IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 November 2023, accepted 17 November 2023, date of publication 20 November 2023,
date of current version 29 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3335124

RESEARCH ARTICLE

Red Kite Optimization Algorithm With Average Ensemble Model for Intrusion Detection for Secure IoT

FAHAD F. ALRUWAILI[1], MASHAEL M. ASIRI[2], FATMA S. ALRAYES[3], SUMAYH S. ALJAMEEL[4], AHMED S. SALAMA[5], AND ANWER MUSTAFA HILAL[6]

[1]Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra 11961, Saudi Arabia
[2]Department of Computer Science, College of Science and Art at Mahayil, King Khalid University, Abha 61421, Saudi Arabia
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[4]Saudi Aramco Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[5]Department of Electrical Engineering, Faculty of Engineering and Technology, Future University in Egypt, New Cairo 11845, Egypt
[6]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

Corresponding authors: Anwer Mustafa Hilal (a.hilal@psau.edu.sa) and Ahmed S. Salama (a.salama@fue.edu.eg)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project under grant number (RGP.2/65/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. The 1st author would like to thank the Deanship of Scientific Research at Shaqra University for supporting this research. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

ABSTRACT The Internet of Things (IoT) based Wireless Sensor Networks (WSNs) contain interconnected autonomous sensor nodes (SN), which wirelessly communicate with each other and the wider internet structure. Intrusion detection to secure IoT-based WSNs is critical for identifying and responding to great security attacks and threats that can cooperate with the integrity, availability, and privacy of the network and its data. Machine learning (ML) algorithms are deployed for detecting difficult patterns and subtle anomalies in IoT data. Artificial intelligence (AI) driven methods are learned and adapted from novel data for improving detection accuracy over time. In this article, we introduce a Red Kite Optimization Algorithm with an Average Ensemble Model for Intrusion Detection (RKOA-AEID) technique for Secure IoT-based WSN. The purpose of the RKOA-AEID methodology is to accomplish security solutions for IoT-assisted WSNs. To accomplish this, the RKOA-AEID technique performs pre-processing to scale the input data using min-max normalization. In addition, the RKOA-AEID technique performs an RKOA-based feature selection approach to elect an optimum set of features. For intrusion detection, an average ensemble learning model is used. Finally, the Lévy-fight chaotic whale optimization Algorithm (LCWOA) can be executed for the optimum hyperparameter chosen for the ensemble models. The performance evaluation of the RKOA-AEID algorithm can be tested on the benchmark WSN-DS dataset. The extensive experimental outcomes stated the higher outcome of the RKOA-AEID algorithm with other approaches with an improved accuracy of 98.94%.

INDEX TERMS The Internet of Things, security, red kite optimization algorithm, deep learning, feature selection.

I. INTRODUCTION

With this enormous and progressive development of Internet technology, giving security to Internet of Things (IoTs) based wireless sensor networks (WSNs) is extremely important as these networks are usually employed in inaccessible landscapes and manage various security attacks [1]. Applications depend on IoT and WSN is revolutionizing a person's life because it can support day-to-day activities. IoT and WSN are possible for making the earth a smart planet. Various IoT network designs are affected by WSNs. The confusion takes place from the resemblance and difference of the

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

2 conditions [2]. It contains transmission capabilities, memory, and limited processing; both networks can be efficient for real-time applications like border region monitoring that requires round-the-clock surveillance [3]. Any sensors can fail or stop functioning in an insecure condition but human support could not have potential [4]. A network has been simply reconfigured by employing robust and energy-efficient routing approaches [5]. IoT and WSN can be prone to selective forwarding, wormhole, grayhole, sinkhole, DoS, blackhole, hello flood attacks, and Sybil, etc. due to their complexities.

In the meantime, Intrusion detection can resolve these issues and ensure network data security [6]. Intrusion detection can be an effective technique, which attempts to alert and identify the attempted intrusions into the system or network [7]. However, the number of online businesses across traffic is increasing every day and therefore, the network features have also become highly difficult thus carrying further challenges for intrusion detection [8]. ML techniques can be primarily employed to produce accurate techniques particularly developed for prediction, classification, and clustering. In this study, ML performs an essential role in IDSs in WSN [9]. Certain security mechanisms were designed for WSNs in conventional analysis. Nevertheless, IDS should be utilized in critical security applications for comprehensive defence. In WSN, the IDS for current efforts could not be directly employed due to resource limits [10]. Hence, various methods are introduced for identifying intrusions in WSNs. The majority of them can be targeted at specific attacks, and in this case, ML-based IDS have determined for WSN utilizing IDS databases.

In this article, we introduce a Red Kite Optimization Algorithm with an Average Ensemble Model for Intrusion Detection (RKOA-AEID) technique for Secure IoT-based WSN. The RKOA-AEID technique performs pre-processing to scale the input data using min-max normalization. In addition, the RKOA-AEID technique performs an RKOA-based feature selection approach to elect an optimum set of features. For intrusion detection, an average ensemble learning model is used. Finally, the Lévy-fight chaotic whale optimization Algorithm (LCWOA) can be executed for the optimum hyperparameter chosen for the ensemble models. The performance evaluation of the RKOA-AEID technique is tested on benchmark IDS datasets. In short, the key contributions are given as follows.

- Develop an RKOA-AIED technique for intrusion detection in IoT-assisted WSNs. To the best of our knowledge, the RKOA-AIED technique never existed in the literature.
- Design RKOA-based FS approach, which helps to determine an optimal set of features, decreasing high dimensionality and considerably improving the accuracy of the intrusion detection model.
- Employs an average ensemble learning model which combines the prediction results of many baseline models for accurate and robust classification. This approach can enhance the reliability of intrusion detection by reducing false positives and negatives.
- To further enhance the ensemble models' performance, the article LCWOA is for selecting optimal hyperparameters.

II. RELATED WORKS

Ramana et al. [11] proposed a Whale Optimized GRU-IDS (WOGRU-IDS) for WSN-IoT network. In the presented method, the WOA is used to fine-tune the hyperparameter of the deep LSTM. The authors [1] developed a Hybrid Muddy Soil Fish Optimizer-based Energy Aware Routing System (HMSFO-EARS) for IoT-aided WSNs. This model focuses mainly on the detection of an optimum route for the transmission of data in IoT-aided WSNs. The algorithm incorporates the MSFO method with the Adaptive β-Hill Climbing (ABHC) concept. Furthermore, this approach develops a fitness function (FF) for reducing energy consumption and increasing lifespan. Rajan and Naganathan [12] devised a Trusted Anonymous Lightweight Attacker Detection (TALAD) system. The proposed method constructs a routing path to the cloud with an extremely trusted node, depending on the chosen path length limit.

