Transactions on Emerging Telecommunications Technologies

WILEY

RESEARCH ARTICLE

Hybrid Bio-Inspired Combined Deep Learning Model for DDoS Attack Detection in Cloud: A Big Data Perspective

Perumal Radhika | Somasundaram Kamalakkannan

Department of Computer Science, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies, Chennai, Tamilnadu, India

Correspondence: Somasundaram Kamalakkannan (kannan.scs@vistas.ac.in)

Received: 5 May 2025 | **Revised:** 29 September 2025 | **Accepted:** 14 November 2025

Keywords: cloud computing | DDoS attack | improved correlation | map-reduce | WSU-ROA

ABSTRACT

One of the most prevalent attacks that cause significant harm and impair cloud performance is Distributed Denial of Service (DDoS). DDoS attacks pose a significant threat to cloud environments, degrading performance and disrupting services. To address this issue, we propose a hybrid bio-inspired deep learning model for DDoS attack detection that leverages big data analytics in the cloud. The proposed model incorporates a MapReduce framework to efficiently process large-scale network traffic data, extracting crucial features such as raw features, packet-based features, improved correlations, and statistical features. These extracted features are further refined using an improved recursive feature elimination (RFE) method, which selects the most relevant attributes for attack detection. The attack detection phase employs a hybrid classifier (HC) that integrates Long Short-Term Memory (LSTM) and Deep MaxOut (DMO) models. To ensure optimal performance, the weights of LSTM and DMO are fine-tuned using the White Shark Updated Remora Optimization (WSU-ROA), enhancing classification accuracy. The proposed HC + WSU-ROA model outperforms other methods, achieving the highest accuracy of 93.98%, compared to the other existing methods, demonstrating its superior effectiveness in DDoS attack detection.

1 | Introduction

Cloud computing (CC) has revolutionized the way computing resources are accessed and managed, providing users with a broad range of services such as big data storage, hardware devices, operating system applications, and comprehensive network infrastructure [1–3]. It is built on utilitarian computing and offers affordable user services. Although CC offers its users a wide range of services, it lacks in the security aspect [4–6]. The CC environment is vulnerable to several cyber-attacks because of its dispersed and unpredictable nature as well as flaws in virtualization technology. DDoS threats are one of the extremely risky attacks [7, 8].

DDoS is a devastating weapon that sends waves of packets at a host or network, overwhelming it. The attacks stop the services that are operating on the target, which prevents authorized traffic from utilizing its services [9–12]. The following are the main features of DDoS attacks: (a) they are exceedingly difficult to detect since they imitate typical user flow. (b) DDoS threats are cost-effective and may be carried out by a single node with little data flow; moreover, they are not target-sensitive since the attacked node can identify the malicious node [13–15]. This form of attack is initiated by taking advantage of system vulnerabilities with a large amount of inefficient network traffic existing in the specified network resources like memory, bandwidth, and time that cause a major interruption to an individual [16–18].

There are several machine learning (ML)-oriented schemes to detect DDoS assaults in CC. The ability to accurately detect these threats in ML-based systems is a major hurdle [19–21]. ELM is a member of the class of Artificial Neural Networks known

© 2025 John Wiley & Sons Ltd.

as single hidden layer feed forward neural networks (SLFNs), which only have one hidden layer [22–25]. Examples include K-Nearest Neighbor, Support Vector Machine (SVM), clustering, and statistical detection techniques [26, 27]. These current studies reveal that several efforts have been made to offer approaches to deal with this challenge by outlining particular remedies for emerging DDoS assaults [4, 16, 28, 29]. Despite its numerous benefits, CC environments are inherently vulnerable due to their distributed nature, reliance on virtualization technologies, and unpredictable usage patterns. One of the most significant security challenges faced by cloud environments is the threat of Distributed Denial of Service (DDoS) attacks. These attacks can overwhelm cloud systems with excessive traffic, rendering them inaccessible and severely disrupting services. The increasing reliance on cloud-based infrastructure and services has made DDoS attacks one of the most dangerous and prevalent cybersecurity threats, posing a critical risk to both service providers and users. The work addresses the challenge of handling large and high-dimensional data by improving feature extraction and selection, which reduces noise and enhances the model's ability to focus on the most relevant traffic patterns. This work aims to fill that gap by proposing a hybrid bio-inspired deep learning model that leverages big data analytics, optimized feature selection (FS), and a combination of Long Short-Term Memory (LSTM) and Deep MaxOut (DMO) models to enhance DDoS detection accuracy and efficiency, thereby improving the security and reliability of cloud environments.

