Dynamic Arithmetic Optimization Algorithm with Deep Learning-based Intrusion Detection System in Wireless Sensor Networks

K. Nirmal
Krishnasamy College of Engineering and Technology, Cuddalore, India
nirmalphd21@gmail.com (corresponding author)

S. Murugan
Dr. M.G.R. Government Arts and Science College for Women, Villupuram, India
smuruganmpt79@gmail.com

Received: 14 August 2024 | Revised: 26 August 2024 | Accepted: 4 September 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | *DOI: https://doi.org/10.48084/etasr.8742*

ABSTRACT

A Wireless Sensor Network (WSN) encompasses interconnected Sensor Nodes (SNs) that interact wirelessly to collect and transfer data. Security in the context of WNS refers to protocols and measures implemented for the overall functionality of the network, along with protecting the availability, confidentiality, and integrity of data against tampering, unauthorized access, and other possible security risks. An Intrusion Detection System (IDS) utilizing Deep Learning (DL) and Feature Selection (FS) leverages advanced methods to enhance effectiveness in the detection of malicious activities in a network by enhancing relevant data features and leveraging the power of Deep Neural Networks (DNNs). This study presents a Dynamic Arithmetic Optimization Algorithm within a DL-based IDS (DAOADL-IDS) in WSNs. The purpose of DAOADL-IDS is to recognize and classify intrusions in a WSN using a metaheuristic algorithm and DL models. To accomplish this, the DAOADL-IDS technique utilizes a Z-score data normalization approach to resize the input dataset in a compatible format. In addition, DAOADL-IDS employs a DAOA-based FS (DAOA-FS) model to select an optimum set of features. A Stacked Deep Belief Network (SDBN) model is employed for the Intrusion Detection (ID) process. The hyperparameter selection of the SDBN model is accomplished using the Bird Swarm Algorithm (BSA). A wide experimental analysis of the proposed DAOADL-IDS method was performed on a benchmark dataset. The performance validation of the DAOADL-IDS technique showed an accuracy of 99.68%, demonstrating superior performance over existing techniques under various measures.

Keywords-intrusion detection system; deep learning; bird swarm algorithm; wireless sensor network; feature selection

I. INTRODUCTION

Today, WSNs support smart IoT applications, and their reliability is significant for various real-time applications such as industry, military, environmental monitoring factors, wide-area surveillance, and healthcare [1]. WSNs play a vital role in the Industry 4.0 revolution and are crucial to collecting data using SNs [2]. Due to the short battery life of SNs, optimal energy consumption is a challenging task, and the energy efficiency of SNs plays an important role due to their limited resources in communication and processing [3]. Therefore, it is important to suggest effective energy consumption procedures to extend the life and stability of WSNs. In addition, optimal energy utilization in WSNs is needed to achieve a longer life and enhance WSN performance [4]. Thus, the combination of sensors in groups is used to minimize dissipation and increase the expandability of the network. Each network cluster has one head called a Cluster Head (CH) that links with other CHs [5].

In grouped WSNs, a routing protocol is used to identify the optimal route between CHs and BS and reduce energy consumption [6]. Routing protocols feature trustworthiness, error tolerance, scalability, data accretion, etc. Due to its impromptu behavior, a WSN can attract numerous internal and external attacks [7]. Some standard attacks used are black and gray holes, wormholes, and DDoS. Therefore, the use of an IDS in a WSN is important [8]. WSNs are not able to provide the sufficient data that IDSs require and are not directly functional to WSNs. Therefore, the construction of an easy and lightweight WSN IDS has become an essential topic in the WSN security area. Thus, it is vital to precisely detect numerous attacks. Some recently proposed IDS methods are based on techniques such as Random Forest (RF), Naive Bayes (NB), Convolutional Neural Networks (CNN), Decision Tree (DT), and other Machine Learning (ML) models [9].

