Enhancing Security in Healthcare Frameworks using Optimal Deep Learning-based Attack Detection and Classification for Medical Wireless Sensor Networks

Ranathive Shanmugavelu
Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India
rs9189@srmist.edu.in (corresponding author)

Vidhya Ravi
Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India
vidhyar@srmist.edu.in

Received: 29 November 2024 | Revised: 13 December 2024 | Accepted: 31 December 2024

 DOI: https://doi.org/10.48084/etasr.9741

ABSTRACT

Wireless Sensor Networks (WSNs) have modernized healthcare, providing vital sign collection and real-time patient monitoring. Healthcare WSNs are vulnerable to cyberattacks, such as false data injection, sensor manipulation, and data eavesdropping, which can disrupt monitoring and endanger patient lives. Traditional Intrusion Detection Systems (IDSs) based on static signatures struggle with evolving threats. Deep Learning (DL)-based IDSs, combined with Feature Selection (FS), offer a more adaptive and effective solution, improving attack detection and protecting patient data. This work presents an innovative Pigeon-Inspired Optimizer-based Feature Selection with Deep Learning-based Attack Detection and Classification (PIOFS-DLADC) method, which focuses on creating an optimal DL framework for attack detection and classification in healthcare WSNs. Initially, patient health data (actual input data) undergo preprocessing using the one-hot encoding system. Then, the PIOFS method selects key features from sensor data streams, reducing dimensionality and improving model efficiency. Furthermore, an attention-based Bidirectional Gated Recurrent Unit (BiGRU) method captures long-term dependencies and prioritizes features for accurate attack classification. The Coati Optimization Algorithm (COA) is employed to tune the hyperparameters of the DL models. The model efficiently explores the hyperparameter space, optimizing the performance for attack detection and classification. Validated on a healthcare WSN dataset, the PIOFS-DLADC model demonstrated an accuracy of 96.78%, which is superior to existing approaches.

Keywords-wireless sensor networks; feature selection; coati optimization algorithm; attack detection; deep learning

I. INTRODUCTION

WSNs use distributed sensors to monitor environmental factors such as temperature, humidity, and pollution [1]. However, they are vulnerable to selective forward attacks, where data is lost during transmission, reducing network efficiency and compromising data integrity [2]. WSNs in healthcare face challenges such as high packet loss due to unstable communication, requiring the distinction between malicious and regular losses [3-4]. Healthcare WSNs, which use wearable biosensors for patient monitoring, must address issues such as self-management, privacy, and routing [5]. Security concerns in these networks arise from the open wireless medium, dynamic topologies, and limited Sensor Node (SN) resources, with threats that affect data integrity [6]. As these systems handle sensitive patient data, security threats, such as man-in-the-middle, eavesdropping, and Denial-of-Service (DoS) attacks, threaten privacy and data integrity [7]. Additionally, advanced attackers target sensitive medical data, stressing the need for robust privacy preservation [8-9]. Emerging technologies such as Blockchain (BC), edge computing, and Machine Learning (ML) improve efficiency but leave systems vulnerable to malware [10].

In [11], an Exponential Polynomial Kernel-based Deep Neural Network (EPK-DNN) model was proposed. The Linear Scaling-based BAT optimizer (LS-BAT) selects and trains the features, while the WSN network is initialized using the

Damerau-Levenshtein-based K-means method. The cluster head was later elected using the rock hyraxes SO technique for sensor data collection. In [12], a hybrid DL mechanism was introduced, employing CNN and LSTM. After preprocessing, the Modified Huber Independent Component Analysis-based Squirrel Search Algorithm (MHICA-SSA) minimizes the data dimensionality, and then the DL-CNN-LSTM method is employed for attack detection. In [13], a DoS IDS was proposed, called STLGBM-DDS, which is an ensemble model utilizing Apache Spark, LightGBM-ML, and data balancing techniques such as Tomek-Links and SMOTE, along with FS through the Information Gain Ratio. In [14], an Optimized Hybrid DNN (OHDNN) was proposed, integrating CNN and LSTM, with FS based on enhanced conditional random fields and parameter optimization through adaptive golden eagle optimization. In [15], an enhanced DL model was proposed, where the extracted features were sent to a Deep Belief Network (DBN) model, with a hybrid mechanism called Local Leader Phase-based GOA (LLP-GOA).

