IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 September 2023, accepted 18 September 2023, date of publication 22 September 2023,
date of current version 9 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3318176

RESEARCH ARTICLE

Modified Equilibrium Optimization Algorithm With Deep Learning-Based DDoS Attack Classification in 5G Networks

MOHAMMED ALJEBREEN[1], FATMA S. ALRAYES[2], MOHAMMED MARAY[3], SUMAYH S. ALJAMEEL[4], AHMED S. SALAMA[5], AND ABDELWAHED MOTWAKEL[6]

[1]Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia
[2]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[3]Department of Information Systems, College of Computer Science, King Khalid University, Abha 62529, 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 & Technology, Future University in Egypt, New Cairo 11845, Egypt
[6]Department of Information Systems, College of Business Administration in Hawtat Bani Tamim, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding author: Abdelwahed Motwakel (am.ismaeil@psau.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 235 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSP2023R459), King Saud University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is partially funded by the Future University in Egypt (FUE).

ABSTRACT 5G networks offer high-speed, low-latency communication for various applications. As 5G networks introduce new capabilities and support a wide range of services, they also become more vulnerable to different kinds of cyberattacks, particularly Distributed Denial of Service (DDoS) attacks. Effective DDoS attack classification in 5G networks is a critical aspect of ensuring the security, availability, and performance of these advanced communication infrastructures. In recent days, machine learning (ML) and deep learning (DL) models can be employed for an accurate DDoS attack detection process. In this aspect, this study designs a Modified Equilibrium Optimization Algorithm with Deep Learning based DDoS Attack Classification (MEOADL-ADC) method in 5G networks. The goal of the MEOADL-ADC technique is the automated classification of DDoS attacks in the 5G network. The MEOADL-ADC technique follows a three-stage process such as feature selection, classification, and hyperparameter tuning. Primarily, the MEOADL-ADC technique employs MEOA based feature selection approach. Next, the MEOADL-ADC technique utilizes the long short-term memory (LSTM) model for the classification of DDoS attacks. Finally, the tunicate swarm algorithm (TSA) is exploited to adjust the hyperparameter of the LSTM model. The design of MEOA-based feature selection and TSA-based hyperparameter tuning shows the novelty of the work. The experimental outcome of the MEOADL-ADC method is tested on a benchmark dataset, and the outcomes indicate the betterment of the MEOADL-ADC algorithm over the current methods with maximum accuracy of 97.60%.

INDEX TERMS 5G networks, DDoS attack mitigation, security, deep learning, feature selection, tunicate swarm algorithm.

I. INTRODUCTION

Mobile devices, including IoT and traffic carried over wireless networks, are quickly increasing and are driven by several aspects [1]. The telecom sector is experiencing a transformation towards 5G networks for fulfilling the necessities of emerging and existing use cases [2]. Hence, the idea of a 5G wireless network lies in rendering higher coverage and high data rates using dense base station deployments with extremely low latency, high capacity, and better Quality of

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

Service (QoS) [3]. The provision of the essential services that 5 G envisions needs new networking structures, service deployment methods, and processing and storage technology described [4]. Such technologies must provide novel difficulties for the functionality of 5G cybersecurity systems [5]. The 5G data networks would connect critical structures that need a higher level of security for ensuring not the safety of the respective infrastructure but also society's safety [6]. For instance, a security breach in the online power supply system can be terrible for each electrical and electronic system that the community relies upon [7]. Hence, in 5G networks, it is significant to highlight and examine the security challenges and build an overview relevant to the latent solutions that resulted in the model of secure 5G systems [8].

Denial-of-service (DoS) attack targets the accessibility of network resources in a region and likely razes a network [9] in case there are many attacks in a well-synchronized and dispersed manner termed distributed denial-of-service (DDoS) attacks. As per Verizon's report, DDoS attacks topped the list of recurrent cybersecurity events in 2017 [10]. It is designed as a smoke screen or beachhead for IT security experts, with other objectives (for instance, data breach) can be established: in cellular networks, the DDoS attack cannot deeply affect the network and its authorized users but have side effects in disturbing 5G that depends on the networks [11]. There is a recent increase of interest and clamour, among research scholars from both industry and academia [12], in using DL or AI for protecting 5G networks—particularly the ones used in critical structures like financial networks, smart grids, etc.—from cyber-attacks [13].

This study designs a Modified Equilibrium Optimization Algorithm with Deep Learning based DDoS Attack Classification (MEOADL-ADC) method in 5G networks. The presented MEOADL-ADC technique employs MEOA based feature selection approach. Next, the MEOADL-ADC technique utilizes the long short-term memory (LSTM) model to detect and classify DDoS attacks. Finally, the tunicate swarm algorithm (TSA) is exploited to adjust the hyperparameter of the LSTM model. The experimental validation of the MEOADL-ADC algorithm is tested on a benchmark dataset.

II. RELATED WORKS

Aldhyani and Alkahtani [14] modelled potential and adaptable IDS through the structures of LSTM and CNN integrated with LSTM (CNN–LSTM) to identify DDoS attacks. The CIC-DDoS2019 datasets have been utilized to devise a proposal to find various DDoS attacks. In [15], modelled a DL-related IDS system for DDoS attacks depends on 3 methods they are RNN, CNN, and DNN. The performance of the model is learned within two classifier kinds (multi-class and binary) utilizing two real traffic datasets TON_IoT dataset and CIC-DDoS2019 dataset. Alashhab et al. [16] presented an LDDoS attack detection method related to the DL technique that has an activation function of the LSTM for identifying different kinds of LDDoS attacks in IoT networks by examining the various kinds of natural traffic and LDDoS attacks, enhancing the precision of LDDoS attack recognition, and minimize the malicious traffic flow.

In [17], the authors introduced the application of a flexible and modular SDN-related structure for detecting application and transport layer DDoS attacks utilizing multiple DL and ML methods. Exploring different DL or ML techniques enabled techniques execute better under different attack kinds and conditions. Jullian et al. [18] apply a distributed structure that depends on DL to avoid diverse sources of vulnerability at once under the same protection mechanism. Both DL methods were assessed: LSTM and feed forward-NNs. In [19], utilize the Bot-IoT data to frame new IDS related to DL and ML methods, which addresses its class imbalance issue. For assessing how it records timestamps and affects forecasting, the author utilized 3 different feature sets for binary and multi-class classification since this aids to prevent feature dependency.