This study presents a Dynamic Arithmetic Optimization Algorithm within a DL-based IDS (DAOADL-IDS) in WSN. DAOADL-IDS utilizes a Z-score data normalization approach to resize the input dataset into a compatible format. In addition, the proposed technique employs the DAOA-based FS (DAOA-FS) model to select an optimum set of features. A Stacked Deep Belief Network (SDBN) model is employed for the Intrusion Detection (ID) process. Finally, the hyperparameter selection of the SDBN model is accomplished by utilizing the Bird Swarm Algorithm (BSA). The key contributions of the proposed DAOADL-IDS technique are as follows:

- The DAOADL-IDS model standardizes the input dataset utilizing Z-score normalization. This preprocessing step contributes to enhanced model accuracy and consistency by confirming that features are on a uniform scale.
- The DAOA-FS approach is implemented to detect and choose the most relevant features. This approach improves performance by focusing on the most crucial attributes, resulting in enhanced accuracy and efficiency for data processing tasks.
- The DAOADL-IDS technique integrates SDBN for ID, employing DL models to detect anomalies with high accuracy. This method improves the detection process by learning intricate patterns and relationships in the data. The use of SDBN contributes to more efficient and precise ID.
- The BSA model is used for fine-tuning. This method optimizes the model settings, improving accuracy and effectiveness. Systematic hyperparameter adjustment through BSA confirms that the model performs optimally across diverse scenarios.
- The DAOADL-IDS method improves the effectiveness and efficiency of the model by incorporating advanced preprocessing, FS, DL, and optimization models. Its novelty relies on the cohesive use of these techniques to enhance overall model performance and adaptability.

II. LITERATURE REVIEW

In [10], a fuzzy-assisted ant colony optimizer was proposed to improve the security of a routing protocol (F-ACO-SQoSRP). In [11], an ANFIS-based clustering method was used and a DBN was applied for efficient ID. In [12], a Deep Q Network (DQN) based on the Taylor Competitive Multi-Verse Optimizer (Taylor CMVO) technique was proposed. In this approach, PSO-based machines manage CHS, Particle-Water Wave Optimization (P-WWO) handles routing with Canberra distance for FS, and IDS is used with DQN trained using a model that integrates CMVO with Taylor sequence. In [13], an IDS was introduced based on the density-assisted Spatial Clustering of Application with Noise (DBSCAN) cluster procedure. In [14], an IoT-based Cluster-Based Routing (CBR) process was introduced for an information-centric WSN. This model used a BWO-based clustering model for CH selection and an Oppositional ABC (OABC) routing technique for path selection. In [15], a classification structure was proposed that incorporated signature and ID with MLP-NN by clustering.

In [16], an AI-based energy-aware IDS and routing technique was proposed, based on a game theory decision model and an ad-hoc on-demand distance vector procedure. In [17], the Double Adaptive Weighting Arithmetic Optimization Algorithm with DL (DAWAOA-DL) approach was introduced, which involved DAWAOA for FS, CNN-GRU for ID, and Adam optimizer for fine-tuning. In [18], the Secure DL-based Energy-Efficient Routing (SDLEER) model was proposed, which combined energy-efficient routing, optimized CH selection, preprocessing, PCA, and Smish-activated RNN-based classification. In [19], a Restricted Boltzmann Machines (RBMs) model was introduced, which utilized a two-tier method with a Chaotic Ant Optimization (CAO) model. In [20], a DL-based IDS was proposed, which used chaotic optimization, data cleansing, extended synthetic sampling, kernel-assisted PCA, chaotic Honey Badger Optimization (HBO), and Dugat-LSTM for classification.

Existing approaches face challenges with scalability and computational efficiency, particularly in parameter tuning and overhead. Anomaly detection models can be sensitive to parameter settings, while cluster-based routing methods may face difficulties with dynamic networks. Conventional signature-based systems often overlook growing threats. Research gaps include improving scalability, real-time performance, adaptability, and managing computational demands.