In [16], a Deep Transfer Learning (DTL) technique was introduced, using a pre-trained CNN, with the final CNN output integrated through ensemble learning. In [17], a method was proposed using the adaptive Taylor-SFO technique. Routing was carried out using adaptive Taylor-SFO to choose the optimal route based on fitness, followed by attack detection with Deep Stacked-AE (DSAE). The network classifier was then tuned using Adaptive Taylor-SFO. In [18], a robust DCNN-based model was designed using a CUDA-based Nvidia-Quad GPU for parallel processing, comprising three subsystems: traffic classification, feature engineering, and feature learning. In [19], a DL-based IDS was proposed, using the Self-Improved Sea Lion Optimizer (SI-SLnO) for optimal weight adjustment. The method calculates trust using a multidimensional two-tier hierarchical mechanism. In [20], a robust IDS was developed using advanced DL techniques to detect and mitigate cybersecurity threats in IoMT. The study in [21] aimed to improve patient monitoring and healthcare quality using DL-based CNNs in cyber-physical healthcare systems. In [22], an Optimized Memory Augmented Graph Neural Network-based DoS Attacks Detection in WSN (DoS-AD-MAGNN-WSN) model was proposed, utilizing preprocessing with an adaptive filter, and feature extraction through nested patch-based methods. In [23], a hybrid Artificial Neural Network - Grasshopper Optimization Algorithm (ANN-GOA) method was proposed for anomaly detection in WSN.

The limitations of these studies include reliance on single datasets, limiting generalizability, and focusing on accuracy without considering real-time constraints such as computational power and network stability. Moreover, many models lack scalability in large-scale dynamic environments. Future work could address these gaps by using diverse datasets, optimizing for real-time performance, and improving scalability.

This work presents an innovative Pigeon-Inspired Optimizer-based Feature Selection with Deep Learning-based Attack Detection and Classification (PIOFS-DLADC) method for healthcare WSNs. Initially, patient health data (actual input data) undergo preprocessing using a one-hot encoding system. Then, the PIOFS method selects key features from sensor data streams, reducing dimensionality and improving model efficiency. Furthermore, an attention-based Bidirectional Gated Recurrent Unit (BiGRU) method captures long-term dependencies and prioritizes features for accurate attack classification. The Coati Optimization Algorithm (COA) is employed for hyperparameter tuning of the DL models. The model efficiently explores the hyperparameter space, optimizing the performance for attack detection and classification. This method was validated using a healthcare WSN dataset. The key contributions of the PIOFS-DLADC model are listed below.

- The PIOFS-DLADC model employs one-hot encoding for sensor data preprocessing, ensuring accurate input representation, while FS is performed using the PIO model to detect relevant features, improving both model efficiency and accuracy.
- The attention-based BiGRU model captures long-term dependencies in the data while dynamically assigning diverse levels of significance to features, improving the capability of the model to classify intrinsic patterns.
- The COA is employed for hyperparameter optimization, fine-tuning the model to improve performance, adaptability, and accuracy in detecting complex patterns in the data.
- The novelty of the PIOFS-DLADC model is its integration of advanced FS, attention-based BiGRU, and hyperparameter tuning techniques, creating a robust and effective framework for attack detection in healthcare WSNs.

II. THE PROPOSED MODEL

The main objective of this study was to design an optimum DL framework for attack detection and classification in healthcare WSNs, combining FS, attention-based DL, and hyperparameter tuning for improved security. Figure 1 shows the entire flow of the PIOFS-DLADC model.