Alkhliwi [13] presents an energy-effective cluster-based routing mechanism with secured IDS in HWSN named EECRP-SID. In the initial stage, the T2FC protocol with 2 input parameters can be employed for the CHS model. In the next phase, the salp swarm optimizer (SSO) algorithm was used for the optimum selection of paths. At last, robust IDS using LSTM is implemented on the CHs. Yao et al. [14] suggest a technique based on DCNN and principal component analysis (PCA) for traffic anomaly detection of DoS in WSN, depending on the WSN vulnerability to attacks and the restricted memory capacity of their devices. The presented algorithm has a more effective capability of feature extraction and lightweight structure that could successfully identify network abnormal traffic in WSN with restricted memory capacity.

Maheswari and Karthika [15] proposed the Multi-tiered Intrusion Detection (MDIT) with a hybrid DL mechanism for better recognition performance in WSN; spotted hyena optimizer (SHO) and LSTM are studied to effectively design IDS. The authors [16] designed a Secure DL (SecDL) technique for cluster-based WSN-IoT networks. A One Time-PRESENT (OT-PRESENT) cryptography system can be developed for accomplishing high-level security. A Fitted DNN (Co-FitDNN) is introduced for optimum route selection. Punithavathi et al. [6] introduce a multiobjective MRFO-based node localization with IDS (MOMRFO-NLID) for WSNs. The proposed method includes two main steps such as optimum Siamese Neural Network (OSNN) based IDS and MRFO based NL. The OSNN approach includes the hyperparameter tuning of the classical SNN with the help of the MRFO technique.

Despite the benefits of existing IDS models available in the literature, a considerable research gap exists which requires

the incorporation of FS, ensemble classification, and hyperparameter tuning processes. While IoT devices continue to proliferate, their resource-limited and dynamic characteristics of the IoT environment pose critical challenges for intrusion detection. The existing models often overlook the crucial step of FS tailored to IoT data, which can lead to suboptimal detection models. Besides, the significant merits of ensemble classification in enhancing accuracy and robustness need to be explored in the context of IoT-based WSNs. Finally, hyperparameter tuning is important to optimize the performance of the detection models but remains an underemphasized area. Bridging this research gap is imperative to develop efficient and resource-aware intrusion detection systems that are well-suited for the evolving landscape of IoT-based WSNs, ultimately bolstering their security and resilience against emerging threats.

III. THE PROPOSED MODEL

In this article, we have focused on the design and development of the RKOA-AEID technique for secure IoT-based WSNs. The goal of the RKOA-AEID technique is to accomplish security solutions for IoT-assisted WSNs. To accomplish this, the RKOA-AEID technique performs different stages of operations namely data pre-processing, RKOA-based feature selection, and LCWOA-based hyperparameter selection. Fig. 1 depicts the workflow of the RKOA-AEID algorithm.

A. DATA NORMALIZATION

The Min-Max normalized approach was employed to scale the data values from a set range (0 to 1) [17]. Primarily, the Min-Max normalized approach subtracts the minimal value in data point X and divides it by its range. The equation of the Min-Max normalized system X_norm is represented in Eq. (1).

$$X\_norm = \frac{(X - X\_\min)}{X\_\max - X\_\min} \tag{1}$$

In this case, the estimation of normalized can be executed only for the training set, and the validation and testing sets are unknown.

B. FEATURE SELECTION USING RKOA

In this work, the RKOA can be used for the optimum choice of features. RKOA is a new meta-heuristic technique simulated by red kites (RKs) social life [18]. The RKs generally create nests near woods and lakes regions that are correct for hunting. For obtaining better outcomes, the meta-heuristic technique must initially navigate the problem searching space fit to prevent trapping in the local optimum. After it slowly moves from exploration to exploitation stages and uses the optimum performance from the final iterations. RKOA takes 3 important phases that are defined:

The first phase—a primary position of birds: During this phase, based on Eq. (2), the RK's position is initialized

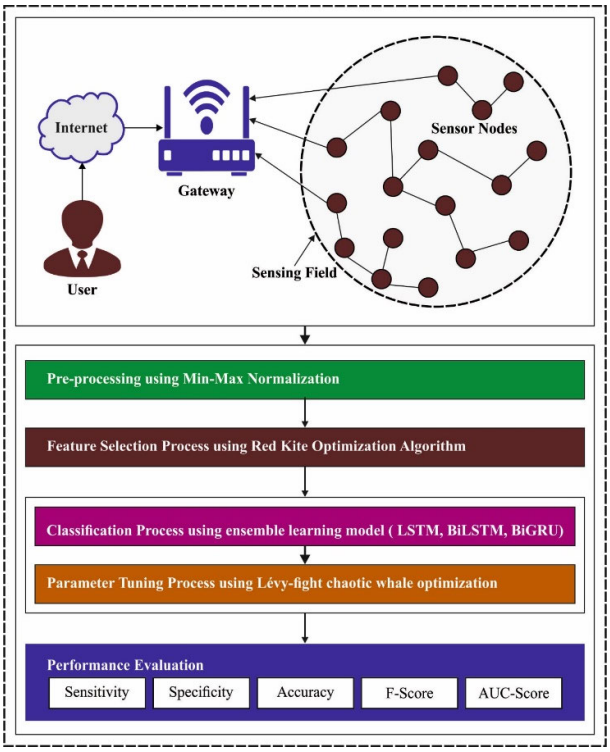

FIGURE 1. Workflow of RKOA-AEID system.

arbitrarily as,

$$Pos_{i,j}(t) = lb + rand \times (ub - lb), i = 1, 2, \ldots, n \text{ and } j = 1, 2, \ldots, d \tag{2}$$

whereas $Pos_{i,j}(t)$ is i^{th} position of RKs at iteration t, lb, and ub defines the lower as well as upper boundaries, correspondingly, n represents the population size, d demonstrates the dimension of the problem, and *rand* implies the random number from zero and one.