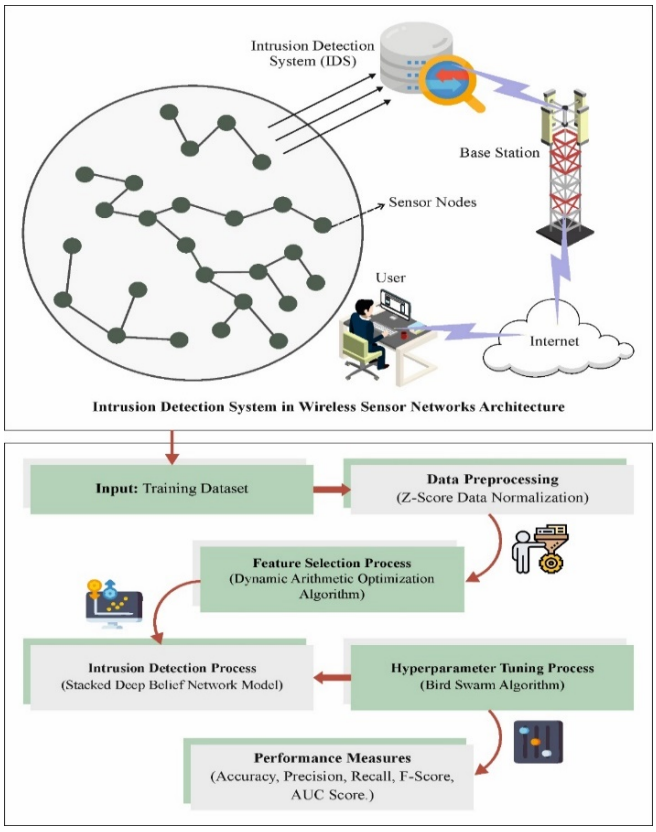

Fig. 1. Workflow of DAOADL-IDS model.

III. THE PROPOSED MODEL

This study presents a novel DAOADL-IDS method to enhance security in WSNs. The objective is to detect and classify intrusions using a metaheuristic method and DL models. The DAOADL-IDS technique applies Z-score data normalization, DAOA-FS, SDBN classification, and BSA-based tuning. Figure 1 illustrates the structure of the proposed DAOADL-IDS approach.

A. Z-Score Normalization

This technique is implemented to normalize the input data and is also known as standardization. It is a statistical model applied to rescale and center a dataset by converting data points into a standard unit deviation in relation to the mean of the entire dataset. This procedure includes dividing by the standard deviation and subtracting the mean. This is widely used in data preprocessing to facilitate comparisons between different parameters with varying scales, promoting a comparable and standardized representation of data across various features.

B. Feature Selection Using the DAOA-FS Technique

The DAOA-FS method is exploited to select an optimal set of features. AOA is a new metaheuristic approach used to leverage the distributional property of arithmetical operators to find the optimum element from the pool of candidate results and includes two main phases: exploitation and exploration [21]. At first, a population of N solutions is initialized with a d-dimension search range represented by $X_i = \{x_{i1}, x_{i2}, \cdots x_{id}\}$, $i = 1,2, \cdots, N$. Then, the phase of the method is defined by a Math Optimizer Accelerated (MOA) function. Next, MOA is evaluated by the following equation, where r_1 is a random integer within [0,1]. If $r_1 > MOA$, then exploration takes place. If $r_1 < MOA$, then exploitation takes place.

$$MOA(iter) = Min + iter\left(\frac{Max - Min}{iter_{max}}\right) \quad (1)$$

where $iter$ is the current iteration count, $MOA(iter)$ denotes the MOA value at that iteration, and $iter_{\max}$ is the maximum iteration count. Max and Min are the maximum and minimum values of the MOA function, set to 1 and 0.2, respectively. Division and multiplication calculations produce distribution values that enhance exploration.