A. Preprocessing

At the primary level, the PIOFS-DLADC technique utilizes a one-hot encoding method for preprocessing [24]. One-hot encoding has become a popular preprocessing method employed in ML, mainly for dealing with categorical data. When utilized for categorical variables, it converts them into binary matrix formats, generating the appropriate input into ML methods that need numerical input. In the setting of one-hot encoding, every type is characterized by a unique binary code, and one bit refers to "hot" (set to 1) for specific categories but all others are set to 0. This approach removes the issues related to employing ordinal numbers for categorical variables, in which numerical representation may inaccurately denote a particular ordinal relationship among the categories.

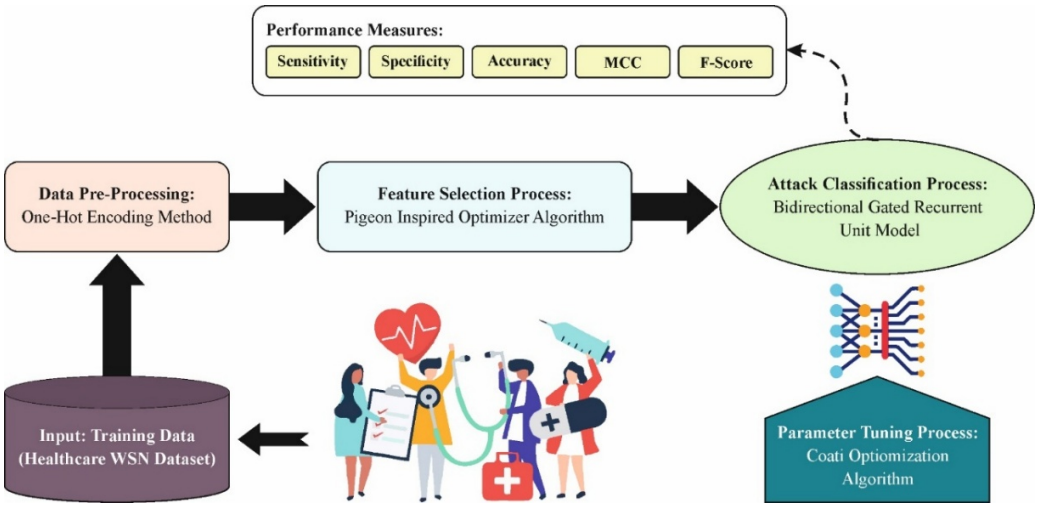

Fig. 1. The overall flow of the PIOFS-DLADC approach.

B. Feature Selection (FS) Process

The PIOFS technique [25] was employed for the FS process. PIO is a swarm intelligence optimization method that replicates pigeons' navigation with two key functions: the Compass and Map operator, using a mental map and magnetic cues, and the Landmark operator, where pigeons rely on landmarks to reach their target. The population is split into two groups, one following the current path and the other exploring new routes.

In the first stage, parameters for the PIO system are set, including the compass operator R, solution space, initial pigeon positions, population size, and iteration count. At each iteration t, the ML method is trained and evaluated based on fitness. The positions $X_i(t)$ and velocities $V_i(t)$ of the pigeons are updated according to:

$$X_i(t) = X_i(t-1) + V_i(t) \quad (1)$$

$$V_i(t) = V_i(t-1)e^{-R(t)} \cdot rand\left(X_g - X_i(t-1)\right) \quad (2)$$

where $rand()$ represents a random number, R is the map factor between 0 and 1, and X_g is the optimal position of the pigeon flock at time t, determined by the highest fitness value. After a set number of rounds, X_i is updated using the landmark operator to continue the iterative process. Pigeons are ranked based on their fitness values, with $N_{landmark}(t)$ representing the number of pigeons at iteration t (3). Pigeons farther from the target are rejected, while those closer move faster. $X_c(t)$ denotes the midpoint of the remaining pigeons, as defined in (4).

$$N_{landmark}(t) = \frac{N_{landmark}(t-1)}{2} \quad (3)$$

$$X_c(t) = \frac{\sum X_i(t) \cdot fitness(X_i(t))}{N_{1andmark}(t) \cdot fitness(X_i(t))} \quad (4)$$