The second phase— leader selection: Choosing the leader is acquired based on Eq. (3):

$$\overrightarrow{Best(t)} = \overrightarrow{Pos_i(t)} \text{ if } f_i(t) < f_{best}(t) \tag{3}$$

In which, $Best(t)$ implies the position of the optimum bird from the iteration t, $Pos(t)$ indicates the position of i^{th} RK from the iteration t, $f_i(t)$ denotes the value of the bird estimation function from the iteration t, and $f_{best}(t)$ implies the value of estimation function of best bird from the iteration.

The third phase—the bird's movements: It can be assumed that RKs need to slowly move from exploration to exploitation stages by assuming a reducing co-efficient (D) based on Eq. (4).

$$D = \left(exp\left(\frac{t}{t\_\max}\right) - \frac{t}{t\_\max} \right)^{-10} \tag{4}$$

In which, t stands for the present iteration and $t\_\max$ signifies the maximal iteration.

The birds upgrade their positions by Eqs. (5) and (6):

$$\overrightarrow{pos_i^{new}(t+1)} = \overrightarrow{Pos_i(t)} + \overrightarrow{P_{mi}(t+1)} \tag{5}$$

FIGURE 2. Steps involved in RKOA.

$$\overrightarrow{P_{mi}(t+1)} = D(t) \times \overrightarrow{P_{mi}(t)} + \overrightarrow{SC(t)} \odot \left(\overrightarrow{Pos_{rws}(t)} - \overrightarrow{Pos_i(t)}\right) + \overrightarrow{UC(t)} \odot \left(\overrightarrow{Best(t)} - \overrightarrow{Pos_i(t)}\right) \quad (6)$$

In which, $Pos_{rws}(t)$ denotes the bird position chosen by the roulette wheel from iteration t, $pos_i^{new}(t+1)$ refers to the novel position of birds, and SC and UC represent the arbitrary vectors of social and individual modules, correspondingly. Afterwards, in the upgrade position, it is essential to verify the searching space boundaries; it could be led to employ in Eq. (7),

$$\overrightarrow{pos_i^{new}(t+1)} = \max\left(\min\left(\overrightarrow{pos_i^{new}(t+1)} + ub\right), lb\right) \quad (7)$$

A novel temporary position is exchanged once the estimation function is enhanced. Then, $Pos_i(t+1)$ is equivalent to $s_i^{new}(t+1)$. As noted, SC and UC denote the arbitrary vectors of social and individual modules, it exemplifies the voice of unity and danger of all the birds and it can be accomplished based on the following relation:

$$\begin{cases} \overrightarrow{SC(t+1)} = \vec{r}_1 \\ \overrightarrow{UC(t+1)} = \vec{r}_2 \end{cases} \quad if\ rand \le 0.5$$
$$\begin{cases} \overrightarrow{SC(t+1)} = \vec{r}_3 \\ \overrightarrow{UC(t+1)} = \vec{r}_1 \end{cases} \quad if\ Otherwise \quad (8)$$

Which, $r_1 \rightarrow$ denotes the arbitrary vector from the range of one and two; $r_2 \rightarrow$ implies the arbitrary vector from the range of one and three, and $r_3 \rightarrow$ stands for the arbitrary vector from the range of zero and one.

In the RKOA, according to the present position of all the birds, the neighbour position is arbitrarily selected using a roulette wheel, and the optimum solution is found still. During the initial iterations, the value of $D(t)$ is around one to search and explore novel spaces. As it moves depending on an individual element, the RK searches novel spaces depending on its position and arbitrarily chosen neighbour. Slowly, this technique moves from the primary to intermediate iterations, and the co-efficient $D(t)$ reduces to achieve balance among the exploration as well as exploitation phases. During the last iterations, this co-efficient prefers zero and the method exploits the search for optimum performance among the attained optimum performances. Fig. 2 represents the steps involved in RKOA.

In the RKOA system, the objectives are combined as a single objective equation for presenting weighted recognition of all the objective importance [19]. During this case, it is implementing an FF to integrate both objectives of FS as depicted in Eq. (9).

$$Fitness(X) = \alpha \cdot E(X) + \beta * \left(1 - \frac{|R|}{|N|}\right) \quad (9)$$

whereas, $Fitness(X)$ defines the fitness value of subset X, $E(X)$ demonstrates the classifier error rate by employing the FS from the X subset, $|R|$ and $|N|$ illustrate the count of FSs and the count of new features from the database correspondingly, α and β denotes the weighted of classifier error and rate of decrease, $\alpha \in [0, 1]$ and $\beta = (1-\alpha)$.

C. INTRUSION DETECTION USING AVERAGE ENSEMBLE MODEL

For intrusion detection, an average ensemble process is applied. The averaging method is one of the simplest ways to combine the prediction of multiple models [20]. It is a popular ensemble algorithm where all the models are separately trained, and the averaging method linearly incorporates the prediction of methods by averaging them to generate the last forecast. This method is easy to implement without any need for further training on a large number of individual forecasts. The last prediction outcomes are commonly defined by a majority vote on the prediction of the classifier and can be represented as hard voting.

$$y_i = mode\{c_1, c_2, \ldots, c_k\} \quad (10)$$

Hard voting is simple to apply and achieves optimum outcomes than the baseline classifier, however, it could not consider the probability of minor forecast class. For instance, in three classifiers with prediction probability of (63, 0.49, and 0.48), hard voting yields (0, 0, 1) as an equivalent prediction of the probability. In such cases, the last hard vote prediction of the 3 classifiers' votes will be 0. Therefore, soft voting assumes the probability values of all the classifiers instead of the prediction label.

$$y = argmax_i \frac{1}{n} \sum_{j=1}^{X} w_{ij} \quad (11)$$

In Eq. (11), W_{ij} refers to the probability of i^{th} class labels of the j^{th} classifier. An improved version of voting is to weigh all the classifiers proportional to their outcome on the validation set.