$$X_{i,j}(iter) = \begin{cases} \frac{X_{best,j}(iter)}{(MOP+\varepsilon)} \times \\ \left(\left[\left(UB_j - LB_j\right) \times \mu + LB_j\right]\right) \text{ if } r_2 < 0.5 \\ X_{best,j}(iter) \times MOP \times \\ \left[\left(UB_j - LB_j\right) \times \mu + LB_j\right] \text{ otherwise} \end{cases} \quad (2)$$

where $X_{i,j}$ denotes the position of i^{th} individual in the j^{th} dimension of optimal solution at $iter$ iteration, $X_{best,j}$ indicates the position of the j^{th} dimension of the optimum individual at $iter^{\text{th}}$ iteration, r_2 represents a random value within [0, 1], ε denotes a small positive value that averts the divisor from becoming 0, μ adjusts the control variable fixed as 0.5, and UB_j and LB_j are the upper and lower limitations at j^{th} parameter:

$$MOP(iter) = 1 - \frac{iter^{\frac{1}{\alpha}}}{iter_{\max}^{\frac{1}{\alpha}}} \quad (3)$$

Here, MOP denotes the math optimizer probability, with α fixed at 5 to control exploitation accuracy. During exploitation, addition and subtraction operators are used for their low dispersion and simplicity in achieving targets. $X_{best,j}(iter)$ is the best solution for dimension j at iteration $iter$. MOP is the modification parameter, and UB_j and LB_j are the upper and lower bounds for dimension j. μ is a scaling factor and r_3 denotes the random number within [0, 1].

$$X_{i,j}(iter) = \begin{cases} X_{best,j}(iter) - MOP \times \\ \left(\left(UB_j - LB_j\right) \times \mu + LB_j\right) \text{ if } r_3 < 0.5 \\ X_{best,j}(iter) + MOP \times \\ \left(\left(UB_j - LB_j\right) \times \mu + LB_j\right) \text{ otherwise} \end{cases} \quad (4)$$

The DAOA model uses evolutionary optimization for various tasks, including forecasting, routing, and portfolio management. Using stochastic and probabilistic searches, it refines solutions to converge on local optima and is applicable in fields such as image processing, scheduling, robotics, and ML/AI. The individual upgrade formula for DAOA is:

$$X_i(t+1) = X_i(t) + a \times \left(X_{best}(t) - X_i(t)\right) + b \times \left(X_i(t) - X_{worst}(t)\right) \quad (5)$$

where $X_i(t)$ refers to the location at time t, $X_{best}(t)$ and $X_{worst}(t)$ are the place of optimum and worst individuals in the population at t time, and the parameters a and b switch the exploitation and exploration performance of the model.

```
Algorithm 1: Pseudocode of DAOA
1: Set parameters of the optimization
   problem
2: Produce an arbitrary initial solution
3: Estimate current solution
4: Repeatedly change solution parameters
5: Check union measures to select if
   the algorithm has united
6: If the algorithm has united, stop, or
   else return to Step 2.
```

In the DAOA-FS method, the objectives are assimilated into a single objective so that a predetermined weight detects each objective importance [22]. Here, an FF is utilized that incorporates both FS objectives:

$$Fitness(X) = \alpha \cdot E(X) + \beta\left(1 - \frac{|R|}{|N|}\right) \quad (6)$$

In (6), the fitness value of the subset is represented as $Fitness(X)$. The error rate of the classifier by using the factors selected in the X subset is denoted by $E(X)$. The feature count chosen and the new feature count from the dataset are $|R|$ and $|N|$, respectively, the classifier error weight and the reduction ratio are α and β, where $\alpha \in [0,1]$ and $\beta = (1 - \alpha)$.

