IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 February 2024, accepted 19 April 2024, date of publication 23 April 2024, date of current version 10 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3392618

RESEARCH ARTICLE

Enhancing Security in IoT-Assisted UAV Networks Using Adaptive Mongoose Optimization Algorithm With Deep Learning

SAUD S. ALOTAIBI[1], AHMED SAYED[2], ELMOUEZ SAMIR ABD ELHAMEED[3], OMAR ALGHUSHAIRY[4], MOHAMMED ASSIRI[5], AND SARA SAADELDEEN IBRAHIM[5]

[1]Department of Information Systems, College of Computing and Information Systems, Umm Al-Qura University, Makkah 24382, Saudi Arabia
[2]Research Center, Future University in Egypt, New Cairo 11835, Egypt
[3]Department of Computer Science, College of Post-Graduated Studies, Sudan University of Science and Technology, Khartoum 11111, Sudan
[4]Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 21589, Saudi Arabia
[5]Department of Computer Science, College of Sciences and Humanities–Al Aflaj, Prince Sattam Bin Abdulaziz University, Al-Aflaj 16273, Saudi Arabia

Corresponding author: Mohammed Assiri (m.assiri@psau.edu.sa)

This study is partially funded by the Future University in Egypt (FUE).

ABSTRACT Due to the sensitive and mission-critical nature of the data collected and transferred, security in IoT-assisted UAV networks is of great significance. Intrusion detection in IoT-assisted UAV networks includes the deployment of complex monitoring systems to identify and respond to cyberattacks, physical breaches, or unauthorized access. This system employs a combination of anomaly detection and signature-based methods to find malicious or unusual activities within the network. A robust intrusion detection mechanism is essential for protecting the security and integrity of the UAVs and the data collected, ensuring that any possible vulnerabilities are promptly addressed and identified. Consequently, this study introduces an adaptive mongoose optimizer algorithm with a deep learning-based intrusion detection (AMOA-DLID) method in IoT-assisted UAV networks. The AMOA-DLID technique intends to ensure security in the IoT-assisted UAV networks via an intrusion detection process. In the presented AMOA-DLID technique, AMOA is initially applied for the feature selection process. The following sparse autoencoder (SAE) model can be exploited for the recognition of the intrusions. Lastly, the recognition rate of the SAE model can be improved by employing the Harris Hawks optimizer (HHO) technique. The detailed experimental study of the AMOA-DLID model is performed on the benchmark dataset of IDS. The extensive results portrayed that the AMOA-DLID technique reaches improved security over other models on the IoT-assisted UAV networks.

INDEX TERMS Intrusion detection system, UAV, IoT, deep learning, Harris Hawks optimization, feature selection.

I. INTRODUCTION

Currently, smart cities have expanded important power as urban regions hold advanced applications to enhance sustainability, efficiency, and excellence of life. Smart cities integrate innovative technologies like the Internet of Things (IoT), artificial intelligence (AI), and big data analytics to integrate different urban methods and develop the quality of services delivered to populations [1]. In smart city environments, UAVs provide novel benefits that make them vital for an extensive range of plans. It provides actual-time observation and checking abilities, allowing experts to gather important data from some resources and places [2]. Whereas, UAVs tested advantages in a variety of situations from the visitor following to environmental estimation and tragedy reaction for public safety. The capability to direct challenging terrain and far-off regions with simplicity creates invaluable effects for developing situational attention as well as fast response time [3]. With great profile processes in aggressive surroundings, effective attacks alongside UAVs have overwhelming effects on the public as well as national safety. UAVs are employed more and become greater targets and

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

attacks beside them are known [4]. Jamming and Spoofing attacks are two well-known and very simple to behavior because they need only cheap software definite radio.

The incorporation of IoT devices with UAVs creates an effective combination for several applications, from environmental monitoring to package delivery. However, this convergence introduces major security challenges that need careful attention. Classical security techniques often lag behind the ever-evolving threat landscape. However, IDS analyzes the network traffic and device behavior in real-time, detecting potential attacks and suspicious activity before they cause damage [5]. This proactive method is crucial to ensure the safety of UAV operation, safeguard sensitive information, and prevent critical system disruption. IoT-assisted UAV network is an intricate ecosystem, with vulnerabilities at different levels – from transmission protocol to individual sensors. IDS offers multi-layered protection by monitoring different data sources, involving network traffic, device logs, and sensor readings. This comprehensive technique helps mitigate and expose threats across the overall network, leaving no blind spots for the attackers to exploit [6].

Numerous present techniques concentrate on conventional network security actions and directing details of UAV operations. Moreover, privacy-preserving models regularly do not excuse for dynamic nature of UAV systems that lead to suboptimal defense. To struggle against threats against UAVs, a trivial on-board IDS is required. Enhanced and highly robust IDS are required for IoT systems [7]. Deep learning (DL) quickly analyzes huge amounts of data as well as supports spontaneous alterations of safety methods upon recognition of malware or safety openings while employing low computational power [8]. Safety networks made on DL do not require a network connection to threat recognition because they function across devices, primary operating methods, and files. The selection of the DL model in IoT significantly aids in IDS. Such selection can be executed by equating techniques to define the most precise one and then executing a particular method [9]. This study has numerous advantages enhanced accuracy and decreased false alarm rate of IDS by employing DL techniques. By strengthening its security, it affects human lives, budgets, technology, and the atmosphere of IoT [10].

This study introduces an adaptive mongoose optimizer algorithm with a deep learning-based intrusion detection (AMOA-DLID) method in IoT-assisted UAV networks. The AMOA-DLID technique intends to ensure security in the IoT-assisted UAV networks via an intrusion detection process. In the presented AMOA-DLID technique, AMOA is initially applied for the feature selection (FS) process. The following sparse autoencoder (SAE) model can be exploited for the recognition of the intrusions. Lastly, the recognition rate of the SAE system can be improved by the usage of the Harris Hawks optimizer (HHO) model. The detailed experimental analysis of the AMOA-DLID algorithm was implemented on the benchmark IDS database. In summary, the key contributions of the study are given as follows.