1) LSTM MODEL

LSTM networks are a form of RNN primarily intended to decide the vanishing gradient problem of RNNs regarding long sequences [21]. An LSTM network design contains a layer of LSTM units and then a typical feedforward network. In a common approach, an LSTM unit functions as follows: assume x_t exists the present input at time t, the output of the input gate as:

$$i_t = \sigma\left(W_i^x x_t + W_i^h h_{t-1} + b_i\right), \tag{12}$$

In which, W_i^x and W_i^h denote the weighted matrices, h_{t-1} implies the preceding hidden layer (HL) of the unit, and b_i stands for the bias vector. The function $\sigma(x) \in (0, 1)$ defines the sigmoid function deployed to the gate. Also, the outcome of forgetting gate f_t is calculated as

$$f_t = \sigma\left(W_f^x x_t + W_f^h h_{t-1} + b_f\right). \tag{13}$$

Lastly, the resultants of output gate o_t and cell state c_t as,

$$c_t = i_t \odot \tanh\left(W_c^x x_t + W_c^h h_{t-1} + b_c\right) + c_{t-1}, \tag{14}$$

$$O_t = \sigma\left(W_o^x x_t + W_o^h h_{t-1} + b_o\right), \tag{15}$$

$$h_t = O_t \odot \tanh\left(c_t\right), \tag{16}$$

whereas $\odot$ refers to the Hadamard product.

2) BiLSTM MODEL

A BiLSTM contains 2 parallel LSTM layers are forward as well as backward directions. While the input has been handled twice, BiLSTM extracts more data from the input. So, increasing contextual data to create optimum forecasts than LSTMs. The BiLSTM structure contains 2 LSTM layers, maintaining previous and forthcoming context at every time of the sequences. The outcomes of all the LSTMs can be integrated depending on the following formula:

$$y_t = W_{\vec{h}y}\vec{h}_t + W_{\overleftarrow{h}y}\overleftarrow{h}_t + b_{y'} \tag{17}$$

In which, $\vec{h}_t$ and $\overleftarrow{h}_t$ represent the outcomes of forward and backward LSTMs.

3) BiGRU MODEL

The BiGRU network implemented in this case integrates forward as well as backward GRU neural networks [22]. The HLs of forward and backward GRU are defined as $\vec{h}_t$ and $\overleftarrow{h}_t$ correspondingly. To provide timestep t, the input is x_t=$(x_1, x_2, \ldots, x_n) \in \mathbb{R}^{n\times d}$. The forward and backward HLs are $\vec{h}_t \in \mathbb{R}^{n\times h}$ and $\overleftarrow{h}_t \in \mathbb{R}^{n\times h}$ correspondingly. h denotes the hidden unit counts.

$$\vec{h}_t = GRU_{fwd}\left(x_t, \vec{h}_{t-1}\right) \tag{18}$$

$$\overleftarrow{h}_t = GRU_{bwd}\left(x_t, \overleftarrow{h}_{t+1}\right) \tag{19}$$

$$h_t = W^T\vec{h}_t + W^V\overleftarrow{h}_t \tag{20}$$

$$o_t = \left(W^o h_t\right) \tag{21}$$

In which, x_t represents the input of timestep t, $\vec{h}_t$ defines the HL of forward GRU at timestep t, and $\overleftarrow{h}_t$ denotes the HL of backward GRU at timestep t. W^T and W^V signify the weighted matrices equivalent to forward HL $\vec{h}_t$ and backward HL $\overleftarrow{h}_t$ from the BiGRU, correspondingly. W^o indicates the weight among the HL and output layers. At last, the BiGRU outcome is sent to the classifier for classification as:

$$y_t = \sigma\left(W^t + b_t\right) \tag{22}$$

whereas, σ stands for the logistic sigmoid function. W^t and b_t denote the weighted matrix and bias from the resultant layer, correspondingly.

D. PARAMETER TUNING USING LCWOA

For the hyperparameter selection process of the DL models, the LCWOA is applied. The hyperparameters tuned by the LCWOA are given as follows: learning rate, number of epochs, and batch size. WOA is based on the performance of whales, comprising encircling prey bubble-net attacking, and searching for prey [23]. WOA is unable to carry out its maximum possible to find the global best solution despite having a good convergence rate that directly affects its computational accuracy. Lévy fight (LF) is added into the exploration stage, resulting in occasional huge jumps and frequent small movements to widen the exploration zone and increase overall exploration abilities. An LF can dramatically increase the diversification and intensification of the WOA leading to improved search capability and avoiding local minimum. Besides this, using a chaotic map may have promising impacts on the WOA convergence rate since it can encourage chaos from the possible place that is only predictable for the primary time and stochastic for a long time. The procedure of chaotic map from the WOA control parameter $[A, C, p, \ell]$ assists in accelerating convergence with better searching capability.

The A and C parameters define the shrinking circle method as allocated with $c(0)$ chaotic mapping instead of the random parameter 'r' as follows:

$$A = 2ac\,(t) - a \tag{23}$$

$$C = 2c\,(t) \tag{24}$$

The parameter 'ℓ' that defines the spiral upgrading position of humpback whales is allocated by $c(t)$ chaotic map as

$$X_i\,(t+1) = L \cdot e^{bc(t)}\cos\left(2\pi c\,(t)\right) + X^*\,(t) \tag{25}$$

Chaotic map c (t) replaces p probability of selecting the shrinking circle mode or spiral mode for updating whale location in all the iterations. The study suggested that the LF trajectory enhances the balance between the exploration as well as exploitation stages. LF can be used to adjust the whale's position as follows:

$$X_i(t+1) = X_i(t) + \mu sign\ r_1 - 1/2].L^{\acute{e}}evy(y) \tag{26}$$

In Eq. (26), $X(t)$ characterizes i^{th} whale location at $t^{het\ th}$ iteration, r_1 signifies a random value range within [0,1],

TABLE 1. Description of database.

Class	No. of Instances
Normal	340066
Blackhole	10049
Grayhole	14596
Flooding	3312
Scheduling Attacks	6638
Total Number of Instances	374661

and μ shows the uniform distribution arbitrary integer. The stochastic random walking approach helps the WOA to ensure that the searching agent would efficiently explore the searching region, as its step length is considerably higher in the long run, which removes local minimal.

The LCWOA approach grows an FF for achieving the best classifier results. It explains a positive integer for exemplifying the good outcome of candidate performances. During this case, the minimized classifier rate of errors can be supposed to be FF, as expressed in Eq. (27).

$$\begin{aligned} fitness\,(x_i) &= Classifier\ Error\ Rate\,(x_i) \\ &= \frac{No.\ of\ misclassified\ instances}{Total\ no.\ of\ instances} * 100 \end{aligned} \quad (27)$$

IV. RESULTS AND DISCUSSION

The performance evaluation of the RKOA-AEID technique is tested on the WSN-DS database [24]. The dataset comprises 374661 instances with 5 classes as depicted in Table 1. From the available 18 features, the RKOA has selected 11 features. For experimental validation, we have used 80:20 and 70:30 of the training/testing dataset. It is a specialized dataset for WSN that was constructed to classify four types of DoS attacks. The considered attacks are Blackhole, Grayhole, Flooding, and Scheduling attacks. The data were collected using NS-2. In addition to including normal behaviour, it was also able to collect 374661 records containing the signatures of these four attacks. The dataset contains normal and malicious network traffic.