C. ID utilizing SDBN

The SDBN model employs DBNs for ID, employing a multi-layered probabilistic structure with parameters for model learning. DBNs consist of a Visible Layer (VL) and a Hidden Layer (HL), where the HL captures the distribution of visible

variables, and the layers are symmetrically connected, though not interlinked within the same layer. The hierarchical processing of stacking RBM is utilized to create the DBN model. RBM is used for encoding the joint probability dispersion via the energy function, the noticeable data is v, the hidden data is h, and w is the weight:

$$E(v,h,\theta) = -\sum_i \sum_j w_{ij}\, v_i h_j - \sum_i b_i^{(v)}\, v_i - \sum_j b_j^{(h)}\, h_j \quad (7)$$

$$p(v,h|\theta) = \frac{\exp(-E(v,h|\theta)}{\Sigma_{v'}\Sigma_{h'}\exp(-E(v',h'|\theta)} \quad (8)$$

The rules are presented for updating the primary state so that any update provides a low-energy state and finally settles into a balance:

$$p(v_i = 1|h,\theta) = \sigma\left(\sum_j w_{ij}\, h_j + b_i^{(v)}\right) \quad (9)$$

$$p(h_i = 1|v,\theta) = \sigma\left(\sum_i w_{ij}\, v_i + b_j^{(h)}\right) \quad (10)$$

The VL receives the input data to train the RBM model, adjusting the θ parameter to maximize the likelihood of the observed data, thereby enhancing the model's ability to generate accurate data. A Contrastive Divergence (CD) model trials the HL's new value with the existing input to provide an entire sample (v_{data}, h_{data}). Moreover, it generates samples for the VL and then for the HL. The model sample (v_{model}, h_{model}) is used to update the weights by:

$$\Delta w_{ij} = \eta\left(v_{i,data}h_{j,data} - v_{i,model}h_{j,model}\right) \quad (11)$$

Stacked DBNs excel in unsupervised feature learning and are widely used in signal processing and image recognition, benefiting from their distributed and hierarchical representations. Pretraining and fine-tuning layers for specific tasks enhance their versatility in machine learning applications.

D. Hyperparameter Tuning Using BSA

Finally, the hyperparameters of the SDBN method were chosen using BSA. The BSA model pretends the bird's performance in vigilance, foraging, and flight [23]. This technique consists of four different foraging mechanisms. The BSA model was chosen due to its effective balance between exploration and exploitation, enabling it to effectively navigate complex search spaces and find optimal parameter settings. Its biologically inspired model improves adaptability and convergence speed, making it suitable for fine-tuning models across various scenarios.

1) Foraging Behavior

Each agent forages for food based on its location and the swarm's optimal position, as illustrated in:

$$x_{i,j}^{(t+1)} = x_{i,j}^t + \left(p_{i,j} - x_{i,j}^t\right) \times C \times rand(O,1) + \left(g_j - x_{i,j}^t\right) \times S \times rand(0,1) \quad (12)$$

whereas S and C denote the social and cognitive coefficients, $rand(0,1)$ creates a random real amount among $(0,1)$, g_j refers to the best location attained by the swarm, and p_{ij} denotes the preceding location of i^{th}agent.

2) Vigilance Behavior

The agent's effort to move to the swarming center is formulated by:

$$x_{i,j}^{(t+1)} = x_{i,j}^t + \left(A_1\left(w_{mean,j} - x_{i,j}^t\right) \times rand(0,1) + A_2\left(p_{k,j} - x_{i,j}^t\right) \times rand(-1,1)\right) \quad (13)$$

$$A_1 = a_1 \times exp\left(-\frac{p_{Fit,i}}{SumFit+\varepsilon} \times N\right) \quad (14)$$

$$A_2 = a_2 \times exp\left(\left(\frac{p_{Fit,i} - p_{Fit,k}}{|p_{Fit,k} - p_{Fit,i}+\varepsilon|}\right) \times \frac{N \times p_{Fit,k}}{SumFit+\varepsilon}\right) \quad (15)$$

where a_1 and a_2 fall in $[0,2]$, k represents a random number in $[1,N]$ such that $k \neq i$, $pFit_j$ denotes the optimal value of the i^{th} agent, $SumFit$ signifies the total fitness of the swarm, $mean_j$ is the average position in the j^{th} dimension, and ε prevents division errors. The A_1 product must not exceed 1, and A_2 indicates the interference effect affecting the swarm's center.