- The main purpose of the AMOA-DLID algorithm is to ensure security in IoT-assisted UAV networks by adaptive and effectual IDS. By integrating nature-inspired optimizer methods (AMOA and HHO) with DL approaches (SAE), the methodology proposes to address the unique problems modelled by security attacks in IoT environments with UAV networks.
- Introduction of the AMOA for the primary FS procedure in the IDS. The AMOA, inspired by the behavior of mongooses was executed to adaptively select the most significant features, improving the efficacy and effectiveness of the following intrusion detection steps.
- Use of the SAE approach for identifying intrusions from the IoT-assisted UAV networks. SAE, a kind of NN, can be deployed to learn and extract meaningful representations from the selected features. Its sparse nature permits for a concise and informative encoding of intrusion patterns, contributing to correct recognition.
- Integration of the HHO algorithm to improve the recognition rate of the SAE methodology. HHO, inspired by the hunting behavior of hawks, can executed to modify the parameters of the SAE algorithm, enhancing its capability to discern subtle patterns connected with intrusions. This contributes to overall performance improvement in intrusion detection.

A. LITERATURE WORKS

Wu et al. [11] developed a Q-learning-based two-fold cooperative IDS (Q-TCID). In particular, this model uses an intelligent dynamic voting technique. In addition, a clever auditing method is also presented to execute system-level examinations. Both methods use Q-learning optimizer plans and cooperate with the exterior atmosphere in their particular Markov result procedures that lead to optimal ID plans. In [12], a traditional deep neural network was proposed as well as executed to categorize several dissimilar kinds of system attacks in IoT. As a test bed for similar consequences, an advanced dataset of CICIDS2017 is extreme and employed. The attained outcomes are equated with the current works. The research designed augmentation models and compared all results to overcome the imbalanced data problem.

In [13], dual distinct methods were designed. In 1st technique, a CNN has been created and integrated with the LSTM deep network layer. The 2nd method created all full connection layers (dense layers) to make an ANN. Therefore, the second method is the tradition of ANN layers with numerous sizes projected. Ullah et al. [14] developed a transformer NN-based IDS (TNN-IDS) specially considered for MQTT-assisted IoT systems. TNN-IDS influences the parallel treating ability of the TNN, which rushes learning procedures and outcomes in enhanced recognition of mischievous attacks. For calculating the act of the developed network, it was evaluated by numerous IDSs based on ML and DL techniques.

In [15], a DL-based ID model is presented by including 3 stages. Primary, FS segment is employed. Next, a DL framework based on GAN is specially developed for ID pointing at a single attack. Finally, a novel ID technique is presented by uniting numerous ID techniques. ID aims at many attacks and is understood over planned GAN-based DL design. Maray et al. [16] developed a Harmony Search algorithm-based FS with Optimum CAE (HSAFS-OCAE) approach. HSAFS model employed for FS. Then, the CAE technique influenced to identification as well as categorization of intrusions from the SDN-enabled IoT atmosphere.

In [17], a privacy-preserving-based protected structure was proposed. Initially, a blockchain module and smart contract-based improved Proof of Work (ePoW) were presented. Next, an LSTM-AE approach was used. An encoded data has been employed by projected Attention-based RNN (A-RNN). The Truncated Backpropagation Through Time (BPTT) model is employed for training. Binary openly obtainable datasets such as ToN-IoT and CICIDS-2017 were used for estimation. Shah et al. [18] developed an AI-based scheme technique with a double objective. It foremost spots malicious users tiresome of negotiation IoT atmosphere utilizing a dual grouping issue. Besides, blockchain expertise is employed to provide tamper-proof storage to hoard non-malicious IoT information. This paper uses DL techniques to categorize malicious as well as non-malicious smart agreements.

Perumalla et al. [19] an oppositional Aquila Optimizer-based FS with ML-assisted IDS (OAOFS-MLIDS) in the IoD platform is introduced. The suggested technique's main aim is to achieve safe access control through the intrusion detection that exists in it. Fatani et al. [20] present a novel IDS architecture based on the combination of DL and optimizer techniques. First, a feature extractor model based on CNN has been introduced. Next, a novel FS technique is employed based on the adapted type of Growth Optimizer (GO), named MGO. Then, the Whale Optimizer Algorithm (WOA) is used to improve the search procedure of the GO. In [21], proposes a search-resampling-optimization (SRO) algorithm. A hybrid A∗ mechanism is used for generating a coarse path as per the boundary state in the search phase. Next, a resampling procedure is employed to cover a sequence of safe dispatch corridors (SDCs) beside the coarse pathway. In [22], we concentrate on cooperative mission assignments for varied UAVs. We design a multi-objective optimizer algorithm to discover a balance amid UAV losses and mission success. The main objective function is formulated by conditional probability theory by presenting the probabilities of UAV loss and task gains.

Chulerttiyawong and Jamalipour [23] present an intelligent Sybil attack recognition method for FANETs-based IoFT utilizing physical layer features of the radio signals produced from the UAVs as identified by 2 ground nodes. A supervised ML method can be deployed and experimented with many distinct classifiers existing in the Weka workbench platform. Pu and Zhu [24] examine a lightweight distributed recognition method, discussed as Lids, to defend against flooding attacks from the IoD platform. The fundamental idea of Lids is that all the drones count the amount of packets that it has sent from an existing time interval and share the self-counting report with other drones under the contacts. Al-Sarawi et al. [25] examine the Passive Rule-based Approach (PRBA) to identify sinkhole nodes from RPL-based IoT networks. The PRBA algorithm depends on 3 presented behavioral indicators: (i) Bidirectional behavior, (ii) Bidirectional frequency behavior, and (iii) Power Consumption behavior.

II. THE PROPOSED MODEL

In this research, we present an AMOA-DLID technique in IoT-assisted UAV networks. The AMOA-DLID technique intends to ensure security in the IoT-assisted UAV networks via an IDS procedure. It has 3 major procedures such as AMOA-based FS, SAE-based classification, and HHO-based parameter tuning. Fig. 1 depicts the entire procedure of the AMOA-DLID technique.