Ayala and Salcedo [20] introduced a security method for 5G Networks wireless access (5GDoSec) for identifying possible intruders and malicious users using the DNN and the ML method; this depends on the access data gathered from a delimited entrance point that groups, classify and identify the authenticated users in the network to identify, based on the active time and the access numbers, the ones that denote a threat. In [21], modelled a novel cognitive closed loop system for rendering distributed dual-layer self-protection abilities to fight against DDoS attacks. Infrastructure Service Providers (ISPs) and Digital Service Providers (DSPs) are systems that feature concurrent autonomous closed loops for various stakeholders' business roles.

In [22], a deep intelligent DDoS attack detection scheme (DI-ADS) was presented for fog-based IoT applications. This structure mostly utilizes a DL method for detecting DDoS attacks from the network. The DLM was fixed on the computation element of the fog node, which forecasts the end IoT device performance. In [23], an LSTM-based method (LSTM-CLOUD) that is planned to detect and prevent DDoS attacks from the public cloud network platform is presented. The proposal of the scheme was dependent upon a signature-based attack detection method. Sayed et al. [24] examine a multi-classifier approach utilizing stacking ensemble DNNs which recognize many kinds of DDoS attacks for addressing the problems abovementioned. Shieh et al. [25] present a novel DDoS detection structure featuring Bi-LSTM, a Gaussian Mixture Model (GMM), and incremental learning.

Though several ML and DL models for DDoS attack classification are available in the literature, it is still needed to enhance the classification performance. Owing to the continual deepening of the model, the number of parameters of DL models also increases quickly which results in model overfitting. At the same time, different hyperparameters have a significant impact on the efficiency of the DL model. Particularly, hyperparameters such as epoch count, batch size, and learning rate selection are essential to attain effectual outcomes. Since the trial and error method for hyperparameter tuning is a tedious and erroneous process, metaheuristic algorithms can be applied. Therefore, in this work, we employ the TSA algorithm for the parameter selection of the LSTM model.

III. THE PROPOSED MODEL

This study introduced a new MEOADL-ADC method for effective DDoS attack classification in the 5G networks. Fig. 1 defines the working process of the MEOADL-ADC method. It comprises feature selection and an optimal classification process. The MEOADL-ADC technique uses feature selection and hyperparameter tuning processes to attain enhanced detection results. In addition, the MEOADL-ADC technique performs three significant processes, namely MEOA-based feature subset selection, LSTM-based classification, and TSA-based hyperparameter tuning.

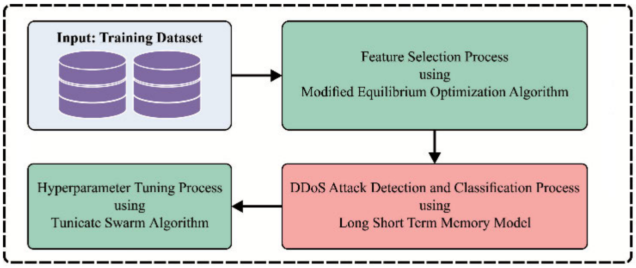
Input: Training Dataset
Feature Selection Process
using
Modified Equilibrium Optimization Algorithm
DDoS Attack Detection and Classification Process
using
Long Short Term Memory Model
Hyperparameter Tuning Process
using
Tunicate Swarm Algorithm

FIGURE 1. Working process of the MEOADL-ADC approach.

A. DESIGN OF MEOA-BASED FEATURE SELECTION

Primarily, the MEOA is applied for the optimal selection of feature subsets. EOA was introduced by using the equilibrium of dynamic mass for controlling the volume via exploring the balanced state of the model to resolve the optimization problem [26]. EOA refers to an optimization technique due to its many benefits, namely the better balancing of exploitation and exploration searches, good population diversity, and simplicity of implementation. Even with the offered benefits, EO has the disadvantage of lacking consideration on fitness assignments. It cannot satisfy the conflicting goals brought by multi-objective functions owing to a higher tendency to reach equilibrium in a single objective and fails in the rest. To resolve the disadvantages of EOA, the MEOA was introduced to handle optimum feature selection that can be expressed as multi-objective optimization problems. The presented method exploits a hyperlearning algorithm that leverages the concept of personal worst and best states in the solution upgrading procedure to solve the multi-objective feature selection problems. Without losing generalization, MEOA includes n sub-swarms of the location vector represented as X to find the optimal set of features concerning the fitness value of the candidate solution. Every sub-swarm of MEOA has a similar search mechanism to the single-swarm EOA. The presented MEOA use the advantages of an external shared pool to ease the sharing of equilibrium state experience between the subswarms when compared with single swarm EOA, which enables the particle to approach the Pareto front further.

The search procedure of the presented method can be defined in the following. In the early stage of the optimization method, the initial location of all the *i-th* particles, viz., X_i for $i = 1, 2, \ldots, n_p$, is generated using Eq. (21):

$$X_{initial} = rand(n_p, d) \times (ub - lb) + lb \tag{1}$$

whereas n_p refers to the dimensional population, lb and ub signify lower and upper boundaries of search space; d represents the dimensional size of the problem. Afterwards completing the initialized procedure, the 4 optimum equilibrium particles (*for instance*, $X_{eq,1}, X_{eq,2}, X_{eq,3}, X_{eq,4}$) and the average position (*that is*, $X_{eq,av}$) of populations can be recognized for constructing an equilibrium pool $X_{eq,poo1}$ which offers many promising search patterns as:

$$X_{eq,pool} = \left(X_{eq,1}, X_{eq,2}, X_{eq,3}, X_{eq,4}, X_{eq,av}\right) \tag{2}$$