3) Flighting Behavior

Birds fly to new areas to avoid risks and find food, with some seeking new patches while others use existing ones. This behavior is calculated by:

$$x_{i,j}^{(t+1)} = x_{i,j}^t + randn(0,1) \times x_{i,j}^t \quad (16)$$

$$x_{i,j}^{(t+1)} = x_{i,j}^t + \left(x_{k,j}^t - x_{i,j}^t\right) \times FL \times randn(0,1) \quad (17)$$

where FL, ranging from 0 to 2, denotes the next producer. Fitness selection is crucial in BSA. The encoder computes candidate performance, with accuracy values assisting as initial conditions for constructing an FF.

$$Fitness = \max(P) \quad (18)$$

$$P = \frac{TP}{TP+FP} \quad (19)$$

where TP and FP denote the true and false positives, respectively.

IV. RESULTS AND DISCUSSION

The DAOADL-IDS approach was tested using the dataset in [24]. The DAOADL-IDS approach selected 16 features out of 23. The simulation was performed by employing Python 3.6.5 on a PC with an i5-8600K CPU, 250GB SSD, GeForce 1050Ti 4GB, 16GB RAM, and 1TB HDD. The parameters include a learning rate of 0.01, ReLU activation, 50 epochs, a dropout of 0.5, and a batch size of 5.

TABLE I. DATASET DETAILS

Type of data	**Instances**
Normal	340066
Blackhole	10049
Grayhole	14596
Flooding	3312
Scheduling Attacks	6638
Overall Instances	**374661**

Table II compares the DAOADL-IDS approach with recent approaches [25-27]. Based on $accu_y$, the DAOADL-IDS

model presents higher a $accu_y$ of 99.68% while the KNN, C4.5, CART, RBN, RF, FFNN, and RNN models exhibited lower values of 99.52%, 98.96%, 97.50%, 97.85%, 96.56%, 96.67%, and 94.95%, respectively. According to $prec_n$, the DAOADL-IDS model achieved a higher $prec_n$ of 92.18% while the KNN, C4.5, CART, RBN, RF, FFNN, and RNN models achieved 91.38%, 89.22%, 91.19%, 89.66%, 89.47%, 91.90%, and 89.69%. With $reca_l$, the DAOADL-IDS technique achieved a greater $reca_l$ of 98.11% while the KNN, C4.5, CART, RBN, RF, FFNN, and RNN methods achieved 96.56%, 90.55%, 94.85%, 92.09%, 90.71%, 92.80%, and 93.23%. On F_{score}, the DAOADL-IDS technique achieved 95% while the KNN, C4.5, CART, RBN, RF, FFNN, and RNN methods achieved 93.59%, 92.63%, 93.19%, 95.90%, 94.80%, 91.23%, and 92.16%, respectively.

TABLE II. RELATIVE EVALUATION OF THE DAOADL-IDS MODEL WITH OTHER METHODS

Model	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
DAOADL-IDS	99.68	92.18	98.11	95.00
KNN	99.52	91.38	96.56	93.59
C4.5	98.96	89.22	90.55	92.63
CART	97.50	91.19	94.85	93.19
RBN	97.85	89.66	92.09	90.95
RF	96.56	89.47	90.71	94.80
FFNN	96.67	91.90	92.80	91.23
RNN	94.95	89.69	93.23	92.16

These results demonstrate the improved effectiveness of the DAOADL-IDS method.

V. CONCLUSION

This study introduced the novel DAOADL-IDS method to improve security in WSNs. The aim was to detect and classify intrusions in WSN. The DAOADL-IDS technique utilizes Z-score data normalization, DAOA-FS, SDBN-based classification, and BSA-based parameter tuning. The DAOADL-IDS technique employs the DAOA-FS method to select a better feature set. The SDBN model is used for the ID process. Finally, the hyperparameter selection of the SDBN model is performed using BSA. A widespread experimental analysis of the DAOADL-IDS technique was performed on a benchmark dataset to validate its ID performance. The performance validation of the DAOADL-IDS technique showed a superior accuracy of 99.68% compared to existing techniques under various measures. The DAOADL-IDS model may face scalability and parameter sensitivity issues, with future work needed to address these challenges and enhance adaptability to dynamic environments.