A. FEATURE SELECTION USING AMOA MODEL

Initially, the AMOA model is applied to the FS process. AMOA is a nature-inspired optimizer method that relies on the behaviors of mongooses in their search for food and their interactions with their environment [26]. It is introduced as a metaheuristic algorithm to resolve optimization problems. The algorithm is stimulated through the foraging behavior of mongooses, particularly their ability to hunt and find food by searching, avoiding predators, and utilizing communication among group members. Here, the individuals in the population are randomly produced with upper and lower boundaries, as follows:

$$X = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,d-1} & x_{1,d} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,d-1} & x_{2,d} \\ & & x_{a,b} & & \\ x_{m,1} & x_{m,2} & \cdots & x_{m,d-1} & x_{m,d} \end{pmatrix} \tag{1}$$

Now set of candidates generated randomly in the present population is denoted as X, $x_{a,b}$ specifies the location of b^{th} dimension of a^{th} population, m indicates size of populations, and d implies dimensional of problems. At last, the optimum solution at all iterations is assessed by using the subsequent formula:

$$x_{a,b} = unifrnd\left(V_{\mathrm{Min}}, V_{\mathrm{Max}}, V_{size}\right) \tag{2}$$

In Eq. (2), *unifrnd* indicates a uniformly distributed random number, the low and up bounds of the searching space V_{Min} and V_{Max} are, correspondingly, and the problem dimension is denoted as V_{size}. Now, the alpha female $\left(\alpha^{f}\right)$ can be regarded as a family unit controller:

$$\alpha^{f} = \frac{F_j}{\Sigma_{j=1}^{m} F_j} \tag{3}$$

In the alpha group , $m{-}b^{s}$ match the amount of mongooses, the number of babysitters is b^{s}, and the sound of female alpha

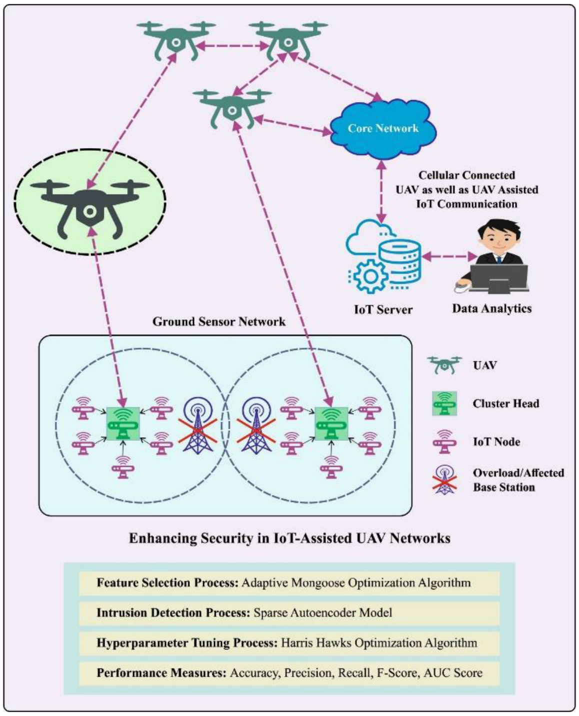
Core Network
Cellular Connected UAV as well as UAV Assisted IoT Communication
IoT Server
Data Analytics
Ground Sensor Network
UAV
Cluster Head
IoT Node
Overload/Affected Base Station
Enhancing Security in IoT-Assisted UAV Networks
Feature Selection Process: Adaptive Mongoose Optimization Algorithm
Intrusion Detection Process: Sparse Autoencoder Model
Hyperparameter Tuning Process: Harris Hawks Optimization Algorithm
Performance Measures: Accuracy, Precision, Recall, F-Score, AUC Score

FIGURE 1. The overall process of the AMOA-DLID algorithm.

towards the direction of other members is denoted by $peep^x$. Next, the sleeping mound can be defined using abundant food, as follows:

$$X_{j+1} = X_j + \delta \times peep^x \tag{4}$$

In Eq. (4), a uniformly distributed random number [–1, 1] is δ:

$$sl_j^m = \frac{F_{j+1} - F_j}{\min\limits_{j\to 1tom} \left\{ \left| F_{j+1}, F_j \right| \right\}} \tag{5}$$

Once the sleeping mound is found, the following formula is used for calculating the average value:

$$\rho = \frac{\Sigma_{j=1}^{m} sl_j^m}{m} \tag{6}$$

After the condition of the babysitter exchange is met, the scouting measures the sleeping mound defined by additional food sources. Usually, the mongooses are known to forage and scout together.

$$X_{j+1} = \begin{cases} X_j - c^v \times \delta \times rand \times \left[X_j - \vec{M}_m if\, \rho_{j+1} > \rho_j \right] \\ X_j + c^v \times \delta \times rand \times \left[X_j - \vec{M}_m else \right] \end{cases} \tag{7}$$

$$c^v = \left(1 - \frac{i^r}{M_{i^r}} \right)^{\left(2 * \frac{i^r}{M_{i^r}} \right)} \tag{8}$$

Now, a random integer within [0, 1] is represented as rand, and the parameter c^v is used to control the group's volatile, collective movement and linearly reduces over iteration.

$$\vec{M}_m = \sum_{j=1}^{m} \frac{X_j * sl_j^m}{X_j} \tag{9}$$

In Eq. (9), the force that drives mongooses towards a new sleeping mound is indicated as $\vec{M}$. In this AMOA, the objective is integrated into a single objective thereby a present weight recognizes the objective significance [27]. The study adopts a fitness function (FF) that fuses the above two objectives of FS as given below.

$$Fitness\,(X) = \alpha \cdot E\,(X) + \beta * \left(1 - \frac{|R|}{|N|} \right) \tag{10}$$

where the fitness value of subset X is $Fitness(X)$, the classifier rate of errors through features selected in X subset is $E(X)$, the amount of selected and original features in the datasets are $|R|$ and $|N|$ correspondingly, the weighted of classifier error and the reduction ratio are α and β, $\alpha \in [0, 1]$ and $\beta = (1-\alpha)$.

B. CLASSIFICATION USING SAE

In this work, the SAE model can be exploited for the recognition of the intrusions. As an unsupervised three-layer NN, AE consists of three layers namely, an input, a hidden layer (HL), and a reconstruction layer (also known as an output layer) [28]. AE could slowly transform the feature vector into an abstract feature vector that will realize the nonlinear conversion from higher to lower dimension data space. Fig. 2 illustrates the SAE architecture. The proposed structure of AE is divided into two phases: the encoder and decoder process and are explained in the following:

The encoder procedure from the input layer to the HL:

$$H = g_{\theta_1}(X) = \sigma\left(W_{ij} X + \varphi_1 \right) \tag{11}$$

The decoder process from HL to the output layer:

$$Y = g_{\theta_2}(H) = \sigma\left(W_{jk} H + \varphi_2 \right) \tag{12}$$

In the above formulas, the input and reconstruction vectors are $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$ and the low-dimensional vector output from the HL is $H=(h_1, h_2, \ldots, h_m)$, $X \in R^n$, $Y \in R^n$, $H \in R^m$(the amount of hidden units is m and the dimension of the input vector is n). The connecting weight matrices between HL and input layers are $W_{ij} \in R^{m\times n}$. The connecting weight matrices between HL and output layers is $W_{jk} \in R^{n\times m}$. To recreate the input dataset as closely as possible while decreasing resource usage in the training process, $W_{jk} = W_{ij}^T$. The bias vector of the input layer and HL are $\varphi_1 \in R^{n\times 1}$ and $\varphi_2 \in R^{m\times 1}$ correspondingly. The sigmoid function is utilized as an activation function. The activation function of HL and output neurons are g_{θ_1} and g_{θ_2} correspondingly:

$$g_{\theta_1}(\cdot) = g_{\theta_2}(\cdot) = \frac{1}{1 + e^{-x}} \tag{13}$$

Consider that the output data by the HL unit is the optimum low-dimension representative of the original dataset and integrates any data existing in the original information. The $J_E(W, \varphi)$ reconstructed error function between H and Y exploits the MSE function, where N denotes the number of input samples.