This work includes the below contributions:

- Improved correlation features are deployed in this work with the inclusion of the proposed hybrid distance evaluation.
- Selects appropriate features via weightage-based improved RFE.
- Performs attack detection using a hybrid classifier that combines models like LSTM and DMO, whose weights are chosen via the White Shark Updated Remora Optimization Algorithm (WSU-ROA) algorithm.

Research Questions:

1. How can a hybrid deep learning model, leveraging big data analytics, be used to accurately and efficiently detect DDoS attacks in cloud environments?
2. How does the WSU-ROA algorithm optimize the performance of a hybrid deep learning model for DDoS detection, and what impact does this have on detection accuracy?

Section 2 discusses the existing works on DDOS AD in the cloud. An overview of developed DDOS AD in the cloud is mentioned in Sections 3 and 4 which explain data generation and the MR framework. Section 5 determines the weightage-based improved RFE and Section 6 describes optimized HC. Sections 7 and 8 explain the outcomes.

2 | Literature Review

2.1 | Related Works

In 2020, Velliangiri and Hari Mohan Pandey [3] suggested an efficient classifier called Fuzzy and Taylor Elephant Herd Optimization (FT-EHO) for identifying DDoS attacks, which was influenced by DBNs. The performance of FT-EHO was contrasted with extant techniques over varied assessment measures. Results demonstrated that the suggested FT-EHO greatly outperformed existing approaches on accuracy (93.8%), rate of detection (97.2%), preciseness (94.9%), and recall (93.8%).

In 2021, Kushwah and Ranga [22] described a DDoS system based on an enhanced Self-Adaptive Evolutionary ELM (SaE-ELM). Two extra elements were added to the SaE-ELM model to enhance it. It first adopted the most appropriate crossover operator. Second, it automatically decided how many neurons of the hidden layer were necessary. These characteristics increased the model's capacity for learning and categorization. The results of the studies demonstrated that the recommended attack detection system executed more effectively than the competing systems.

In 2020, Bhardwaj et al. [8] suggested a new model that combined SAE to learn features with a DNN for separating internet traffic from legitimate traffic and DDoS traffic. This work deployed AE and DNN to effectively identify DDoS threats. The suggestions made in this article resulted in a smaller network that avoided overfitting, negligible error, and security in opposition to exploding and disappearing gradients.

In 2021, Agarwal et al. [16] introduced a unique FS-WOA DNN technique in 2021. Here, min–max normalization replaced every input in a fixed range. Then, the proposed FS-WOA was fed with that standardized data to choose the best features. A DNN classifier was deployed that distinguished the attacked and normal data.

A novel technique for identifying DDoS assaults in a CC context was presented by Kushwah and Ranga in 2020 [30]. An artificial neural network (ANN) called the V-ELM was used to create the suggested system. Additionally, experiments were run to evaluate how the suggested system operated with various parameter values. The efficacy of the proposed system was compared against other approaches using two benchmark datasets.

In 2020, Priyanka Verma et al. [6] proposed the Attacked VM Detection and Recovery (AVDR) paradigm, which enhances the effectiveness of current migration strategies while minimizing collateral harm. A linear model to assess attack power was also presented as the AVDR architecture that focused on attack strength. The outcomes demonstrated the superiority of the suggested work over the competing models.