For every iteration, the original location X_{old} of every particle from the sub-swarm is upgraded by connecting with solution member X_{eq} was arbitrarily chosen in an equilibrium $X_{eq,pool}$. The solution upgrading processes of every particle is obtained as:

$$X_{new} = X_{eq} + \frac{G}{\lambda}(1 - F) + \left(X_{old} - X_{eq}\right) \times F \tag{3}$$

$$F = a_1 sign\,(r - 0.5)\left(e^{-\lambda t} - 1\right) \tag{4}$$

In which, X_{old} and X_{new} define the present and novel location vector of particles, correspondingly; r demonstrates the random integer ranges from zero to one; $a1$ is constant (i.e., $a1 = 2$); λ refers to the random vector with values ranging from zero to one. An iteration counter t is measured as:

$$t = (1 - \frac{T}{T_{\max}})^{a_2\left(\frac{T}{T_{\max}}\right)} \tag{5}$$

whereas a_2 refers to the constant (for instance , $a_2 = 1$); $T_{\max}$ and T imply the maximal and present iteration counts correspondingly. The generation rate G is achieved as:

$$G = \begin{cases} 0.5\, r_1 & if\ r_2 \geq GP \\ 0 & if\ r2 < GP \end{cases} \tag{6}$$

In which r_1 and r_2 indicate the random number between zero and one, GP represents a generation probability and is fixed as 0.5.

The presented MEOA was improved in EOA by the combination of external archive dominance conditions for determining a suitable group of solutions for tackling the multi-objective optimizer problems, which are commonly defined as:

$$\begin{aligned} &\text{Min } F(X) = \{f_1(x), f_2(x), \ldots, f_n(x)\} \\ &Subjected\ to\text{:} \begin{cases} g_i(X) \leq 0 & i = 1, 2, \ldots - q \\ h_i(X) = 0 & i = 1, 2, \ldots l \end{cases} \end{aligned} \tag{7}$$

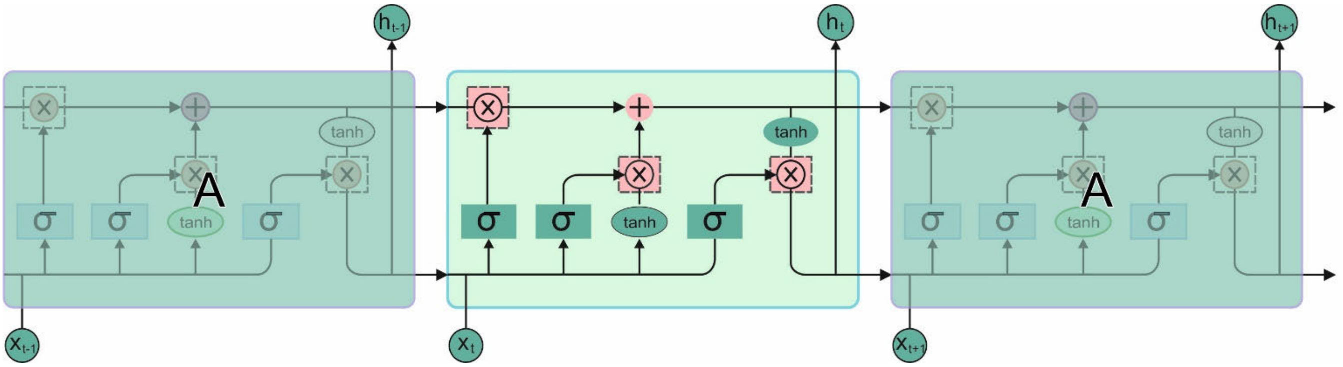

FIGURE 2. Structure of LSTM [27].

Here $F(x)$ denotes the vector of multi-objective functions; $h_i(X)$ and $g_i(X)$ represent q and l inequality and equality constraints, correspondingly. A novel solution set was upgraded and detected in the external archive in all iterations. This archive upgrading procedure enabled the interchange of valuable data among particles at the time of the optimizer model.

The solution quality of all equilibrium particles was iteratively assessed through the multi-objective functions for defining an optimum set of features from every generated feature. Here, two objective functions of reducing the number of selected features $S(X)$ and reducing the classification error ER (X) are proposed to resolve the feature selection problem:

$$Minimize: ER\ (X), \quad S(X)\, X \in R^n \tag{8}$$

Without losing generalization, the fitness function (FF) utilized for assessing the quality of all particles is shown as follows below:

$$\downarrow Fit = \alpha ER + \beta \left(\frac{|S|}{|O|}\right) \tag{9}$$

In Eq. (9), $|O|$ and $|S|$ indicate the dimensional of the original feature set and feature selection subset, correspondingly; the two weight infectors α and β denote the influence of classifier error and dimensional of feature selection on FF, whereas $\alpha\varepsilon[0, 1]$ and $\beta = 1 - \alpha$.

B. DDOS ATTACK DETECTION USING OPTIMAL DL MODEL

This work uses the LSTM model for the DDoS attack detection process. Owing to the existence of recurrent connections in the LSTM network is selected that facilitates memorization of received data [27]. These characteristics allow LSTM to learn the long-term dependency, thus overcoming the backflow and gradient disappearance drawback. RNN is provided to estimate the vague consecutive pattern of the spatial and temporal consecutive data. Moreover, the connection of the peephole allows LSTM to recognize the timed pattern precisely and calculate the internal state from the weight and cost matrices.

Fig. 2 demonstrates the multilayer structure of LSTM used to enhance the accuracy of DNN, in which activation data in the 1st layer is given to the 2nd layer for additional processing to the time series problem. By linking the LSTM layer, all the layers from the LSTM is a hierarchical structure that attains input in the HL of the prior layer. The training of multi-layer LSTM identifies the sequence pattern of time sequences. Thus, the architecture of interconnected multi-memory cells is presented for recognizing the long-term sequence and dependency of time sequences. Layer 1 of multi-layer LSTM proceeds input in the dataset C_{t-1}, while layer 2 is attained in the prior time step of $h_{t-1}^{(2)}$. Also, the results of the current time step of layer 1, viz., $h_t^{(1)}$. The mathematical formulations describe the mechanism of LSTM cell, and it is defined by Eq. (10):

$$\alpha_t = \sigma\left(W_\alpha \cdot [h_{t-1}, x_t] + b_\alpha\right) \tag{10}$$

where $[\cdot]$ denotes the concatenate operation; σ denotes the sigmoid function, W_α indicates the weight matrix of $\alpha - th$ layer and β_t and γ_t represent as input gate and tanh layers, correspondingly:

$$\beta_t = \sigma\left(W_\beta \cdot [h_{t-1}, x_t] + b_\beta\right) \tag{11}$$

$$\gamma_t = \tanh\left(W_\gamma \cdot [h_{t-1}, x_t] + b_\gamma\right) \tag{12}$$