$$J_E\left(W,\varphi\right)=\frac{1}{2N}\sum_{r=1}^{N}||Y^{(r)}-X^{(r)}||^2 \tag{14}$$

Based on computation learning of the receptive field of cells in the mammalian main visual cortex, Olshausen originally proposed the concept of sparse coding. Owing to the inevitable problems of AE, for instance, the input dataset is transferred to the output layer. Even though the original input dataset is perfectly recovered, the AE doesn't extract any meaningful feature. Assume that the average activation of neurons in the HL is $\hat{\rho}_j$, $\hat{\rho}_j=\frac{1}{N}\sum_{i=1}^{N}[n_j\left(x_i\right)]$. We expect the average activation $\hat{\rho}_j$ to approach the constant ρ that is closer to 0. Thus, we added Kullback-Leibler (KL) divergence as a regularization term to the error function for achieving the abovementioned purpose:

$$KL(\rho||\hat{\rho}_j)=\rho\log\frac{\rho}{\hat{\rho}_j}+(1-\rho)\log\frac{1-\rho}{1-\hat{\rho}_j} \tag{15}$$

Now, the error function of SAE comprises two different parts: MSE, and a regularization term. as given below:

$$J_{sparse}\left(W,b\right)=J\left(W,b\right)+\mu\sum_{j=1}^{m}KL(\rho||\hat{\rho}_j) \tag{16}$$

In Eq. (16), the amount of hidden units is m and the weight factor which controls the strength of sparse item is μ. Also, the weight attenuation item is added to the error function to prevent over-fitting, the attenuation coefficient of weight is represented as λ.

$$\begin{aligned}J_{sparse}\left(W,b\right)&=J_E\left(W,b\right)+\mu\sum_{j=1}^{m}KL(\rho||\hat{\rho}_j)\\&\quad+\frac{\lambda}{2}\sum_{r=1}^{3}\sum_{i=1}^{m}\sum_{j=1}^{m+1}(w_{ij}^{r})^2\end{aligned} \tag{17}$$

C. PARAMETER TUNING USING HHO

Lastly, the recognition rate of the SAE technique can be enhanced by the usage of the HHO technique. HHO is a new swarm intelligence (SI) optimization method whose main motivation comes from the hunting processes of Harris hawks [29]. The global search and local development stages are two different hunting processes of HHO:

$$\begin{aligned}&X\left(t+1\right)\\&=\begin{cases}X_{rand}\left(t\right)-r_1\left|X_{rand}\left(t\right)-2r_2X\left(t\right)\right|q\geq 0.5\\(X_{rabbit}\left(t\right)-X_m\left(t\right))-r_3\left(LB+r_4\left(UB-LB\right)\right)\\q< 0.5\end{cases}\end{aligned} \tag{18}$$

Here location vector of hawks at t iteration is $X(t+1)$, the location of the rabbit is $X_{rabbit}\left(t\right)$, the upper and lower boundaries of variables are LB and UB, the existing location vector of hawks is $X(t)$, random integers within (0, 1) that are updated in all iterations are represented as r_1, r_2, r_3, r_4, and q, an arbitrarily elected hawk from current population is $X_{rand}(t)$, and the average location of the existing populace of hawks is indicated by X_m.

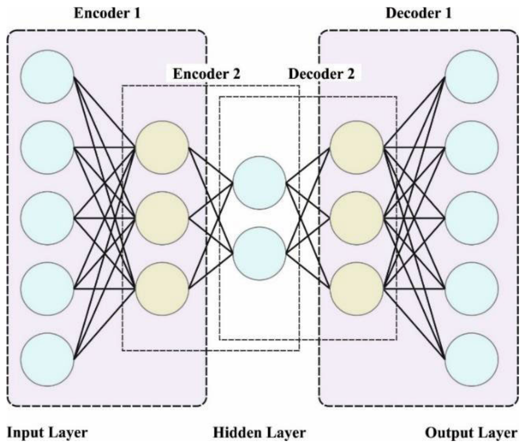

FIGURE 2. SAE architecture.

The soft and hard besiege with quick progressive dive has four different parts of local development. If escape energy $|E|<1$, then local progress takes place. The equation for local development is given below:

(1) Soft besiege

$$\begin{aligned}X\left(t+1\right)&=X\left(t\right)-E\left|JX_{rabbit}\left(t\right)-X\left(t\right)\right|\\X\left(t\right)&=X_{rabbit}\left(t\right)-X\left(t\right)\end{aligned} \tag{19}$$

(2) Hard besiege

$$X\left(t+1\right)=X_{rabbit}\left(t\right)-E\left|X\left(t\right)\right| \tag{20}$$

(3) Soft besiege with quick progressive dive

$$Y=X_{rabbit}\left(t\right)-E\left|JX_{rabbit}\left(t\right)-X\left(t\right)\right| \tag{21}$$

(4) Hard besiege with quick progressive dive

$$\begin{aligned}Y&=X_{rabbit}\left(t\right)-E\left|JX_{rabbit}\left(t\right)-X_m\left(t\right)\right|\\X_m\left(t\right)&=\frac{1}{N}\sum_{i=1}^{N}X_i\left(t\right)\end{aligned} \tag{22}$$

Now the hawk position at t^{hetth} iteration is $X_i(t)$ and the overall amount of hawks is represented by N.

The HHO method develops an FF to achieve improved effectiveness of detection. It describes an optimistic integer to distinguish the best performance of the solution candidate. The reduction of classifier error rate can be viewed as an FF,

$$\begin{aligned}fitness\left(x_i\right)&=Classifier\ Error\ Rate\left(x_i\right)\\&=\frac{No.of\ misclassified\ instances}{Totalno.of\ instances}*100\end{aligned} \tag{23}$$

III. PERFORMANCE VALIDATION

The proposed model is simulated using Python 3.6.5. In this part, IDS outcomes of the AMOA-DLID system are tested by employing the NSL-KDD database including 125973 samples with 42 features as described in Table 1. It is accessible at https://www.unb.ca/cic/datasets/nsl.html. The NSL-KDD

TABLE 1. Details on database.