In 2020, Hezavehi and Rahmani [31] suggested a TPA-based DDoS AD system in a cloud context. Second, they offered a variety of basic assumptions and cloud setups to create simulation tests to evaluate the recommended framework. Then, they provided the findings from simulation studies to evaluate the approach's viability.

In 2021, Arul and Punidha [32] suggested a Supervised SD-LVQ model by which was used to identify MemCached threats by malevolent software on various Cloud PCs. Several application service calls connected to various damaging attacks on cloud servers that were memcached for DDoS threats were categorized

by LVQ. The results of the test showed that 97.2% were truly positive and only 0.03% were falsely negative.

In 2024, Kalvikkarasi and Saraswathi [33] suggested that DDoS attack detection was presented: CBCO-ERNN, an optimized Elman recurrent neural network (ERNN) based on chaotic bacterial colony optimization (CBCO). To determine the ideal ERNN architecture structure (number of hidden neurons) and parameters (weights and biases), the suggested approach makes use of CBCO. By initializing the bacterial population and choosing the proper chemotaxis step size value, chaos theory is used to enhance BCO's exploration and exploitation capabilities.

In 2023, Balasubramaniam et al. [34] developed a unique algorithm: the suggested gradient hybrid leader optimization (GHLBO) algorithm makes it simple and efficient to detect DDoS attacks. This optimized approach is in charge of training a deep stacked autoencoder (DSA) that effectively identifies the assault. In this case, the deep maxout network (DMN) with an overlap coefficient fuses features, and the oversampling procedure augments the data.

In 2024, Sumathi and Rajesh [35] proposed an ANN-based hybrid GBS (Gray Wolf Optimizer [GWO] + Back Propagation Network [BPN] + Self Organizing Map [SOM]) intrusion detection system (IDS) for the detection of intrusion in the CC environment. The base classifier, BPN, was chosen for this research after evaluating the performance of a comprehensive set of neural network algorithms on the standard benchmark UNSW-NS 15 dataset. BPN intrusion detection performance was further improved by combining it with SOM and GWO. Hybrid FS was made using a correlation-based approach and stratified 10-fold cross-validation (STCV) ranking based on weight matrix value (W). These selected features were further fine-tuned using metaheuristic GWO hyperparameter tuning based on a fitness function. The proposed IDS technique was validated using the standard benchmark UNSW-NS 15 dataset. However, the integration of multiple methods increases the computational complexity.

In 2022, Sumathi et al. [36] employed a LSTM recurrent neural network and autoencoder and decoder based deep learning strategy with a gradient descent learning rule. The network parameters like weight vectors and bias coefficients were tuned optimally by employing a hybrid Harris Hawks optimization (HHO) and particle swarm optimization (PSO) algorithm. The introduced hybrid optimization algorithm selected the essential attributes, and the results obtained confirmed that the proposed LSTM and deep learning model show better performance in detection.

2.2 | Research Gaps

Large amounts of network traffic are used in DDoS attacks to target many computers. Studies have demonstrated that packet-based attack-detecting processes give promising outcomes over traditional signature-based attack identification techniques, which have not been able to identify such attacks well. Many existing studies have explored DDoS attack detection using a variety of techniques, including traditional ML models, statistical methods, and deep learning approaches. However, despite the breadth of research in this area, several key challenges remain unaddressed, particularly in the context of cloud environments and big data.

For DDoS assaults, there is a paucity of training data. Companies frequently refuse to openly admit they have been hacked and do not disclose information on network attacks, as it might harm their company's reputation. The WSU-ROA algorithm introduced in this work represents a novel optimization technique that dynamically adjusts the weights of the LSTM and DMO models based on their performance during detection. This allows the model to adapt to changing attack patterns and traffic dynamics, ensuring that the detection system remains accurate and efficient over time. Most existing methods either use static weights or focus on optimizing single-model performance, rather than combining multiple models in an optimized, adaptive way. The features and limitations of the existing methods are tabulated in Table 1.