Meanwhile, the existing state C_t is upgraded from the prior state C_{t-1}:

$$C_t = \alpha_t \cdot C_{t-1} + \beta_t \cdot \gamma_t \tag{13}$$

The output gate of the sigmoid function is represented by 0_t, it is evaluated as follows:

$$o_t = \sigma\left(W_o \cdot [h_{t-1}, x_t] + b_o\right) \tag{14}$$

Referring to C_t and 0_t, the existing hidden state of h_t is evaluated as follows:

$$h_t = o_t tanh\left(C_t\right) \tag{15}$$

In Eq. (15), the related layer bias was denoted by b_α, b_β, b_γ, and b_o; the related layer weight is characterised by W_α, W_β, W_γ, and W_o. Lastly, the final state of LSTM is defined by the softmax activation function as:

$$h_{final} = softmax\left(h_t\right) \tag{16}$$

Algorithm 1 Pseudocode of TSA

```
Input: Tunicate population $T_i (i = 1, 2, 3, \ldots pop)$
Output: Optimum tunicate individual
Procedure: $YSA$
Initialize variables $X_{min}, X_{\max}$, etc.
Evaluate the fitness values of all the tunicates
$\overrightarrow{T_{source}}$ identifies the better tunicate individual
    While (iteration $< Mak_{iterations}$) do
    for $i = 1$ to pop, do Upgrade the location of every tunicate by Eq. (23).
    End for
    Upgrade parameters ($\overrightarrow{A}$, $\overrightarrow{G}$, $\overrightarrow{F}$, and $\overrightarrow{M}$
    Check individual tunicate
    Upgrade $T_i$ if there is the best solution than the
    Preceding optimum solution
    Iteration ← iteration + 1
    End while
Return $T_i$
End
```

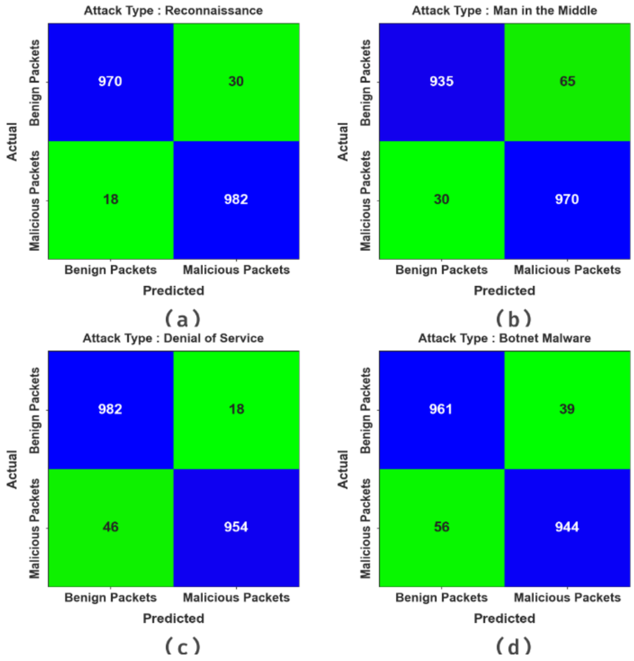

FIGURE 3. Confusion matrices of MEOADL-ADC method (a) Reconnaissance, (b) Man in the Middle, (c) DoS, and (d) Botnet Malware.

To modify the hyperparameter values of the LSTM, the TSA is used. The TSA is a new bio-inspired metaheuristic algorithm [28]. Tunicates stimulated TSA. Tunicates are marine creatures that can locate food sources in the sea. Tunicate navigates and forages for food with the help of two major strategies: swarm intelligence and jet propulsion. In the mathematical expression, a tunicate move to the best position and remains closer to the better individual while avoiding conflicts between the individual members. In herd behaviour, population member updates their position based on the better individual population.

TABLE 1. Details of database.

Class	Attack Type			
	Reconnaissance	Man in the Middle	Denial of Service	Botnet Malware
Benign Packets	1000	1000	1000	1000
Malicious Packets	1000	1000	1000	1000
Total Number of Samples	2000	2000	2000	2000

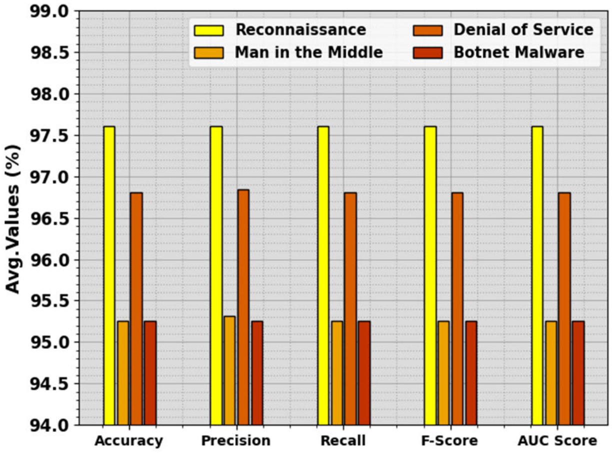

FIGURE 4. The average outcome of the MEOADL-ADC approach under varying attack types.

1) MATHEMATICAL MODEL OF JET PROPULSION

These behaviours are developed to ensure the social balance of power amongst tunicates and prevent collisions between them.

$$\overrightarrow{A} = \frac{\overrightarrow{G}}{\overrightarrow{M}} \tag{17}$$

$$\overrightarrow{G} = r_2 + r_3 - \overrightarrow{F} \tag{18}$$

$$\overrightarrow{F} = 2.r_1 \tag{19}$$

$$\overrightarrow{M} = \lfloor X_{\min} + r_1 \cdot X_{\max} - X_{\min} \rfloor \tag{20}$$

where $X_{\min}$ and $X_{\max}$ values are taken as 1 and 4, correspondingly. Essential parameter analyses were introduced by Kaur et al. In this study, a parameter analysis wasn't implemented for this value.