In Fig. 3, the confusion matrices show the attack detection results of the RKOA-AEID technique. The figure highlighted that the RKOA-AEID technique attained proper identification of different kinds of attacks.

The attack detection results of the RKOA-AEID technique are tested with 80:20 of TR set/TS set as depicted in Table 2 and Fig. 4. The results exemplify that the RKOA-AEID technique is recognized in 5 classes. On 80% of the TR set, the RKOA-AEID method offers average $accu_y$, $sens_y$, $spec_y$, F_{score}, and AUC_{score} of 98.94%, 75.33%, 96.45%, 79.52%, and 85.89% respectively. Also, on 20% of TS set, the RKOA-AEID approach achieves average $accu_y$, $sens_y$, $spec_y$, F_{score}, and AUC_{score} of 98.92%, 74.60%, 96.37%, 78.76%, and 85.48% correspondingly.

The attack detection outcomes of the RKOA-AEID methodology are tested with 70:30 of TR set/TS set as represented in Table 3 and Fig. 5. The outcome illustrated that

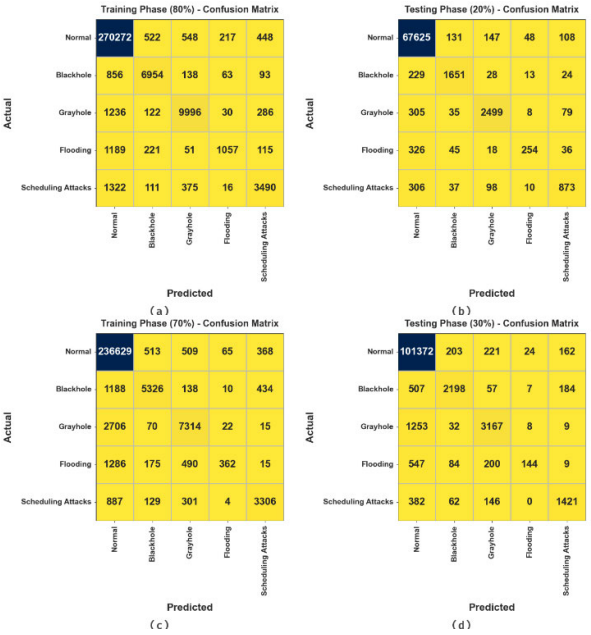

FIGURE 3. Confusion matrices of (a-b) 80:20 of TR set/TS set and (c-d) 70:30 of TR set/TS set.

TABLE 2. Attack detection of RKOA-AEID algorithm on 80:20 of TR set/TS set.

Class	$Accu_y$	$Sens_y$	$Spec_y$	F_{Score}	AUC_{Score}
TR set (80%)					
Normal	97.89	99.36	83.40	98.84	91.38
Blackhole	99.29	85.81	99.67	86.74	92.74
Grayhole	99.07	85.66	99.61	87.77	92.63
Flooding	99.37	40.14	99.89	52.64	70.02
Scheduling Attacks	99.08	65.68	99.68	71.62	82.68
Average	98.94	75.33	96.45	79.52	85.89
TS set (20%)					
Normal	97.86	99.36	83.04	98.83	91.20
Blackhole	99.28	84.88	99.66	85.90	92.27
Grayhole	99.04	85.41	99.60	87.44	92.50
Flooding	99.33	37.41	99.89	50.20	68.65
Scheduling Attacks	99.07	65.94	99.66	71.44	82.80
Average	98.92	74.60	96.37	78.76	85.48

the RKOA-AEID algorithm recognized on 5 classes. On 70% of the TR set, the RKOA-AEID algorithm gains average $accu_y$, $sens_y$, $spec_y$, F_{score}, and AUC_{score} of 98.58%, 66.73%, 94.73%, 71.47%, and 80.73% correspondingly. Afterwards, on 30% of TS set, the RKOA-AEID method achieves average $accu_y$, $sens_y$, $spec_y$, F_{score}, and AUC_{score} of 98.54%, 66%, 94.58%, 70.82%, and 80.29% correspondingly.

Fig. 6 illustrates the training accuracy TR_accu_y and VL_accu_y of the RKOA-AEID algorithm on 80:20 of the TR set/TS set. The TL_accu_y is defined by the evaluation of the RKOA-AEID methodology on the TR dataset whereas the VL_accu_y is calculated by assessing the performance on a separate testing dataset. The outcome depicts that TR_accu_y and VL_accu_y upsurge with an increase in epochs.

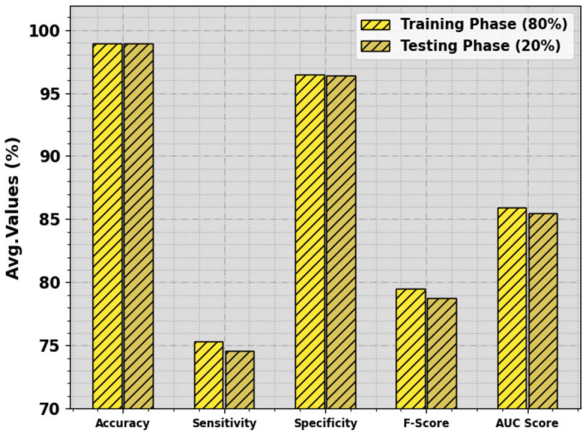

FIGURE 4. Average of RKOA-AEID algorithm on 80:20 of TR set/TS set.

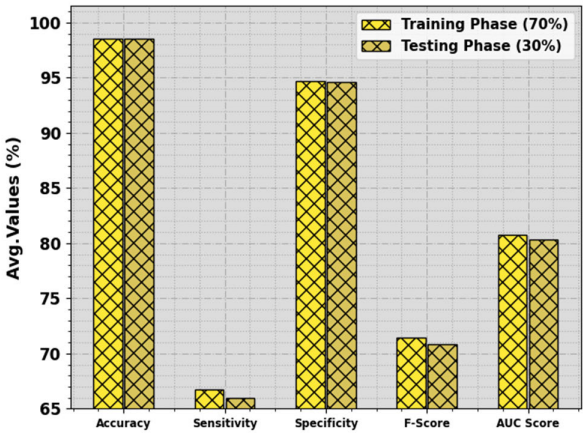

FIGURE 5. Average of RKOA-AEID algorithm on 70:30 of TR set/TS set.