In the PIOFS method, $N_{landmark}(t)$ represents the reduced population at iteration t, and $fitness(X_i(t))$ denotes the objective function value for the pigeon's location. The new location is updated according to (5), where pigeons adjust their positions based on the best midpoint each iteration, allowing for quick convergence to the optimal solution. The Fitness Function (FF), as defined in (10), balances FS (minimized) and classification accuracy (maximized).

$$X_i(t+1) = X_i(t) + rand\left(X_c(t+1) - X_i(t)\right) \quad (5)$$

$$V_i(t+1) = V_i(t) \cdot e^{-R(t)} \cdot rand\left(X_c(t) - X_i(t)\right) \quad (6)$$

$$Fitness = \alpha\gamma_R(D) + \beta\frac{|R|}{|C|} \quad (7)$$

where $|C|$ denotes the total number of features, $|R|$ is the size of the selected subset, $\gamma_R(D)$ indicates the classification error rate, and α and β are factors representing classification quality and subset length, where $\alpha \in [1,0]$ and $\beta = 1 - \alpha$.

C. Classification Using Attention-based BiGRU Model

At this stage, the attention-based BiGRU model is used for classification [26]. This model was chosen for its ability to capture both forward and backward dependencies while focusing on relevant features, providing enhanced classification performance than other models. RNNs are designed for sequence data processing but encounter challenges such as gradient vanishing, which gated architectures such as LSTM and GRU address. LSTM, introduced in 1997, manages long-term dependencies with memory units, while GRU, developed in 2014, simplifies LSTM by integrating input and forget gates. A BiGRU-based encoder-decoder model with a feature attention layer efficiently captures data trends by focusing on relevant features and refining inputs based on prior data.

Unidirectional log data, which is not ideal for target data prediction, is processed using the FAtt layer and split into forward $\overrightarrow{x_d}$ and backward $\overleftarrow{x_d}$ depth data. The bi-directional Hidden Layers (HLs) are obtained by training a self-determined GRU model for each direction. The forward $\overrightarrow{h_d}$ and backward $\overleftarrow{h_d}$ HLs of the same depth are merged into h_d as the decoder input. The decoder includes a GRU network layer and a Deep Attention mechanism (DAtt) layer. The DAtt layer applies a global attention model to capture detailed historical

and current depth data in the log. It considers the encoder output ($\{h_d\}_{d=1}^{D}$) as input and combines it with the feedback data (g_{d-1}) from the GRU model to measure depth-related information (c_d).

D. COA-based Hyperparameter Tuning

Finally, the COA optimally adjusts the hyperparameter values of the attention-based BiGRU approach [27]. This model was chosen for hyperparameter tuning due to its effective search space exploration and its ability to optimize model performance effectively. Coatis, or coatimundis, are small mammals of the Procyonidae family, known for their slender head, flexible nose, and long balancing tail. The COA mimics their natural behaviors for optimization. The COA is a population-based meta-heuristic method where coatis represent candidate solutions. The position of each coati, X_i, is initialized randomly in the search space using

$$X_i: \chi_{i,j} = lb_j + r \cdot (ub_j - lb_j),$$
$$i = 1,2,\dots,N,\ \ j = 1,2,\dots,m, \quad (8)$$

where lb_j and ub_j are the lower and upper bounds of the j^{th} decision variable, and r is a random number between 0 and 1. The population matrix X is formed as:

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix} = \begin{bmatrix} \chi_{1,1} & \cdots & \chi_{1,j} & \cdots & \chi_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ \chi_{i,1} & \cdots & \chi_{i,j} & \cdots & \chi_{i,m} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ \chi_{N,1} & \cdots & \chi_{N,j} & \cdots & \chi_{N,m} \end{bmatrix}_{N \times M} \quad (9)$$

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N \times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N \times 1}, \quad (10)$$

The performance of each coati is evaluated using the objective function F, as defined in (10). F represents the vector of attained values, with F_i depicting the function value for the i^{th} coati. The coati with the best objective function value is considered the optimal population member, and its performance is updated in each iteration.