Classes	No. of Instances
Dos	45927
R2l	995
Probe	11656
U2r	52
Normal	67343
Total No. of Instances	125973

dataset is a group of network traffic datasets applied for intrusion detection study. It is a modified version of the KDD'99 datasets. The NSL-KDD database was formed to address the limitations of the KDD'99 datasets, such as the imbalance of attack and normal traffic and the high number of redundant records. The AMOA-DLID technique has designated a set of 22 features.

A series of measures employed for observing the classification results are accuracy ($accu_y$), precision ($prec_n$), recall ($reca_l$), and F-score (F_{score}).

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{24}$$

Precision is employed in order to measure the ratio of correctly forecast positive instances among all the instances that were predicted as positive.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{25}$$

Recall is utilized to measure the ratio of positive samples correctly categorized.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{26}$$

Accuracy is applied to measure the ratio of correctly categorized samples (positives and negatives) beside complete samples (amount of samples that have been classified).

$$\text{F} - \text{score} = \frac{2\text{TP}}{2\text{TP} + \text{FP} + \text{FN}} \tag{27}$$

F-score is a measure uniting the harmonic mean of precision and recall.

The confusion matrices attained by the AMOA-DLID algorithm with 80:20 and 70:30 of the TRA phase/TES phase are shown in Fig. 3. The achieved findings refer to the efficient detection and classification with all five classes.

In Table 2 and Fig. 4, complete intrusion classification outcomes of the AMOA-DLID technique are portrayed at 80:20 of the TRA phase/TES phase. The outcomes infer that the AMOA-DLID technique reaches effectual identification of the intrusions. With 80% of the TRA phase, the AMOA-DLID technique offers an average $accu_y$ of 99.56%, $prec_n$ of 92.58%, $reca_l$ of 86.36%, F_{score} of 88.03%, and AUC_{score} of 93.01%. Additionally, with 20% of the TES phase, the AMOA-DLID system gains an average $accu_y$ of 99.56%, $prec_n$ of 92.58%, $reca_l$ of 86.36%, F_{score} of 88.03%, and AUC_{score} of 93.01%.

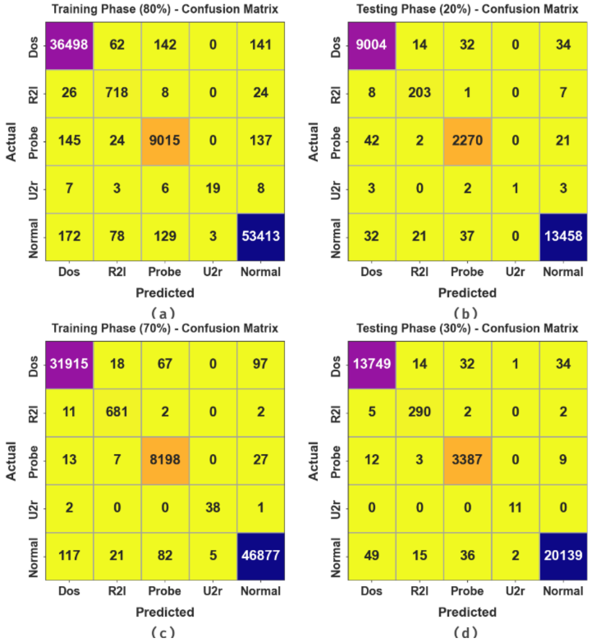

FIGURE 3. Confusion matrices of (a-c) TRA phase of 80% and 70% and (b-d) TES phase of 20% and 30%.

TABLE 2. Intrusion classifier analysis of AMOA-DLID technique at 80:20 of TRA phase/TES phase.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TRA Phase (80%)					
Dos	99.31	99.05	99.06	99.06	99.26
R2l	99.78	81.13	92.53	86.45	96.18
Probe	99.41	96.94	96.72	96.83	98.20
U2r	99.97	86.36	44.19	58.46	72.09
Normal	99.31	99.42	99.29	99.36	99.32
Average	99.56	92.58	86.36	88.03	93.01
TES Phase (20%)					
Dos	99.35	99.06	99.12	99.09	99.30
R2l	99.79	84.58	92.69	88.45	96.27
Probe	99.46	96.93	97.22	97.07	98.45
U2r	99.97	100.00	11.11	20.00	55.56
Normal	99.38	99.52	99.34	99.43	99.39
Average	99.59	96.02	79.90	80.81	89.79

An overall intrusion classifier outcome of the AMOA-DLID method is depicted at 70:30 of the TRA phase/TES phase as shown in Table 3 and Fig. 5. The experimental outcomes conclude that the AMOA-DLID system attains effective detection of intrusions.

With 70% of the TRA phase, the AMOA-DLID system reaches an average $accu_y$ of 99.79%, $prec_n$ of 95.90%, $reca_l$ of 97.78%, F_{score} of 96.82%, and AUC_{score} of 98.81%. Moreover, with 30% of the TES phase, the AMOA-DLID method attain an average $accu_y$ of 99.77%, $prec_n$ of 93.18%, $reca_l$ of 99.04%, F_{score} of 95.83%, and AUC_{score} of 99.44%.

Fig. 6 establishes classifier performances of the AMOA-DLID system at 80:20 and 70:30. Figs. 6a-6c illustrates $accu_y$ curve of the AMOA-DLID system. The outcome states that the AMOA-DLID approach gains higher $accu_y$ outcomes over the highest epochs. Furthermore, the maximum validation $accu_y$ over TRA $accu_y$ depicts that the

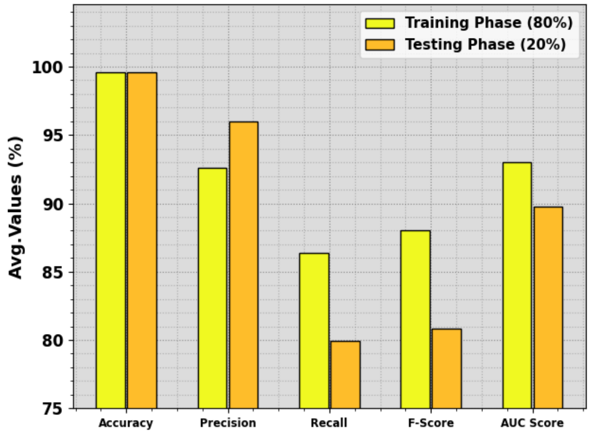

FIGURE 4. Average of AMOA-DLID model at 80:20 of TRA phase/TES phase.