TABLE 3. Attack detection of RKOA-AEID algorithm on 70:30 of TR set/TS set.

Class	$Accu_y$	$Sens_y$	$Spec_y$	F_{Score}	AUC_{Score}
TR set (70%)					
Normal	97.13	99.39	74.91	98.44	87.15
Blackhole	98.99	75.06	99.65	80.04	87.35
Grayhole	98.38	72.22	99.43	77.48	85.83
Flooding	99.21	15.55	99.96	25.94	57.76
Scheduling Attacks	99.18	71.45	99.68	75.44	85.56
Average	98.58	66.73	94.73	71.47	80.73
TS set (30%)					
Normal	97.06	99.40	74.19	98.40	86.79
Blackhole	98.99	74.43	99.65	79.46	87.04
Grayhole	98.29	70.87	99.42	76.68	85.14
Flooding	99.22	14.63	99.96	24.68	57.30
Scheduling Attacks	99.15	70.66	99.67	74.87	85.17
Average	98.54	66.00	94.58	70.82	80.29

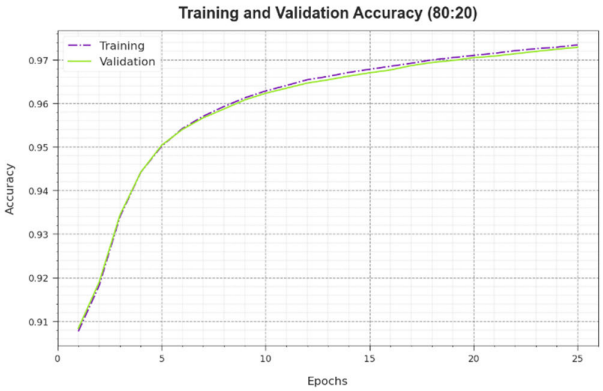

FIGURE 6. $Accu_y$ curve of RKOA-AEID algorithm on 80:20 of TR set/TS set.

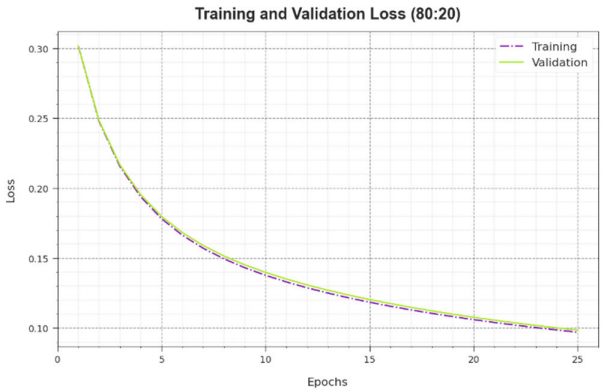

FIGURE 7. Loss curve of RKOA-AEID algorithm on 80:20 of TR set/TS set.

Accordingly, the performance of the RKOA-AEID methodology obtains improvement on the TR and TS database with a higher number of epochs.

In Fig. 7, the *TR_loss* and *VR_loss* results of the RKOA-AEID system on 80:20 of the TR set/TS set are exposed. The *TR_loss* defines the error among the predictive outcome and original values on the TR data. The *VR_loss* represents the measure of the performance of the RKOA-AEID system on individual validation data. The results indicate that the *TR_loss* and *VR_loss* tend to reduce with rising epochs. It portrayed the enhanced performance of the RKOA-AEID approach and its ability to generate accurate classification. The lesser value of *TR_loss* and *VR_loss* establishes the greater outcome of the RKOA-AEID technique on capturing patterns and relationships.

A comprehensive precision-recall (PR) examination of the RKOA-AEID approach is portrayed on 80:20 of the TR set/TS set in Fig. 8. The outcome values defined that the RKOA-AEID method outcomes in greater PR values. Afterwards, it can be obvious that the RKOA-AEID methodology attains better PR outcomes in 5 classes.

In Fig. 9, a ROC curve of the RKOA-AEID methodology is defined on 80:20 of the TR set/TS set. The outcome values referred that the RKOA-AEID algorithm has led to greater values of ROC. Next, it can be apparent that the RKOA-AEID approach obtains maximal ROC outcomes in 5 classes.

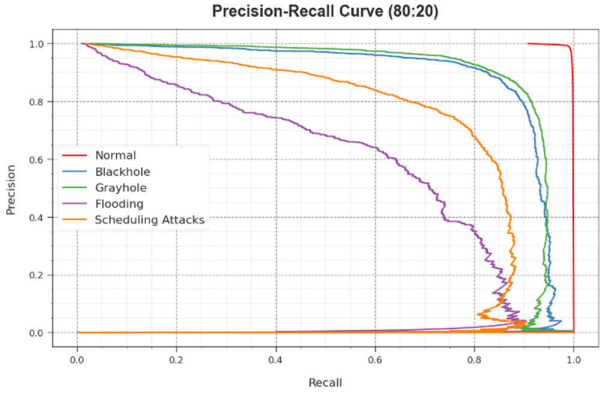

FIGURE 8. PR curve of RKOA-AEID algorithm on 80:20 of TR set/TS set.

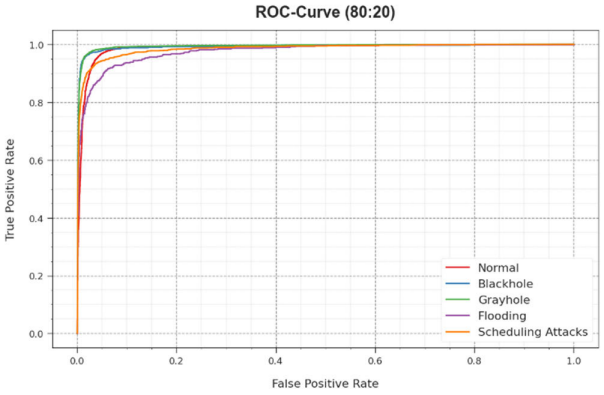

FIGURE 9. ROC curve of RKOA-AEID algorithm on 80:20 of TR set/TS set.