REFERENCES

[1] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, vol. 26, no. 5, pp. 3169–3182, Jul. 2020, https://doi.org/10.1007/s11276-019-02129-w.

[2] N. Sahar, R. Mishra, and S. Kalam, "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, pp. 39–50, https://doi.org/10.1007/978-981-15-8377-3_4.

[3] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020, https://doi.org/10.1109/ACCESS.2019.2962829.

[4] M. P. Ramkumar, T. Daniya, P. Mano Paul, and S. Rajakumar, "Intrusion detection using optimized ensemble classification in fog computing paradigm," *Knowledge-Based Systems*, vol. 252, Sep. 2022, Art. no. 109364, https://doi.org/10.1016/j.knosys.2022.109364.

[5] C. A. de Souza, C. B. Westphall, R. B. Machado, L. Loffi, C. M. Westphall, and G. A. Geronimo, "Intrusion detection and prevention in fog based IoT environments: A systematic literature review," *Computer Networks*, vol. 214, Sep. 2022, Art. no. 109154, https://doi.org/10.1016/j.comnet.2022.109154.

[6] A. A. Abdussami and Dr. M. F. Farooqui, "Incremental deep neural network intrusion detection in fog based IoT environment: An optimization assisted framework," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 6, pp. 1847–1859, Dec. 2021, https://doi.org/10.21817/indjcse/2021/v12i6/211206191.

[7] M. A. Rahman, A. T. Asyhari, L. S. Leong, G. B. Satrya, M. Hai Tao, and M. F. Zolkipli, "Scalable machine learning-based intrusion detection system for IoT-enabled smart cities," *Sustainable Cities and Society*, vol. 61, Oct. 2020, Art. no. 102324, https://doi.org/10.1016/j.scs.2020.102324.

[8] B. Mopuru and Y. Pachipala, "Advancing IoT Security: Integrative Machine Learning Models for Enhanced Intrusion Detection in Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14840–14847, Aug. 2024, https://doi.org/10.48084/etasr.7641.

[9] B. Mopuru and Y. Pachipala, "Enhanced Intrusion Detection in IoT with a Novel PRBF Kernel and Cloud Integration," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14988–14993, Aug. 2024, https://doi.org/10.48084/etasr.7767.

[10] S. Subramani and M. Selvi, "Intrusion detection system using RBPSO and fuzzy neuro-genetic classification algorithms in wireless sensor networks," *International Journal of Information and Computer Security*, vol. 20, no. 3–4, pp. 439–461, Jan. 2023, https://doi.org/10.1504/IJICS.2023.128857.

[11] M. Maheswari and R. A. Karthika, "A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 118, no. 2, pp. 1535–1557, May 2021, https://doi.org/10.1007/s11277-021-08101-2.

[12] P. S. Khot and U. Naik, "Taylor CMVO: Taylor Competitive Multi-Verse Optimizer for intrusion detection and cellular automata-based secure routing in WSN," *International Journal of Intelligent Robotics and Applications*, vol. 6, no. 2, pp. 306–322, Jun. 2022, https://doi.org/10.1007/s41315-022-00225-3.

[13] R. Zhang, J. Zhang, Q. Wang, and H. Zhang, "DOIDS: An Intrusion Detection Scheme Based on DBSCAN for Opportunistic Routing in Underwater Wireless Sensor Networks," *Sensors*, vol. 23, no. 4, Jan. 2023, Art. no. 2096, https://doi.org/10.3390/s23042096.

[14] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, and K. Shankar, "A Novel Hybrid Optimization for Cluster-Based Routing Protocol in Information-Centric Wireless Sensor Networks for IoT Based Mobile Edge Computing," *Wireless Personal Communications*, vol. 127, no. 1, pp. 39–62, Nov. 2022, https://doi.org/10.1007/s11277-021-08088-w.