The movement of population members toward the better neighbouring direction

$$\overrightarrow{T_{d\imath stance}} = \left| \overrightarrow{T_{source}} - r \cdot \overrightarrow{T\,(x)} \right| \tag{21}$$

In Eq. (21), $\overrightarrow{T_{d\imath stance}}$ represents the distance between the food source and the population individual, x signifies the existing iteration, $\overrightarrow{T_{source}}$ indicates the location of the food source (the location of better tunicate), $\overrightarrow{T(x)}$ shows the tunicate position and r shows the randomly generated

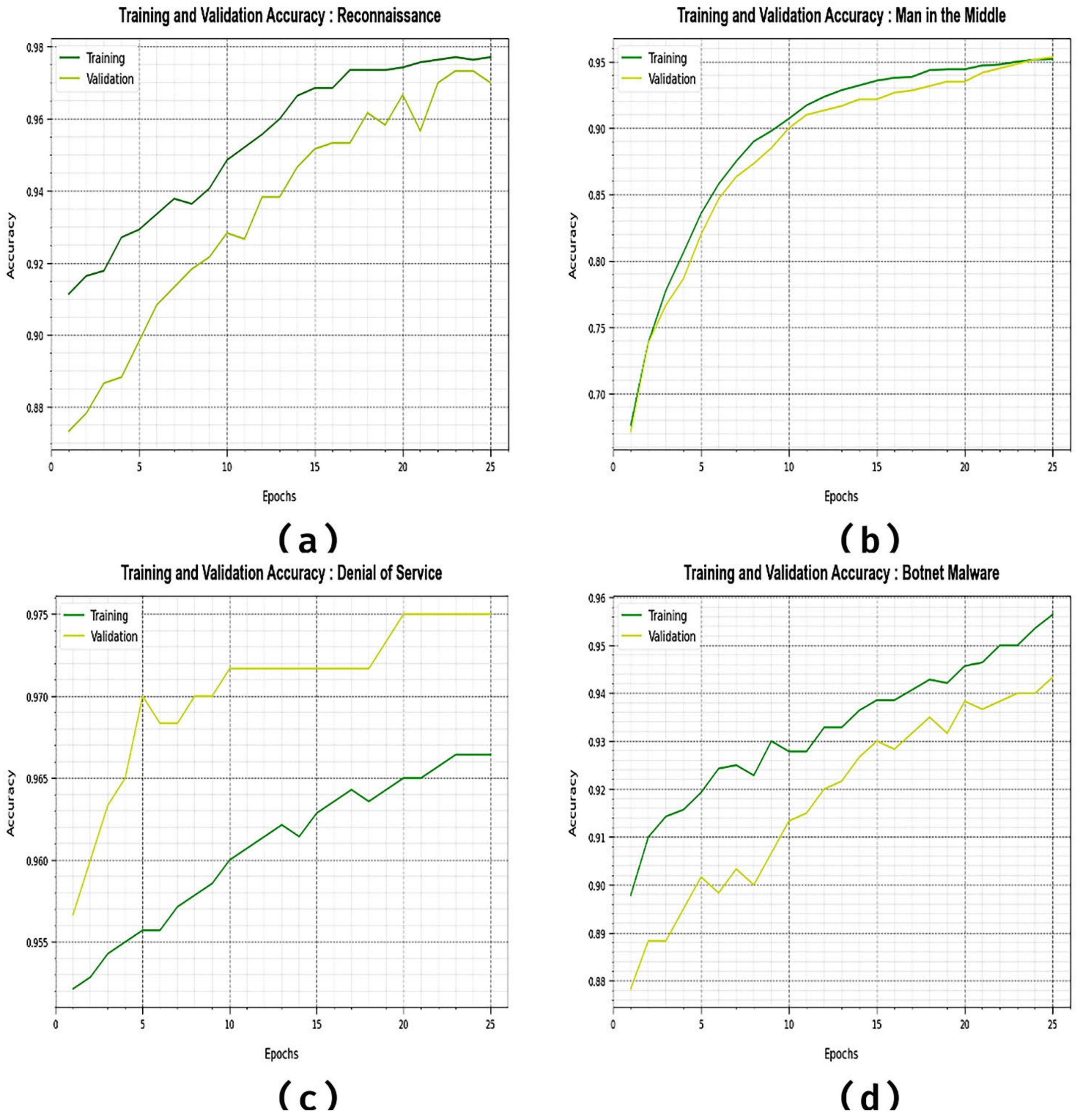

FIGURE 5. Accuracy curve of MEOADL-ADC approach (a) Reconnaissance, (b) Man in the Middle, (c) DoS, and (d) Botnet Malware.

value [0, 1].

$$\overrightarrow{T(x')}=\begin{cases}\overrightarrow{T_{source}}+\overrightarrow{A}\cdot\overrightarrow{T_{d\imath stance}}, & if\ r\geq 0.5\\ \overrightarrow{T_{source}}+\overrightarrow{A}\cdot\overrightarrow{T_{d\imath stance}}, & if\ r<0.5\end{cases}\tag{22}$$

where $\overrightarrow{T(x')}$ denotes the updated $\overrightarrow{T(x)}$ (tunicate position) concerning $\overrightarrow{T_{source}}$ (the food source position), and r represents the randomly generated value [0, 1].

Mathematical Model of Swarm Behavior.