TABLE 4. Comparative outcome of RKOA-AEID algorithm with other methods [25], [26], [27].

Methods	$Accu_y$	$Sens_y$	$Spec_y$	F_{Score}
RKOA-AEID	98.94	75.33	96.45	79.52
AdaBoost	95.69	69.22	95.00	76.13
GB	94.58	71.03	94.09	71.92
XGBoost	96.83	71.51	94.43	71.01
KNN-AOA	97.20	70.16	96.04	73.85
KNN-PSO	92.89	71.30	95.08	70.48

The outcomes of the RKOA-AEID algorithm are compared with other classifiers in Table 4 and Fig. 10 [25], [26], [27]. The comparison outcomes stated that the RKOA-AEID system reported effectual outcomes over other models. Based on $accu_y$, the RKOA-AEID technique offers an increasing $accu_y$ of 98.94% while the Adaboost, GB, XGBoost, KNN-AOA, and KNN-PSO models obtain decreasing $accu_y$ values of 95.69%, 94.58%, 96.83%, 97.20%, and 92.89% respectively. Also, based on $sens_y$, the RKOA-AEID approach attains a higher $sens_y$ of 75.33% while the Adaboost, GB, XGBoost, KNN-AOA, and KNN-PSO approaches attain lesser $sens_y$ values of 69.22%, 71.03%, 71.51%, 70.16%, and 71.30% correspondingly. Next to that, concerning F_{score}, the RKOA-AEID algorithm achieves enhancing F_{score} of

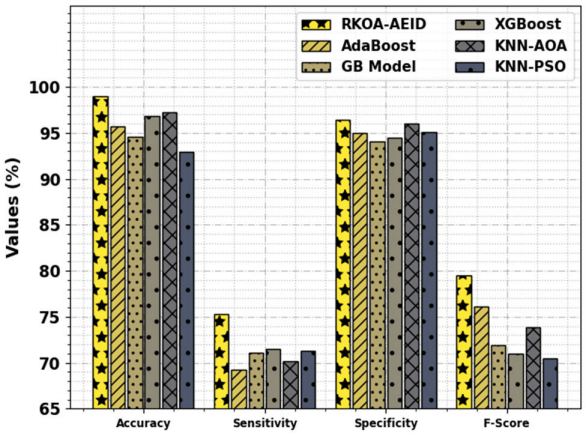

FIGURE 10. Comparative outcome of RKOA-AEID algorithm with other methods.

TABLE 5. CT outcome of RKOA-AEID algorithm with other METHODS [25], [26], [27].

Methods	Computational Time (sec)
RKOA-AEID	1.97
AdaBoost	3.52
GB Model	2.57
XGBoost	3.67
KNN-AOA	4.77
KNN-PSO	5.60

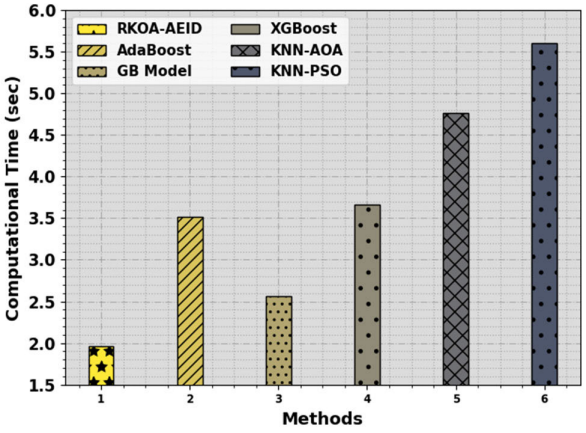

FIGURE 11. CT outcome of RKOA-AEID algorithm with other methodologies.

79.52% while the Adaboost, GB, XGBoost, KNN-AOA, and KNN-PSO methodologies gain minimal F_{score} values of 76.13%, 71.92%, 71.01%, 73.85%, and 70.48% correspondingly.

Finally, the comparative computation time (CT) results of the RKOA-AEID technique are made in Table 5 and Fig. 11. The RKOA-AEID technique offers a reduced CT of 1.97s. On the other hand, the AdaBoost, GB, XGBoost, KNN-AOA,

and KNN-PSO algorithms provide increased CT values of 3.52s, 2.57s, 3.67s, 4.77s, and 5.60s respectively.

These results confirmed the better performance of the RKOA-AEID technique. The improved results of the RKOA-AEID technique are due to the integration of the RKOA-based FS, ensemble classification, and LCWOA-based hyperparameter tuning. The RKOA algorithm selects the related and useful features from the available set of features. With the elimination of irrelevant features, the proposed model can concentrate on essential factors contributing to the classification process. Besides, the proposed model leverages ensemble learning, a robust mechanism that combines the strengths of multiple DL techniques. On the other hand, the LCWOA-based optimizer chooses the optimal values for the hyperparameters of a given HDL model. Hyperparameters are settings that are not learned during training but must be set before training. They can have a significant impact on the performance of the model, and selecting the optimal values can lead to better accuracy. By combining the RKOA-based FS algorithm and LCWOA-based hyperparameter tuning, the proposed model can achieve even better results by focusing on the most relevant features and selecting the optimal settings for the algorithm.

V. CONCLUSION

In this article, we have focused on the design and development of the RKOA-AEID technique for secure IoT-based WSNs. The goal of the RKOA-AEID technique is to accomplish security solutions for IoT-assisted WSNs. To accomplish this, the RKOA-AEID technique performs different stages of operations namely data pre-processing, RKOA-based feature selection, and LCWOA-based hyperparameter selection. In this work, the RKOA is applied to elect an optimum set of features. For intrusion detection, an average ensemble learning model is used comprising three DL models. Finally, the LCWOA can be executed for the optimum hyperparameter chosen for the ensemble models. The performance outcome of the RKOA-AEID approach can be tested on benchmark IDS datasets. The extensive experimental outcomes point out the better result of the RKOA-AEID method with improved accuracy of 98.94% and decreased CT of 1.97s. In future, the performance of the proposed model can be tested on large-scale real-time databases.

ACKNOLWEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project under grant number (RGP.2/65/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. The 1st author would like to thank the Deanship of Scientific Research at Shaqra University for supporting this research. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444). This study is partially funded by the Future University in Egypt (FUE).