[15] D. R. K. Chougale, "Intrusion Detection System based on Energy Efficient Dynamic Clustering in a Heterogeneous Environment of Wireless Sensor Networks (WSNs)," *Neuro Quantology*, vol. 20, no. 9, pp. 4756–4766, 2022.

[16] P. Aruchamy, S. Gnanaselvi, D. Sowndarya, and P. Naveenkumar, "An artificial intelligence approach for energy-aware intrusion detection and secure routing in internet of things-enabled wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 23, 2023, Art. no. e7818, https://doi.org/10.1002/cpe.7818.

[17] V. K. Kalimuthu and R. Velumani, "Modeling of Intrusion Detection System Using Double Adaptive Weighting Arithmetic Optimization

Algorithm with Deep Learning on Internet of Things Environment," *Brazilian Archives of Biology and Technology*, vol. 67, May 2024, Art. no. e24231010, https://doi.org/10.1590/1678-4324-2024231010.

[18] M. Sakthimohan, J. Deny, and G. E. Rani, "Secure deep learning-based energy efficient routing with intrusion detection system for wireless sensor networks," *Journal of Intelligent & Fuzzy Systems*, vol. 46, no. 4, pp. 8587–8603, Jan. 2024, https://doi.org/10.3233/JIFS-235512.

[19] J. Srivastava and J. Prakash, "Multi-modal for Energy Optimization and Intrusion Detection in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 133, no. 1, pp. 289–321, Nov. 2023, https://doi.org/10.1007/s11277-023-10768-8.

[20] R. Devendiran and A. V. Turukmane, "Dugat-LSTM: Deep learning based network intrusion detection system using chaotic optimization strategy," *Expert Systems with Applications*, vol. 245, Jul. 2024, Art. no. 123027, https://doi.org/10.1016/j.eswa.2023.123027.

[21] Y. Qiu, L. Wu, C. Zuo, R. Jia, and H. Zhang, "Optimal scheduling of solar-surface water source heat pump system based on an improved arithmetic optimization algorithm," *Egyptian Informatics Journal*, vol. 24, no. 4, Dec. 2023, Art. no. 100415, https://doi.org/10.1016/j.eij.2023.100415.

[22] M. Mafarja *et al.*, "Classification framework for faulty-software using enhanced exploratory whale optimizer-based feature selection scheme and random forest ensemble learning," *Applied Intelligence*, vol. 53, no. 15, pp. 18715–18757, Aug. 2023, https://doi.org/10.1007/s10489-022-04427-x.

[23] F. A. Hashim, R. A. Khurma, D. Albashish, M. Amin, and A. G. Hussien, "Novel hybrid of AOA-BSA with double adaptive and random spare for global optimization and engineering problems," *Alexandria Engineering Journal*, vol. 73, pp. 543–577, Jul. 2023, https://doi.org/10.1016/j.aej.2023.04.052.

[24] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *Journal of Sensors*, vol. 2016, no. 1, 2016, Art. no. 4731953, https://doi.org/10.1155/2016/4731953.

[25] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, "An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs," *Sensors*, vol. 22, no. 4, Jan. 2022, Art. no. 1407, https://doi.org/10.3390/s22041407.

[26] P. Gite, K. Chouhan, K. Murali Krishna, C. Kumar Nayak, M. Soni, and A. Shrivastava, "ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4.5 and CART classifiers," *Materials Today: Proceedings*, vol. 80, pp. 3769–3776, Jan. 2023, https://doi.org/10.1016/j.matpr.2021.07.378.

[27] A. Singh, J. Amutha, J. Nagar, S. Sharma, and C. C. Lee, "AutoML-ID: automated machine learning model for intrusion detection using wireless sensor network," *Scientific Reports*, vol. 12, no. 1, May 2022, Art. no. 9074, https://doi.org/10.1038/s41598-022-13061-z.