The herding behaviour of tunicate is demonstrated below:

$$T\left(\overrightarrow{x}+1\right)=\frac{\overrightarrow{T\left(x'\right)}+T\left(\overrightarrow{x}-1\right)}{2+r1}\tag{23}$$

Fitness selection has become a main factor in the TSA approach. Solution encoding is utilized to calculate the goodness (aptitude) of the candidate solution. The accuracy value is the crucial condition used to design the fitness

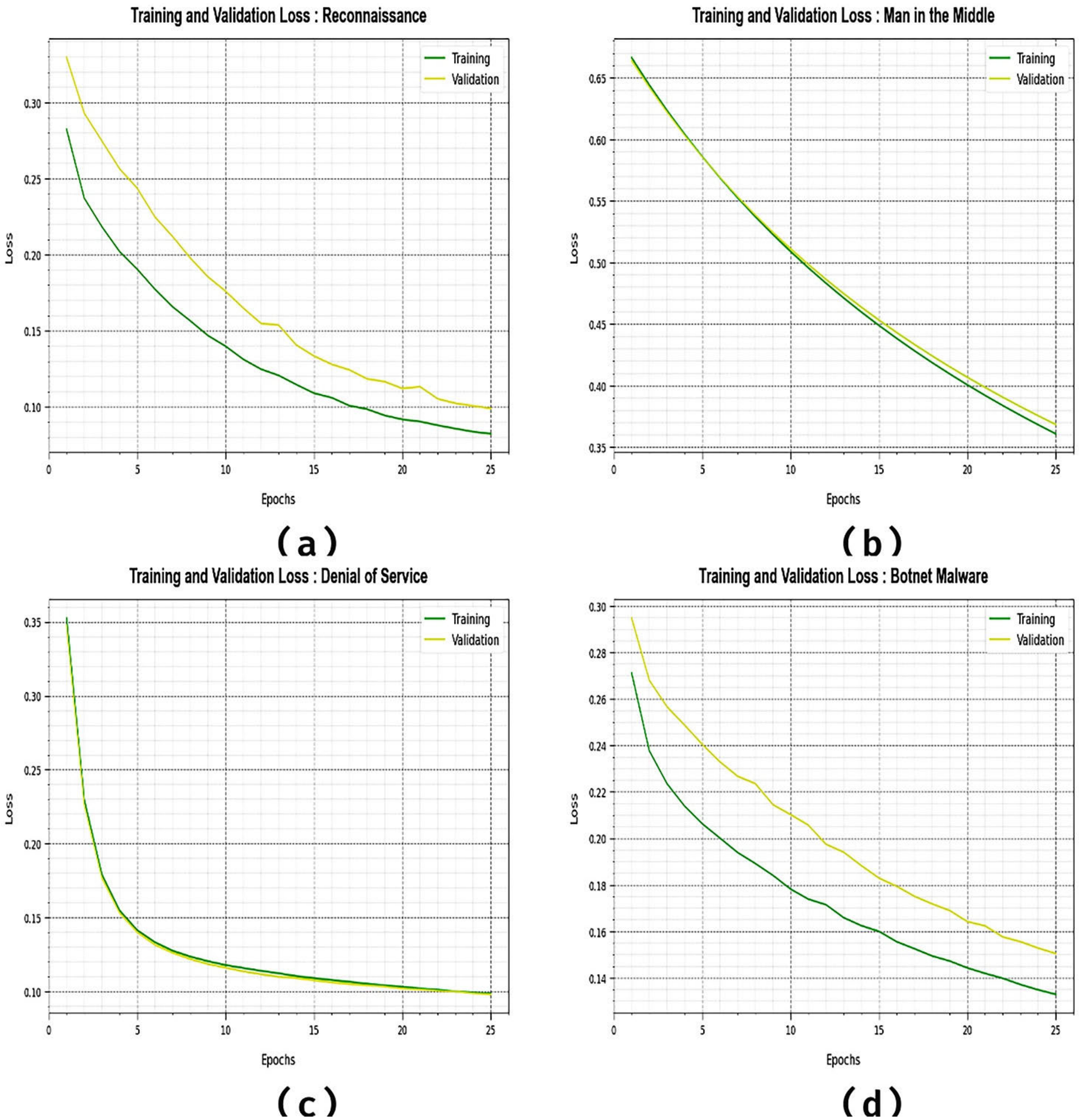

FIGURE 6. Loss curve of MEOADL-ADC approach (a) Reconnaissance, (b) Man in the Middle, (c) DoS, and (d) Botnet Malware.

function.

$$Fitness = \max(P) \tag{24}$$

$$P = \frac{TP}{TP + FP} \tag{25}$$

where TP represent the true positive, and FP symbolizes the false positive value.

IV. PERFORMANCE VALIDATION

The proposed model is simulated using the Python tool. In this study, the DDoS attack detection performance of the MEOADL-ADC technique is tested on the Kitsune Network Attack Dataset [29], available at https://www.kaggle.com/datasets/ymirsky/network-attack-dataset-kitsune. The Kitsune dataset provides a total of 21,017,596 network packets for 9 individual attacks among 4 types of real network intrusion attacks. It includes network packets of similar IPs (unlike other datasets that use different IPs) for each attack on normal and malicious traffic. For experimental validation, in this work, we have chosen 8000 samples with four types of attacks, as defined in Table 1. Each attack has two subclasses, namely benign and malicious.

TABLE 2. Attack type classification outcome of the MEOADL-ADC approach.

Attack Type: Reconnaissance					
Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
Benign Packets	97.00	98.18	97.00	97.59	97.60
Malicious Packets	98.20	97.04	98.20	97.61	97.60
Average	97.60	97.61	97.60	97.60	97.60
Attack Type: Man in the Middle					
Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
Benign Packets	93.50	96.89	93.50	95.17	95.25
Malicious Packets	97.00	93.72	97.00	95.33	95.25
Average	95.25	95.31	95.25	95.25	95.25
Attack Type: Denial of Service					
Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
Benign Packets	98.20	95.53	98.20	96.84	96.80
Malicious Packets	95.40	98.15	95.40	96.75	96.80
Average	96.80	96.84	96.80	96.80	96.80
Attack Type: Botnet Malware					
Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}
Benign Packets	96.10	94.49	96.10	95.29	95.25
Malicious Packets	94.40	96.03	94.40	95.21	95.25
Average	95.25	95.26	95.25	95.25	95.25

TABLE 3. Comparative outcome of the MEOADL-ADC model [30].