REFERENCES

[1] M. Rizwanullah, H. Alsolai, M. K. Nour, A. S. A. Aziz, M. I. Eldesouki, and A. A. Abdelmageed, "Hybrid muddy soil fish optimization-based energy aware routing in IoT-assisted wireless sensor networks," *Sustainability*, vol. 15, no. 10, p. 8273, May 2023.

[2] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100213.

[3] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Quality of service aware secure data transmission model for Internet of Things assisted wireless sensor networks," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 1, Jan. 2023, Art. no. e4664.

[4] S. Sharma and V. K. Verma, "An integrated exploration on Internet of Things and wireless sensor networks," *Wireless Pers. Commun.*, vol. 124, no. 3, pp. 2735–2770, Jun. 2022.

[5] F. Naseer, M. N. Khan, and A. Altalbe, "Telepresence robot with DRL assisted delay compensation in IoT-enabled sustainable healthcare environment," *Sustainability*, vol. 15, no. 4, p. 3585, Feb. 2023.

[6] R. Punithavathi, R. T. Selvi, R. Latha, G. Kadiravan, V. Srikanth, and N. K. Shukla, "Robust node localization with intrusion detection for wireless sensor networks," *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 143–156, 2022.

[7] M. Basheri and M. Ragab, "Quantum cat swarm optimization based clustering with intrusion detection technique for future Internet of Things environment," *Comput. Syst. Sci. Eng.*, vol. 46, no. 3, pp. 3783–3798, 2023.

[8] I. Mehmood, A. Ullah, K. Muhammad, D.-J. Deng, W. Meng, F. Al-Turjman, M. Sajjad, and V. H. C. de Albuquerque, "Efficient image recognition and retrieval on IoT-assisted energy-constrained platforms from big data repositories," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9246–9255, Dec. 2019.

[9] H. Ashraf, F. Khan, U. Ihsan, F. Al-Quayed, N. Z. Jhanjhi, and M. Humayun, "MABPD: Mobile agent-based prevention and black hole attack detection in wireless sensor networks," in *Proc. Int. Conf. Bus. Anal. Technol. Secur. (ICBATS)*, Mar. 2023, pp. 1–11.

[10] T. V. Ramana, M. Thirunavukkarasan, A. S. Mohammed, G. G. Devarajan, and S. M. Nagarajan, "Ambient intelligence approach: Internet of Things based decision performance analysis for intrusion detection," *Comput. Commun.*, vol. 195, pp. 315–322, Nov. 2022.

[11] K. Ramana, A. Revathi, A. Gayathri, R. H. Jhaveri, C. V. L. Narayana, and B. N. Kumar, "WOGRU-IDS—An intelligent intrusion detection system for IoT assisted wireless sensor networks," *Comput. Commun.*, vol. 196, pp. 195–206, Dec. 2022.

[12] D. A. J. Rajan and E. R. Naganathan, "Trust based anonymous intrusion detection for cloud assisted WSN-IoT," *Global Transitions Proc.*, vol. 3, no. 1, pp. 104–108, Jun. 2022.

[13] S. Alkhliwi, "Energy efficient cluster based routing protocol with secure IDS for IoT assisted heterogeneous WSN," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 11, pp. 1–8, 2020.

[14] C. Yao, Y. Yang, K. Yin, and J. Yang, "Traffic anomaly detection in wireless sensor networks based on principal component analysis and deep convolution neural network," *IEEE Access*, vol. 10, pp. 103136–103149, 2022.

[15] M. Maheswari and R. A. Karthika, "A novel hybrid deep learning framework for intrusion detection systems in WSN-IoT networks," *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 365–382, 2022.

[16] S. Sujanthi and S. Nithya Kalyani, "SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT," *Wireless Pers. Commun.*, vol. 114, no. 3, pp. 2135–2169, Oct. 2020.

[17] S. Gurumoorthy, A. K. Kokku, P. Falkowski-Gilski, and P. B. Divakarachari, "Effective air quality prediction using reinforced swarm optimization and bi-directional gated recurrent unit," *Sustainability*, vol. 15, no. 14, p. 11454, Jul. 2023.

[18] S. M. Alshareef and A. Fathy, "Efficient red kite optimization algorithm for integrating the renewable sources and electric vehicle fast charging stations in radial distribution networks," *Mathematics*, vol. 11, no. 15, p. 3305, Jul. 2023.

[19] M. Mafarja, T. Thaher, M. A. Al-Betar, J. Too, M. A. Awadallah, I. A. Doush, and H. Turabieh, "Classification framework for faulty-software using enhanced exploratory whale optimizer-based feature selection scheme and random forest ensemble learning," *Appl. Intell.*, vol. 53, no. 15, pp. 18715–18757, Aug. 2023.

[20] A. Mohammed and R. Kora, "An effective ensemble deep learning framework for text classification," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8825–8837, Nov. 2022.

[21] T. Mwata-Velu, J. G. Avina-Cervantes, J. M. Cruz-Duarte, H. Rostro-Gonzalez, and J. Ruiz-Pinales, "Imaginary finger movements decoding using empirical mode decomposition and a stacked BiLSTM architecture," *Mathematics*, vol. 9, no. 24, p. 3297, Dec. 2021.

[22] A. Al Hamoud, A. Hoenig, and K. Roy, "Sentence subjectivity analysis of a political and ideological debate dataset using LSTM and BiLSTM with attention and GRU models," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 10, pp. 7974–7987, Nov. 2022.

[23] S. Syama, J. Ramprabhakar, R. Anand, and J. M. Guerrero, "A hybrid extreme learning machine model with Lévy flight chaotic whale optimization algorithm for wind speed forecasting," *Results Eng.*, vol. 19, Sep. 2023, Art. no. 101274.

[24] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *J. Sensors*, vol. 2016, Aug. 2016, Art. no. 4731953.

[25] M. Aljebreen, M. A. Alohali, M. K. Saeed, H. Mohsen, M. A. Duhayyim, A. A. Abdelmageed, S. Drar, and S. Abdelbagi, "Binary chimp optimization algorithm with ML based intrusion detection for secure IoT-assisted wireless sensor networks," *Sensors*, vol. 23, no. 8, p. 4073, Apr. 2023.

[26] M. Alqahtani, A. Gumaei, H. Mathkour, and M. A. M. B. Ismail, "A genetic-based extreme gradient boosting model for detecting intrusions in wireless sensor networks," *Sensors*, vol. 19, no. 20, p. 4383, Oct. 2019.

[27] 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, p. 1407, Feb. 2022.