TABLE 3. Intrusion classifier outcome of AMOA-DLID technique at 70:30 of TRA phase/TES phase.

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TRA Phase (70%)					
Dos	99.63	99.55	99.43	99.49	99.59
R2l	99.93	93.67	97.84	95.71	98.90
Probe	99.78	98.19	99.43	98.81	99.62
U2r	99.99	88.37	92.68	90.48	96.34
Normal	99.60	99.73	99.52	99.63	99.61
Average	99.79	95.90	97.78	96.82	98.81
TES Phase (30%)					
Dos	99.61	99.52	99.41	99.47	99.57
R2l	99.89	90.06	96.99	93.40	98.45
Probe	99.75	97.98	99.30	98.63	99.55
U2r	99.99	78.57	100.00	88.00	100.00
Normal	99.61	99.78	99.50	99.64	99.62
Average	99.77	93.18	99.04	95.83	99.44

AMOA-DLID algorithm reaches ably on the test database. However, Figs. 6b-6d represents the loss outcome of the AMOA-DLID technique. The simulation value shows that the AMOA-DLID technique reaches nearby outcomes of TRA and validation losses. This can be identified that the AMOA-DLID method gains proficiency on the test database.

Fig. 7 defines the classifier outcome of the AMOA-DLID algorithm at 80:20 and 70:30. Figs. 7a-7c depicts the PR curve of AMOA-DLID methodology. The outcomes implied that the AMOA-DLID algorithm outcomes in the maximum outcome of PR. Besides, it can be obvious that the AMOA-DLID system gains superior values of PR in every class. However, Figs. 7b-7d establishes the ROC curve of the AMOA-DLID approach. The outcome is definite that the AMOA-DLID system resulted in better values of ROC. Furthermore, it becomes clear that the AMOA-DLID system extends superior values of ROC on each class.

In Table 4, a brief comparison research of the AMOA-DLID model takes place with recent approaches [30]. In Fig. 8, a comparative $accu_y$ and $prec_n$ results of the AMOA-DLID technique is provided. The results stated that the AMOA-DLID method achieves enhanced results over other techniques. Based on $accu_y$, the AMOA-DLID

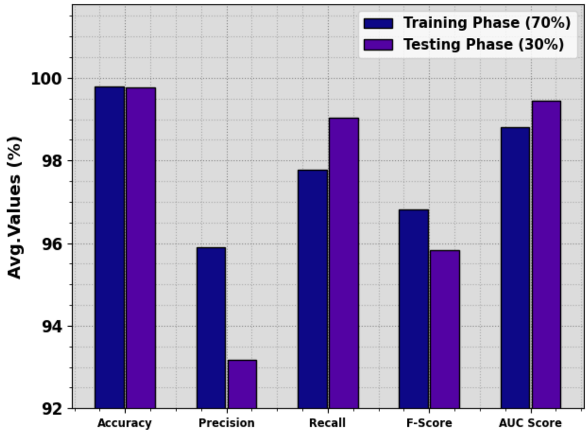

FIGURE 5. Average of AMOA-DLID technique at 70:30 of TRA phase/TES phase.

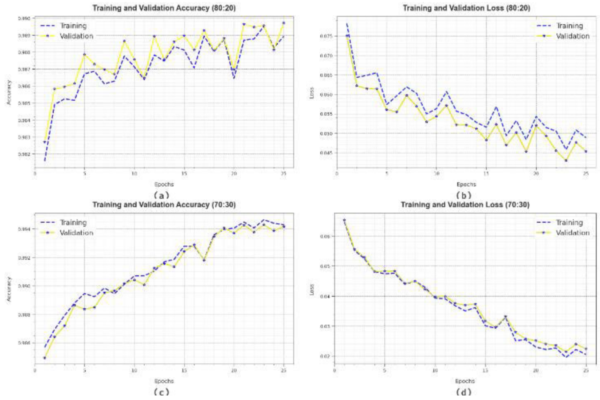

FIGURE 6. (a-c) $Accu_y$ curve of 80:20 and 70:30 and (b-d) Loss curve of 80:20 and 70:30.

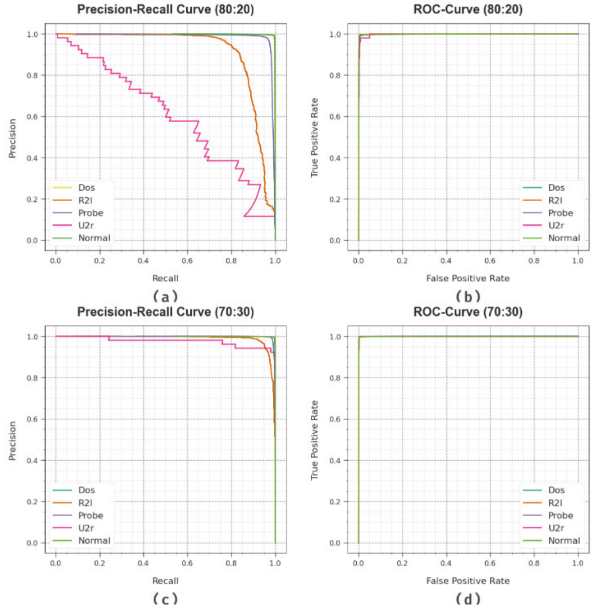

FIGURE 7. (a-c) PR curve on 80:20 and 70:30 and (b-d) ROC curve on 80:20 and 70:30.

TABLE 4. Comparison analysis of the AMOA-DLID technique with other approaches [30].

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
AMOA-DLID	99.79	95.90	97.78	96.82
DRL-BWO Model	98.70	94.95	75.00	74.20
IDBN Model	95.32	91.06	74.03	72.11
T-SID Model	94.38	94.22	79.50	72.89
DL Model	91.80	93.83	75.47	73.56
DPC-DBN Model	94.39	94.70	78.12	73.59
AK-NN Model	91.78	92.64	79.77	74.25

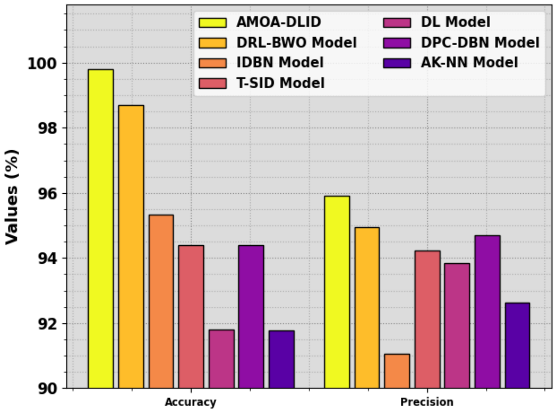

FIGURE 8. $Accu_y$ and $prec_n$ outcome of AMOA-DLID technique with other methods.