1) Exploration Stage

The position of the optimum population member is considered the lizard's position. While some coatis climb the tree, others wait for the lizard to fall. The coati's position increase from the tree is modeled using:

$$X_i^{P1}: \chi_{i,j}^{P1} = \chi_{i,j} + r \cdot (Iguana_j - I \cdot x_{i,j}),$$
$$for\ i = 1,2,\dots,\left\lfloor \frac{N}{2} \right\rfloor\ and\ j = 1,2,\dots,m \quad (11)$$

Afterward, the lizard falls to the ground from an arbitrary location within the search space. Based on this position, coatis move out of the search space, as inspired by (12) and (13):

$$Iguana_j^G = lb_j + r \cdot (ub_j - lb_j), j = 1,2,\dots,m \quad (12)$$

$$X_i^{P1} I: x_{i,j}^{P1} = \begin{cases} x_{i,j} + r \cdot (\mathrm{I}guana_j^G - I \cdot x_{i,j}), & F_{Iguana^G} < F_i, \\ x_{i,j} + r \cdot (x_{i,j} - Iguana_j^G), & else, \end{cases}$$
$$\text{for } i = \left\lfloor \frac{N}{2} \right\rfloor + 1, \left\lfloor \frac{N}{2} \right\rfloor + 2, \dots, N \text{ and } j = 1,2,\dots,m \quad (13)$$

A new position is calculated for each coati if it improves the objective value. If not, the coati remains in its previous position. The update is performed for $i = 1,2,\dots,N$, as defined in:

$$X_i = \begin{cases} X_i^{P1}, & F_i^{P1} < F_i, \\ X_i, & else. \end{cases} \quad (14)$$

Let X_i^{P1} represent the new position of the i^{th} coati, with $\chi_{i,j}^{P1}$ as its j^{th} dimension and F_i^{P1} as its objective value. r is a random number between 0 and 1, and $Iguana$ denotes the best position in the search space. I is a randomly chosen integer from $\{1,2\}$, and $Iguana^G$ represents the lizard's ground position, with $\lfloor \cdot \rfloor$ denoting the floor function.

2) Exploitation Stage

In the secondary stage, coatis move to a safer position near their current location, simulating predator escape behavior and showcasing COA's exploitation ability. This is achieved by placing coatis near their current positions based on:

$$lb_j^{local} = \frac{lb_j}{t}, ub_j^{local} = \frac{ub_j}{t}, where\ t = 1,2,\dots,T \quad (15)$$

$$X_i^{P2}: \chi_{i,j}^{P2} = \chi_{i,j} + (1 - 2r) \cdot \left(lb_j^{local} + r \cdot \left(ub_j^{local} - lb_j^{local}\right)\right) \quad (16)$$
$$i = 1,2,\dots,N, j = 1,2,\dots,m,$$

The recently commutated position is suitable once it enhances the value of the main function that this condition emulates utilizing:

$$X_i = \begin{cases} X_i^{P2}, & if\ F_i^{P2} < F_i, \\ X_i, & else, \end{cases} \quad (17)$$

where X_i^{P2} represents the new position of the i^{th} coati in the secondary COA phase, with $\chi_{i,j}^{P2}$ as its j^{th} dimension and F_i^{P2} as its objective function value. Here, r is a random number, t is the iteration counter, and lb^{local} and ub^{local} are the local bounds for the j^{th} variable, while lb_j and ub_j are the global bounds.