Methods	$Accu_y$	$F1_{score}$
MEOADL-ADC	97.60	97.60
K-Means ++	92.62	91.02
ANN Algorithm	92.28	90.20
NB Algorithm	95.09	93.18
KNN Algorithm	44.72	26.57
SVM Algorithm	50.00	16.67
RF Algorithm	62.48	58.86
Stacking	62.65	29.83

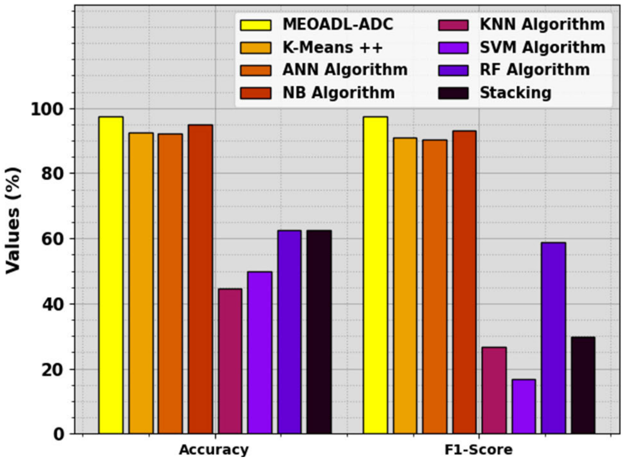

FIGURE 7. $Accu_y$ and F_{score} analysis of the MEOADL-ADC approach with other techniques.

The confusion matrices of the MEOADL-ADC technique are shown in Fig. 3. The outcomes identified that the MEOADL-ADC technique recognizes benign and malicious packets. For instance, the MEOADL-ADC technique recognized 970 benign and 982 malicious packets on reconnaissance attacks. Next, the MEOADL-ADC system recognized 935 benign and 970 malicious packets on man-in-the-middle attacks. Simultaneously, the MEOADL-ADC method recognized 982 benign and 954 malicious packets on denial of service attacks. Finally, the MEOADL-ADC method detected 961 benign and 944 malicious packets in a botnet malware attack.

Table 2 and Fig. 4 report the overall attack type classification results of the MEOADL-ADC technique. The results stated that the MEOADL-ADC technique identified benign and malicious packets.

For instance, on reconnaissance attack, the MEOADL-ADC technique gained an average $accu_y$ of 97.60%, $prec_n$ of 97.61%, $reca_l$ of 97.60%, F_{score} of 97.60%, and AUC_{score} of 97.60%. Meanwhile, on man in the middle attack, the MEOADL-ADC system gained an average $accu_y$ of 95.25%, $prec_n$ of 95.31%, $reca_l$ of 95.25%, F_{score} of 95.25%, and AUC_{score} of 95.25%. Moreover, on denial of service attack, the MEOADL-ADC method gained an average $accu_y$ of 96.80%, $prec_n$ of 96.84%, $reca_l$ of 96.80%, F_{score} of 96.80%, and AUC_{score} of 96.80%. At last, on botnet malware attack, the MEOADL-ADC algorithm gained an average $accu_y$ of 95.25%, $prec_n$ of 95.26%, $reca_l$ of 95.25%, F_{score} of 95.25%, and AUC_{score} of 95.25%.

Fig. 5 examines the accuracy of the MEOADL-ADC method during the training and validation process under varying attack types. The figure notifies that the MEOADL-ADC technique reaches increasing accuracy values over increasing epochs. Furthermore, the increasing validation accuracy over training accuracy shows that the MEOADL-ADC technique learns effectively under varying attack types.

The loss analysis of the MEOADL-ADC technique at the time of training and validation is demonstrated under varying attack types in Fig. 6. The outcomes indicate that the MEOADL-ADC technique reaches closer values of training and validation loss. It is observed that the MEOADL-ADC technique learns efficiently under varying attack types.

Table 3 and Fig. 7 show a comparative $accu_y$ and F_{score} examination of the MEOADL-ADC technique [30]. The results indicate the betterment of the MEOADL-ADC technique in terms of $accu_y$ and F_{score}. Based on $accu_y$, the MEOADL-ADC technique gains an increasing $accu_y$

of 97.60% while the K-means++, ANN, NB, KNN, SVM, RF, and stacking models obtain decreasing $accu_y$ of 92.62%, 92.28%, 95.09%, 44.72%, 50%, 62.48%, and 62.65% respectively.

Besides, based on the F_{score}, the MEOADL-ADC method gains increasing F_{score} of 97.60% while the K-means++, ANN, NB, KNN, SVM, RF, and stacking approaches attain decreasing F_{score} of 91.02%, 90.20%, 93.18%, 26.57%, 16.67%, 58.86%, and 29.83% correspondingly. Therefore, the MEOADL-ADC technique demonstrated enhanced performance over other models on the DDoS attack detection process in the 5G environment.

V. CONCLUSION

In this study, a new MEOADL-ADC method was introduced for effective DDoS attack classification in 5G networks. The presented MEOADL-ADC technique makes use of feature selection and hyperparameter tuning processes to attain enhanced detection results. In addition, the MEOADL-ADC technique performs three major processes: MEOA-based feature subset selection, LSTM-based classification, and TSA-based hyperparameter tuning. The experimental outcomes of the MEOADL-ADC algorithm are tested on a benchmark dataset, and the outcomes indicate the betterment of the MEOADL-ADC method over the recent algorithms. The proposed model forms a key part of the overall network security strategy to safeguard the potential of 5G networks in delivering high-speed, low-latency communication while maintaining robust protection against malicious activities. Hence, the MEOADL-ADC approach can be applied for an accurate DDoS attack detection technique. In the upcoming years, the performance of the MEOADL-ADC approach can be boosted by the design of outlier removal methodologies.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 235 /44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSP2023R459), King Saud University, Riyadh, Saudi Arabia. We Would like to thank SAUDI ARAMCO Cybersecurity Chair for funding this project. This study is partially funded by the Future University in Egypt (FUE).

REFERENCES

[1] L. Lei, L. Kou, X. Zhan, J. Zhang, and Y. Ren, "An anomaly detection algorithm based on ensemble learning for 5G environment," *Sensors*, vol. 22, no. 19, p. 7436, Sep. 2022.