TABLE 5. CT analysis of AMOA-DLID technique with other approaches.

Methods	Computational Time (sec)
AMOA-DLID	0.69
DRL-BWO Model	1.46
IDBN Model	2.12
T-SID Model	3.91
DL Model	3.06
DPC-DBN Model	2.65
AK-NN Model	2.93

model offers a higher $accu_y$ of 99.79% however, the DRL-BWO model, IDBN method, T-SID system, DL technique, DPC-DBN approach, and AK-NN technique provide lower $accu_y$ values of 98.70%, 95.32%, 94.38%, 91.80%, 94.39%, and 91.78%, correspondingly. Also, based on $prec_n$, the AMOA-DLID approach provides a superior $prec_n$ of 95.90% whereas the DRL-BWO model, IDBN method, T-SID system, DL technique, DPC-DBN approach, and AK-NN technique offer minimal $prec_n$ values of 94.95%, 91.06%, 94.22%, 93.83%, 94.70%, and 92.64%, correspondingly.

In Fig. 9, a comparative $recal_l$ and F_{score} outcomes of the AMOA-DLID algorithm are provided. The outcome implied that the AMOA-DLID system attains better performances with other approaches. Based on $reca_l$, the AMOA-DLID system reaches a superior $reca_l$ of 97.78% while the DRL-BWO model, IDBN method, T-SID system, DL technique, DPC-DBN approach, and AK-NN technique attains minimal $reca_l$ values of 75%, 74.03%, 79.50%, 75.47%, 78.12%, and 79.77%, correspondingly. Followed by, based on F_{score}, the AMOA-DLID method provides a superior F_{score} of 96.82% whereas the DRL-BWO model, IDBN method, T-SID system, DL technique, DPC-DBN approach, and AK-NN technique gain decreased F_{score} values of 74.20%, 72.11%, 72.89%, 73.56%, 73.59%, and 74.25%, correspondingly.

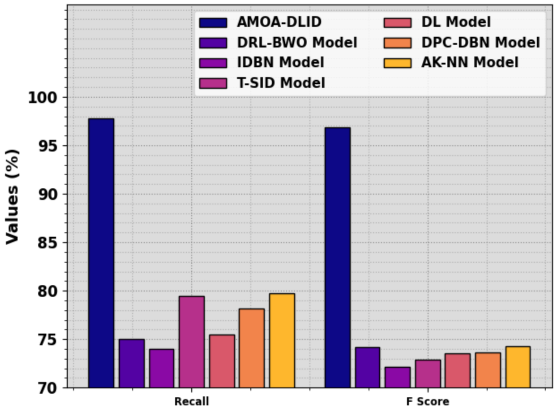

FIGURE 9. $Reca_l$ and F_{score} outcome of AMOA-DLID technique with other methods.

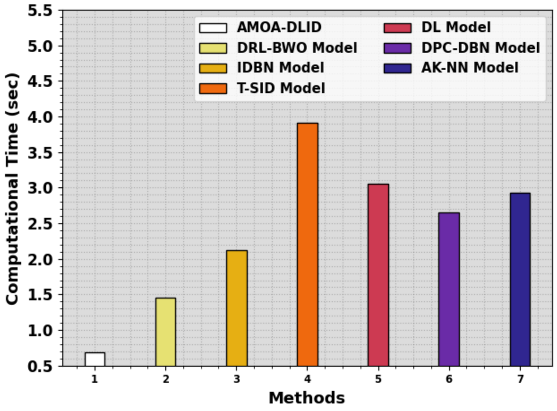

FIGURE 10. CT outcome of AMOA-DLID technique with other methods.

In Table 5 and Fig. 10, a comparative computational time (CT) analysis of the AMOA-DLID algorithm with other existing methodologies. The simulation values inferred that the T-SID system has achieved inefficient performances with an enhanced CT value of 3.91s. Besides, the DL and AK-NN models have exhibited somewhat better results with CT values of 3.06s and 2.93s. In addition, the DPC-DBN, IDBN, and DRL-BWO approaches have demonstrated reasonable and closer CT values of 2.665s, 2.12s, and 1.46s respectively. However, the AMOA-DLID algorithm has outperformed the better solution with a lesser CT value of 0.69s.

Thus, the AMOA-DLID technique can be employed for an accurate intrusion detection process.

IV. CONCLUSION

In this article, we present an AMOA-DLID technique in IoT-assisted UAV networks. The AMOA-DLID technique intends to ensure security in the IoT-assisted UAV networks via an intrusion detection procedure. It has 3 main procedures such as AMOA-based FS, SAE-based classification, and HHO-based parameter tuning. Initially, the AMOA model is applied to the FS process. Followed by, the SAE model can be exploited for the recognition of the intrusions. Lastly, the recognition rate of the SAE technique can be enriched by the use of the HHO method. The detailed experimental analysis of the AMOA-DLID method is performed on a benchmark IDS database. The extensive results portrayed that the AMOA-DLID technique reaches improved security over other models on the IoT-assisted UAV networks.

The combined use of AMOA and SAE is computationally expensive, particularly for real-time processing and large datasets. This poses a challenge for the resource-constraint UAV. While AMOA provides FS, the DL nature of SAE makes it intrinsically less interpretable. Understanding why a certain feature is considered relevant for intrusion detection can be challenging. Future work could integrate Explainable AI (XAI) methods with the SAE model could improve interpretability, which allows for potentially identifying potential biases and a better understanding of the decision-making process.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number: IFP22UQU4210118DSR164.

REFERENCES

[1] N. Alturki, T. Aljrees, M. Umer, A. Ishaq, S. Alsubai, O. Saidani, S. Djuraev, and I. Ashraf, "An intelligent framework for cyber-physical satellite system and IoT-aided aerial vehicle security threat detection," *Sensors*, vol. 23, no. 16, p. 7154, Aug. 2023.

[2] R. Hamadi, "Artificial intelligence applications in intrusion detection systems for unmanned aerial vehicles," Ph.D. dissertation, 2023.

[3] R. Majeed, N. A. Abdullah, M. F. Mushtaq, M. Umer, and M. Nappi, "Intelligent cyber-security system for IoT-aided drones using voting classifier," *Electronics*, vol. 10, no. 23, p. 2926, Nov. 2021.