The COA method calculates an FF to improve classification effectiveness, using a positive integer to indicate the efficiency of candidate solutions. The FF is determined by minimizing the classification error rate by:

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{No.of\ misclassified\ instances}{Total\ No.of\ instances} \times 100 \quad (18)$$

III. EXPERIMENTAL VALIDATION

The experimental analysis of the PIOFS-DLADC approach is determined by employing the WSN-DS database [28], which holds five classes and 18 features as represented in Table I. The PIOFS technique chose a set of 8 features (Is_CH,

Dist_To_CH, ADV_S, JOIN_S, SCH_S, Rank, DATA_S, Data_Sent_To_BS, Expaned Energy). The proposed technique was simulated using Python 3.6.5 on a PC with i5-8600k, 250GB SSD, GeForce 1050Ti 4GB, 16GB RAM, and 1TB HDD. The parameter settings were: learning rate: 0.01, activation: ReLU, epoch count: 50, dropout: 0.5, and batch size: 5.

TABLE I. DATASET DETAILS

Label	Class	Actual instances	Experiment
C1	Normal	340066	3000
C2	Blackhole	10049	3000
C3	Grayhole	14596	3000
C4	Flooding	3312	3000
C5	Scheduling Attacks	6638	3000
Total no. of instances		**374661**	**15000**

Table II presents a comprehensive comparison analysis of the PIOFS-DLADC method using $accu_y$, $sens_y$, $spec_y$, and F_{score} [29]. Models such as KNN with 96.40% $accu_y$, AdaBoost with 96.30%, and CNN+RNN with 96.14% performed well, while the PIOFS-DLADC model outperformed all models with an $accu_y$ of 96.78%, $sens_y$ of 93.35%, $spec_y$ of 92.02%, and an F_{score} of 97.98%.

TABLE II. COMPARISON OF THE PIOFS-DLADC APPROACH WITH OTHER METHODS [29, 30]

Methods	$Accu_y$	$Sens_y$	$Spec_y$	F_{Score}
RNN	96.50	76.89	86.20	87.52
CNN+RNN	96.14	91.17	91.20	91.69
AdaBoost	96.30	92.96	91.47	91.09
GB Model	94.23	91.95	89.55	92.43
XGBoost	95.91	92.75	90.14	90.70
KNN	96.40	92.99	91.20	90.79
KNN-PSO	96.47	92.01	91.21	92.59
PIOFS-DLADC	96.78	93.35	92.02	97.98

IV. CONCLUSION

This study introduced an innovative PIOFS-DLADC method for healthcare WSNs. Initially, the patient health data are preprocessed using one-hot encoding. The PIOFS method selects the most informative features from the sensor data, reducing dimensionality. An attention-based BiGRU captures long-term dependencies and assigns importance to features for accurate attack classification. Finally, the COA fine-tunes the model's hyperparameters, optimizing performance for attack detection and classification. The PIOFS-DLADC model was examined on the WSN-DS dataset. The performance validation of the PIOFS-DLADC model portrayed a superior accuracy of 96.78% over existing approaches. The limitations of the PIOFS-DLADC model include reliance on a single dataset and real-time system constraints. Future work could expand the dataset, integrate it with real-time systems, and incorporate multimodal data for better accuracy and scalability.

REFERENCES

[1] S. M. Naser, Y. H. Ali, and D. A. Obe, "Deep learning model for cyber-attacks detection method in wireless sensor networks," *Periodicals of Engineering and Natural Sciences*, vol. 10, no. 2, pp. 251–259, Apr. 2022.

[2] J. L. Webber *et al.*, "An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks," *Computers and Electrical Engineering*, vol. 111, Nov. 2023, Art. no. 108964, https://doi.org/10.1016/j.compeleceng.2023.108964.

[3] E. Jayabalan and R. Pugazendi, "Deep learning model-based detection of jamming attacks in low-power and lossy wireless networks," *Soft Computing*, vol. 26, no. 23, pp. 12893–12914, Dec. 2022, https://doi.org/10.1007/s00500-021-06111-7.

[4] M. Al-Hawawreh and M. S. Hossain, "A privacy-aware framework for detecting cyber attacks on internet of medical things systems using data fusion and quantum deep learning," *Information Fusion*, vol. 99, Nov. 2023, Art. no. 101889, https://doi.org/10.1016/j.inffus.2023.101889.