[2] A. S. Rajawat, S. B. Goyal, P. Bedi, S. Kautish, and D. P. Shrivastava, "Analysis assaulting pattern for the security problem monitoring in 5G-enabled sensor network systems with big data environment using artificial intelligence/machine learning," *IET Wireless Sensor Syst.*, Feb. 2023.

[3] T. E. Ali, Y.-W. Chong, and S. Manickam, "Machine learning techniques to detect a DDoS attack in SDN: A systematic review," *Appl. Sci.*, vol. 13, no. 5, p. 3183, Mar. 2023.

[4] D. Said, "Quantum computing and machine learning for cybersecurity: Distributed denial of service (DDoS) attack detection on smart micro-grid," *Energies*, vol. 16, no. 8, p. 3572, Apr. 2023.

[5] S. B. Atitallah, M. Driss, W. Boulila, and I. Almomani, "An effective classification approach for DoS attacks in wireless sensor networks using deep transfer learning models and majority voting," in *Proc. Int. Conf. Comput. Collective Intell.*, Hammamet, Tunisia: Springer, 2022, pp. 180–192.

[6] M. S. Khan, B. Farzaneh, N. Shahriar, N. Saha, and R. Boutaba, "SliceSecure: Impact and detection of DoS/DDoS attacks on 5G network slices," in *Proc. IEEE Future Networks World Forum (FNWF)*, Oct. 2022, pp. 639–642.

[7] I. Ortet Lopes, D. Zou, F. A. Ruambo, S. Akbar, and B. Yuan, "Towards effective detection of recent DDoS attacks: A deep learning approach," *Secur. Commun. Netw.*, vol. 2021, pp. 1–14, Nov. 2021.

[8] H. Kumar, Y. Aoudni, G. G. R. Ortiz, L. Jindal, S. Miah, and R. Tripathi, "Light weighted CNN model to detect DDoS attack over distributed scenario," *Secur. Commun. Netw.*, vol. 2022, pp. 1–10, Jun. 2022.

[9] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network," *Ad Hoc Netw.*, vol. 140, Mar. 2023, Art. no. 103026.

[10] N. Yadav, S. Pande, A. Khamparia, and D. Gupta, "Intrusion detection system on IoT with 5G network using deep learning," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–13, Mar. 2022.

[11] H. Zhou, Y. Zheng, X. Jia, and J. Shu, "Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN," *Comput. Netw.*, vol. 225, Apr. 2023, Art. no. 109642.

[12] A. Wani and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," *CAAI Trans. Intell. Technol.*, vol. 6, no. 3, pp. 281–290, Sep. 2021.

[13] Y. Zhang, Y. Liu, X. Guo, Z. Liu, X. Zhang, and K. Liang, "A BiLSTM-based DDoS attack detection method for edge computing," *Energies*, vol. 15, no. 21, p. 7882, Oct. 2022.

[14] T. H. H. Aldhyani and H. Alkahtani, "Cyber security for detecting distributed denial of service attacks in Agriculture 4.0: Deep learning model," *Mathematics*, vol. 11, no. 1, p. 233, Jan. 2023.

[15] M. A. Ferrag, L. Shu, H. Djallel, and K.-K.-R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in Agriculture 4.0," *Electronics*, vol. 10, no. 11, p. 1257, May 2021.

[16] A. A. Alashhab, M. S. M. Zahid, A. Muneer, and M. Abdukkahi, "Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 11, pp. 1–7, 2022.

[17] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," *IEEE Access*, vol. 9, pp. 108495–108512, 2021.

[18] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, and R. Canal, "Deep-learning based detection for cyber-attacks in IoT networks: A distributed attack detection framework," *J. Netw. Syst. Manag.*, vol. 31, no. 2, p. 33, Apr. 2023.

[19] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models," *Sensors*, vol. 22, no. 9, p. 3367, Apr. 2022.

[20] S. C. V. Ayala and O. J. Salcedo, "5G network access security model through deep neural networks clustering," *J. Eng. Sci. Technol.*, vol. 17, no. 5, pp. 3555–3569, 2022.

[21] P. Benlloch-Caballero, Q. Wang, and J. M. A. Calero, "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks," *Comput. Netw.*, vol. 222, Feb. 2023, Art. no. 109526.

[22] S. P. K. Gudla, S. K. Bhoi, S. R. Nayak, and A. Verma, "DI-ADS: A deep intelligent distributed denial of service attack detection scheme for fog-based IoT applications," *Math. Problems Eng.*, vol. 2022, pp. 1–17, Aug. 2022.

[23] H. Aydin, Z. Orman, and M. A. Aydin, "A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment," *Comput. Secur.*, vol. 118, Jul. 2022, Art. no. 102725.

[24] M. I. Sayed, I. M. Sayem, S. Saha, and A. Haque, "A multi-classifier for DDoS attacks using stacking ensemble deep neural network," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2022, pp. 1125–1130.

[25] C.-S. Shieh, W.-W. Lin, T.-T. Nguyen, C.-H. Chen, M.-F. Horng, and D. Miu, "Detection of unknown DDoS attacks with deep learning and Gaussian mixture model," *Appl. Sci.*, vol. 11, no. 11, p. 5213, Jun. 2021.

[26] M. Abdel-Basset, V. Chang, and R. Mohamed, "A novel equilibrium optimization algorithm for multi-thresholding image segmentation problems," *Neural Comput. Appl.*, vol. 33, no. 17, pp. 10685–10718, Sep. 2021.

[27] M. Alrifaey, W. H. Lim, C. K. Ang, E. Natarajan, M. I. Solihin, M. R. M. Juhari, and S. S. Tiang, "Hybrid deep learning model for fault detection and classification of grid-connected photovoltaic system," *IEEE Access*, vol. 10, pp. 13852–13869, 2022.

[28] B. A. Ş. Emine, "Enhanced tunicate swarm algorithm for big data optimization," *Sakarya Univ. J. Sci.*, vol. 27, no. 2, pp. 313–334, Apr. 2023.

[29] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," 2018, *arXiv:1802.09089*.

[30] Y.-E. Kim, Y.-S. Kim, and H. Kim, "Effective feature selection methods to detect IoT DDoS attack in 5G core network," *Sensors*, vol. 22, no. 10, p. 3819, May 2022.