[4] U. I. Vivian, I. N. Cosmas, D.-S. Kim, and J.-M. Lee, "DATA-FedAVG: Delay-aware truncated accuracy-based federated averaging for intrusion detection in UAV network," *J. Korean Inst. Commun. Inf. Sci.*, vol. 48, no. 6, pp. 648–668, Jun. 2023.

[5] J. K. Samriya, M. Kumar, and R. Tiwari, "Energy-aware ACO-DNN optimization model for intrusion detection of unmanned aerial vehicle (UAVs)," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 8, pp. 10947–10962, Aug. 2023.

[6] N. Moustafa and A. Jolfaei, "Autonomous detection of malicious events using machine learning models in drone networks," in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Sep. 2020, pp. 61–66.

[7] A. Zainudin, R. Akter, D. S. Kim, and J. M. Lee, "FedIoV: A federated learning-assisted intrusion messages detection in Internet of Vehicles," in *Proc. DBPIA*, 2022, pp. 305–306.

[8] R. Zhang, J.-P. Condomines, and E. Lochin, "A multifractal analysis and machine learning based intrusion detection system with an application in a UAS/RADAR system," *Drones*, vol. 6, no. 1, p. 21, Jan. 2022.

[9] R. T. Mehmood, G. Ahmed, and S. Siddiqui, "Simulating ML-based intrusion detection system for unmanned aerial vehicles (UAVs) using COOJA simulator," in *Proc. 16th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2022, pp. 1–10.

[10] A. Zekry, A. Sayed, M. Moussa, and M. Elhabiby, "Anomaly detection using IoT sensor-assisted ConvLSTM models for connected vehicles," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, Apr. 2021, pp. 1–6.

[11] M. Wu, Z. Zhu, Y. Xia, Z. Yan, X. Zhu, and N. Ye, "A Q-learning-based two-layer cooperative intrusion detection for Internet of Drones system," *Drones*, vol. 7, no. 8, p. 502, Aug. 2023.

[12] O. K. Sahingoz, U. Cekmez, and A. Buldu, "Internet of Things (IoTs) security: Intrusion detection using deep learning," *J. Web Eng.*, pp. 1721–1760, Oct. 2021.

[13] E. H. Salman, M. A. Taher, Y. I. Hammadi, O. A. Mahmood, A. Muthanna, and A. Koucheryavy, "An anomaly intrusion detection for high-density Internet of Things wireless communication network based deep learning algorithms," *Sensors*, vol. 23, no. 1, p. 206, Dec. 2022.

[14] S. Ullah, J. Ahmad, M. A. Khan, M. S. Alshehri, W. Boulila, A. Koubaa, S. U. Jan, and M. M. Iqbal Ch, "TNN-IDS: Transformer neural network-based intrusion detection system for MQTT-enabled IoT networks," *Comput. Netw.*, vol. 237, Dec. 2023, Art. no. 110072.

[15] L. Nie, Y. Wu, X. Wang, L. Guo, G. Wang, X. Gao, and S. Li, "Intrusion detection for secure social Internet of Things based on collaborative edge computing: A generative adversarial network-based approach," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 1, pp. 134–145, Feb. 2022.

[16] M. Maray, H. M. Alshahrani, K. A. Alissa, N. Alotaibi, A. Gaddah, A. Meree, M. Othman, and M. Ahmed Hamza, "Optimal deep learning driven intrusion detection in SDN-enabled IoT environment," *Comput., Mater. Continua*, vol. 74, no. 3, pp. 6587–6604, 2023.

[17] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16492–16503, Sep. 2022.

[18] H. Shah, D. Shah, N. K. Jadav, R. Gupta, S. Tanwar, O. Alfarraj, A. Tolba, M. S. Raboaca, and V. Marina, "Deep learning-based malicious smart contract and intrusion detection system for IoT environment," *Mathematics*, vol. 11, no. 2, p. 418, Jan. 2023.

[19] S. Perumalla, S. Chatterjee, and A. P. S. Kumar, "Modelling of oppositional Aquila optimizer with machine learning enabled secure access control in Internet of Drones environment," *Theor. Comput. Sci.*, vol. 941, pp. 39–54, Jan. 2023.

[20] A. Fatani, A. Dahou, M. Abd Elaziz, M. A. A. Al-qaness, S. Lu, S. A. Alfadhli, and S. S. Alresheedi, "Enhancing intrusion detection systems for IoT and cloud environments using a growth optimizer algorithm and conventional neural networks," *Sensors*, vol. 23, no. 9, p. 4430, Apr. 2023.

[21] X. Wang, B. Li, X. Su, H. Peng, L. Wang, C. Lu, and C. Wang, "Autonomous dispatch trajectory planning on flight deck: A search-resampling-optimization framework," *Eng. Appl. Artif. Intell.*, vol. 119, Mar. 2023, Art. no. 105792.

[22] X. Gao, L. Wang, X. Yu, X. Su, Y. Ding, C. Lu, H. Peng, and X. Wang, "Conditional probability based multi-objective cooperative task assignment for heterogeneous UAVs," *Eng. Appl. Artif. Intell.*, vol. 123, Aug. 2023, Art. no. 106404.

[23] D. Chulerttiyawong and A. Jamalipour, "Sybil attack detection in Internet of Flying Things-IoFT: A machine learning approach," *IEEE Internet Things J.*, 2023.

[24] C. Pu and P. Zhu, "Defending against flooding attacks in the Internet of Drones environment," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[25] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, "Passive rule-based approach to detect sinkhole attack in RPL-based Internet of Things networks," *IEEE Access*, vol. 11, pp. 94081–94093, 2023.

[26] D. Ramachandran, S. Naqi, G. Perumal, and Q. Abbas, "DLTN-LOSP: A novel deep-linear-transition-network-based resource allocation model with the logic overhead security protocol for cloud systems," *Sensors*, vol. 23, no. 20, p. 8448, Oct. 2023.

[27] 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, pp. 18715–18757, Feb. 2023.

[28] B. Yan and G. Han, "Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system," *IEEE Access*, vol. 6, pp. 41238–41248, 2018.

[29] W. Zilong and S. Peng, "A multi-strategy dung beetle optimization algorithm for optimizing constrained engineering problems," *IEEE Access*, vol. 11, pp. 98805–98817, 2023.

[30] V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea, S. Y. Alyahyan, and M. A. Raza, "Optimal deep reinforcement learning for intrusion detection in UAVs," *Comput., Mater. Continua*, vol. 70, no. 2, pp. 2639–2653, 2022.