[5] B. Almaslukh, "Deep Learning and Entity Embedding-Based Intrusion Detection Model for Wireless Sensor Networks," *Computers, Materials & Continua*, vol. 69, no. 1, pp. 1343–1360, 2021, https://doi.org/10.32604/cmc.2021.017914.

[6] K. Hussain, Y. Xia, A. N. Onaizah, T. Manzoor, and K. Jalil, "Hybrid of WOA-ABC and proposed CNN for intrusion detection system in wireless sensor networks," *Optik*, vol. 271, Dec. 2022, Art. no. 170145, https://doi.org/10.1016/j.ijleo.2022.170145.

[7] Z. A. Khan, S. Amjad, F. Ahmed, A. M. Almasoud, M. Imran, and N. Javaid, "A Blockchain-Based Deep-Learning-Driven Architecture for Quality Routing in Wireless Sensor Networks," *IEEE Access*, vol. 11, pp. 31036–31051, 2023, https://doi.org/10.1109/ACCESS.2023.3259982.

[8] K. Khedhiri, D. Djabbour, and A. Cherif, "The Performance of Stable Zones Protocol for Heterogeneous Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15876–15881, Aug. 2024, https://doi.org/10.48084/etasr.7716.

[9] N. Gupta and B. B. Agarwal, "Suspicious Activity Classification in Classrooms using Deep Learning," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12226–12230, Dec. 2023, https://doi.org/10.48084/etasr.6228.

[10] K. Audah, N. K. Noordin, W. Hussein, M. F. B. A. Rasid, A. Sali, and A. Flah, "Maximizing DRL-based Energy Efficiency in IRS-NOMA using a DDPG Algorithm for the Next Generation of Wireless Communications," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14801–14810, Aug. 2024, https://doi.org/10.48084/etasr.7536.

[11] B. Raveendranadh and S. Tamilselvan, "An accurate attack detection framework based on exponential polynomial kernel-centered deep neural networks in the wireless sensor network," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 3, 2023, Art. no. e4726, https://doi.org/10.1002/ett.4726.

[12] C. A. Subasini, S. P. Karuppiah, A. Sheeba, and S. Padmakala, "Developing an attack detection framework for wireless sensor network-based healthcare applications using hybrid convolutional neural network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, 2021, Art. no. e4336, https://doi.org/10.1002/ett.4336.

[13] M. Dener, S. Al, and A. Orman, "STLGBM-DDS: An Efficient Data Balanced DoS Detection System for Wireless Sensor Networks on Big Data Environment," *IEEE Access*, vol. 10, pp. 92931–92945, 2022, https://doi.org/10.1109/ACCESS.2022.3202807.

[14] S. Karthic and S. M. Kumar, "Hybrid Optimized Deep Neural Network with Enhanced Conditional Random Field Based Intrusion Detection on Wireless Sensor Network," *Neural Processing Letters*, vol. 55, no. 1, pp. 459–479, Feb. 2023, https://doi.org/10.1007/s11063-022-10892-9.

[15] J. A. Santhi and T. V. Saradhi, "Attack detection in medical Internet of things using optimized deep learning: enhanced security in healthcare sector," *Data Technologies and Applications*, vol. 55, no. 5, pp. 682–714, Apr. 2021, https://doi.org/10.1108/DTA-10-2020-0239.

[16] S. Ben Atitallah, M. Driss, W. Boulila, and I. Almomani, "An Effective Detection and Classification Approach for DoS Attacks in Wireless Sensor Networks Using Deep Transfer Learning Models and Majority Voting," in *Advances in Computational Collective Intelligence*, 2022, pp. 180–192, https://doi.org/10.1007/978-3-031-16210-7_14.

[17] M. Kumar and J. Ali, "Adaptive Taylor-Sail Fish Optimization based deep Learning for Detection of Black Hole and Sybil Attack in Wireless Sensor Network," in *2023 International Conference on Sustainable*

Computing and Data Communication Systems (ICSCDS), Erode, India, Mar. 2023, pp. 1237–1244, https://doi.org/10.1109/ICSCDS56580.2023.10104946.

