the BAOA-SAE algorithm focuses on the election of prominent features in the network data. Next, the SAE algorithm is implemented to categorize the existence of intrusions. To improve the intrusion rate, the BAOA-SAE technique employs BFOA method. A broad range of simulated outcome was performed on benchmark IDS dataset. The extensive outcomes highlighted the high efficiency of the BAOA-SAE method over other existing approaches. Therefore, the proposed model can be employed for accurate and automated intrusion detection and classification process. In future, the outlier detection process can be used for enhancing intrusion detection performance.

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

REFERENCES

1. Ramkumar MP, Daniya T, Paul PM, Rajakumar S. Intrusion detection using optimized ensemble classification in fog computing paradigm. Knowl Based Syst. 2022;252(2):109364. doi:10.1016/j.knosys.2022.109364.
2. Souza CA, Westphall CB, Machado RB, Loffi L, Westphall CM, Geronimo GA. Intrusion detection and prevention in fog based IoT environments: A systematic literature review. Comput Netw. 2022;214(4):109154. doi:10.1016/j.comnet.2022.109154.
3. Chang V, Golightly L, Modesti P, Xu QA, Doan LMT, Hall K, et al. A Survey on Intrusion Detection Systems for Fog and Cloud Computing. Future Internet. 2022;14(3):89. doi:10.3390/fi14030089.
4. Pundir S, Wazid M, Singh DP, Das AK, Rodrigues JJ, Park Y. Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. IEEE Access. 2019;8:3343-63.
5. Abdussami AA. Incremental deep neural network intrusion detection in fog based IoT environment: An optimization assisted framework. Indian J Comput Sci Eng. 2021;12(6):1847-59. doi:10.21817/indjcse/2021/v12i6/211206191.
6. Kumar KV, Thiruppathi M. Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog Assisted Wireless Sensor Network. Acta Montan Slovaca. 2023;28(2). doi:10.46544/AMS.v28i2.18.
7. Rahman MA, Asyhari AT, Leong LS, Satrya GB, Tao MH, Zolkipli MF. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustain Cities Soc. 2020;61(1):102324. doi:10.1016/j.scs.2020.102324.
8. Kumar KV, Rajakani V. Modeling of Intrusion Detection System using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning on Internet of Things Environment. Braz Arch Biol Technol. 2024;67. doi:10.1590/1678-4324-2024231010.
9. Saif S, Das P, Biswas S, Khari M, Shanmuganathan V. HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare. Microprocess Microsyst. 2022;104622. doi:10.1016/j.micpro.2022.104622.
10. Fang W, Zhang W, Chen W, Liu Y, Tang C. TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing. Wirel Netw. 2020;26(11):3169-82. doi:10.1007/s11276-019-02129-w.
11. Sahar N, Mishra R, Kalam S. Deep learning approach-based network intrusion detection system for fog-assisted IoT. In: Proceedings of international conference on big data, machine learning and their applications, Singapore. 2021. p. 39-50. doi:10.1007/978-981-15-8377-3_4.
12. Kumar KV, Balakrishnan S. Multi-objective Sand Piper Optimization Based Clustering with Multihop Routing Technique for IoT Assisted WSN. Braz Arch Biol Technol. 2023;66. doi:10.1590/1678-4324-2023220866.
13. Gupta IK, Mishra AK, Diwan TD, Srivastava S. Unequal clustering scheme for hotspot mitigation in IoT-enabled wireless sensor networks based on fire hawk optimization. Comput Electr Eng. 2023;107:108615. doi:10.1016/j.compeleceng.2023.108615.
14. Jacob SS, Karthikeyan B, Johnpeter T, Jayamala R. Deployment with Location Knowledge by Multi Area Approach for Detecting Replica Nodes in Wireless Sensor Network. Tech Vjesn. 2024;31(1):254-61. doi:10.17559/TV-20230508000613.
15. Jasim AA, Idris MYI, Razalli Bin Azzuhri S, Issa NR, Rahman MT, Khyasudeen MFB. Energy-efficient wireless sensor network with an unequal clustering protocol based on a balanced energy method (EEUCB). Sensors (Basel). 2021;21(3):784. doi:10.3390/s21030784.
16. Balakrishnan S, Kumar KV. Hybrid Sine-Cosine Black Widow Spider Optimization based Route Selection Protocol for Multihop Communication in IoT Assisted WSN. Tech Vjesn. 2023;30(4). doi:10.17559/TV-20211216115635.

17. El Assari Y. Energy-efficient multi-hop routing with unequal clustering approach for wireless sensor networks. Int J Comput Netw Commun (IJCNC). 2020;12(3):57-75. doi:10.5121/ijcnc.2020.12304.
18. Rajakani V, Kumar KV. Barnacles Mating Optimizer with Hopfield Neural Network Based Intrusion Detection in Internet of Things Environment. Tech Vjesn. 2023;30(6). doi:10.17559/TV-20211216115635.
19. Agrawal D, Pandey S. Load balanced fuzzy-based unequal clustering for wireless sensor networks assisted Internet of Things. Eng Rep. 2020;2(6). doi:10.1002/eng2.12130.
20. Thiruppathi M, Kumar KV. Seagull Optimization-based Feature Selection with Optimal Extreme Learning Machine for Intrusion Detection in Fog Assisted WSN. Tech Vjesn. 2023;30(5). doi:10.17559/TV-20211216115635.
21. Li G, Wang P, Zhou B, He H, Hao W, Yang T. QoS-aware secure transmission design for VLC with semi-grant-free NOMA scheme. Opt Express. 2023 Mar 27;31(7):11923-39. doi:10.1364/oe.485673.
22. Kumar G, Mohan S, Nagesh A. An ensemble of feature subset selection with deep belief network based secure intrusion detection in big data environment. Indian J Comput Sci Eng (IJCSE). 2021;12(2):409-20. doi:10.21817/indjcse/2021/v12i2/211202101.
23. Thiruvenkatasamy S, Sivaraj R, Vijayakumar M. Blockchain Assisted Fireworks Optimization with Machine Learning based Intrusion Detection System (IDS). Tech Vjesn. 2024;31(2):596-603. doi:10.17559/TV-20230712000798.
24. Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for internet of things. Future Gener Comput Syst. 2018;82:761-8. doi:10.1016/j.future.2017.08.043.
25. Yang Y, Zheng K, Wu C, Niu X, Yang Y. Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks. Appl Sci. 2019;9(2):238. doi:10.3390/app9020238.
26. Jayamala R, Oliver AS, Jayanthi J, Nithya N. Enhanced Secured and Real-Time Data Transmissions in Wireless Sensor Networks using SFRT Routing Protocol. Tech Vjesn. 2024;31(2):420-425. doi:10.17559/TV-20230617000742.


© 2024 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)