[18] Q. A. Al-Haija, C. D. McCurry, and S. Zein-Sabatto, "Intelligent Self-reliant Cyber-Attacks Detection and Classification System for IoT Communication Using Deep Convolutional Neural Network," in *Selected Papers from the 12th International Networking Conference*, 2021, pp. 100–116, https://doi.org/10.1007/978-3-030-64758-2_8.

[19] R. B. Kagade and S. Jayagopalan, "Optimization assisted deep learning based intrusion detection system in wireless sensor network with two-tier trust evaluation," *International Journal of Network Management*, vol. 32, no. 4, 2022, Art. no. e2196, https://doi.org/10.1002/nem.2196.

[20] K. Vaisakhkrishnan, G. Ashok, P. Mishra, and T. G. Kumar, "Guarding Digital Health: Deep Learning for Attack Detection in Medical IoT," *Procedia Computer Science*, vol. 235, pp. 2498–2507, Jan. 2024, https://doi.org/10.1016/j.procs.2024.04.235.

[21] G. R. Bhagwatrao and R. Lakshmanan, "Automated Patient Activity Identification in Cyber-physical Systems Using A Unique Deep Learning Approach and Multi-objective Optimization," *International Journal of Sensors, Wireless Communications and Control*, vol. 13, no. 5, pp. 339–352, Oct. 2023, https://doi.org/10.2174/0122103279274650231010053723.

[22] A. Pushpalatha, S. Pradeep, M. V. Pullarao, and S. Sankar, "Optimized memory augmented graph neural network-based DoS attacks detection in wireless sensor network," *Network: Computation in Neural Systems*, pp. 1–27, Aug. 2024, https://doi.org/10.1080/0954898X.2024.2392786.

[23] T. Thamaraimanalan and S. Ramalingam, "Hybrid Artificial Neural Network-based Grasshopper Optimization Algorithm for Anomaly Detection in Wireless Body Area Networks," *IETE Journal of Research*, vol. 70, no. 4, pp. 3738–3752, Apr. 2024, https://doi.org/10.1080/03772063.2024.2305845.

[24] M. K. Dahouda and I. Joe, "A Deep-Learned Embedding Technique for Categorical Features Encoding," *IEEE Access*, vol. 9, pp. 114381–114391, 2021, https://doi.org/10.1109/ACCESS.2021.3104357.

[25] T. A. Alghamadi and S. S. Alotaibi, "Internet of Things Enabled DDoS Attack Detection Using Pigeon Inspired Optimization Algorithm with Deep Learning Approach," *Computers, Materials and Continua*, vol. 80, no. 3, pp. 4047–4064, Sep. 2024, https://doi.org/10.32604/cmc.2024.052796.

[26] L. Zeng, W. Ren, and L. Shan, "Attention-based bidirectional gated recurrent unit neural networks for well logs prediction and lithology identification," *Neurocomputing*, vol. 414, pp. 153–171, Nov. 2020, https://doi.org/10.1016/j.neucom.2020.07.026.

[27] M. Dehghani, Z. Montazeri, E. Trojovská, and P. Trojovský, "Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems," *Knowledge-Based Systems*, vol. 259, Jan. 2023, Art. no. 110011, https://doi.org/10.1016/j.knosys.2022.110011.

[28] 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.

[29] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," *Journal of Big Data*, vol. 10, no. 1, Feb. 2023, Art. no. 17, https://doi.org/10.1186/s40537-023-00692-w.

[30] C. Murugesh and S. Murugan, "Moth Search Optimizer with Deep Learning Enabled Intrusion Detection System in Wireless Sensor Networks," *International Journal of Electrical and Electronics Engineering*, vol. Volume 10, Apr. 2023, https://doi.org/10.14445/23488379/IJEEE-V10I4P108.