3 | Overview of Developed DL Model for DDoS Attack Detection in the Cloud

CC is revolutionizing IT technology by offering end users virtualized, scalable resources on-demand with greater versatility, lesser maintenance, and lower infrastructure expenses. These resources are made available through the Internet using well-known networking formats, standards and protocols and they are controlled by various management groups. The basic technology and outdated protocols include vulnerabilities and bugs that allow attackers to gain access. One of the most prevalent attacks that cause significant harm and impair cloud performance is DDoS, which must be resisted. These phases include data generation, feature extraction, FS, and attack detection using a hybrid classifier. The final outputs of the hybrid classifier for attack detection determine whether an attack is present or absent. This approach leverages the strengths of both the DMO and LSTM models, ensuring robust and accurate detection of DDoS attacks by integrating the outcomes of both models. The steps of the proposed DDoS AD model in the cloud are as follows.

- Data generation is the initial phase; this work considers the DDoS dataset from the big data perspective.
- Map reduce framework: As the work considers the big data perspective, we are using the Map reduce framework.
- Mapper handles the big data and processes the feature extraction, which includes raw features, packet feature extractor, improved correlation, and statistical features. Reducer will provide the combined feature set from the mappers.
- From the extracted feature set, appropriate features are selected via weightage-based improved RFE.
- The selected feature is subjected to the attack detection phase, where the HCs including LSTM and DMO are proposed.
- For precise and accurate detection, the weights of LSTM and DMO are optimally chosen using the WSU-ROA algorithm.

The adopted DL model for DDoS AD in the cloud is portrayed in Figure 1.

TABLE 1 | Review on existing works.

Author	Methodology	Feature	Limitations
Velliangiri and Hari Mohan Pandey [3]	FT-EHO	• Accuracy, precision and recall were maximized	• Computational cost is high
Gopal Singh Kushwah et al. [22]	SaE-ELM	• Detection accuracy was high	• Additional enhancements are needed to enhance the performance
Bhardwaj et al. [8]	AE and DNN	• Precision, Recall and F1-score were higher	• Need to identify attacks in real-time
Agarwal et al. [16]	FS-WOA – DNN	• Maximal accuracy was obtained	• It is extremely expensive due to intricate data models
Gopal Singh Kushwah et al. [30]	V-ELM	• Detection accuracy was greater	• It is not suitable for large datasets
Priyanka Verma et al. [6]	AVDR	• Reliable	• Need optimal strategy in the recovery phase for better results
Sasha Mahdavi Hezavehi and Rouhollah Rahmani [31]	TPANGND	• Maximum valid • Response time and precision	• High cost
Arul and Punidha [32]	Supervised SD-LVQ	• Higher TP ratio	• Still, difficult to detect all malicious attacks

4 | Data Generation and Map Reduce Framework-Based Feature Extraction

4.1 | Data Generation

Data Generation is the initial phase, here, the input data is taken from the dataset (considered as the big data) and is represented by *ID*. The data is gathered from cloud network logs, which include packet-level information such as source IP, destination IP, packet size, protocol type, and time stamps.

4.2 | Feature Extraction Using MR Framework

The big data is handled using the MR framework. MR [37] is a programming approach used in a distributed system for computing [38] to handle enormous amounts of data. It is employed for managing data that cannot be accommodated in a physical memory. These two operations are carried out in two phases, each of which is followed by a data transfer between cluster nodes. Data in the type of "key, value" pairs is processed in parallel throughout these phases. From the dataset, the map function gets the input and produces intermediary output. The map function's output is organized to be used as input for the reducer function. This involves data exchanges among map and reduce operations. The values are gathered at each node while the reduction function is executed for a certain key. The reduce function also generates the final result in the form "key, value" [38]. MR functions are employed in this study to discover the features of big data [37]. Accordingly, the mapper phase includes the extraction of features like raw features, Packet feature extractor, Improved Correlation and statistical features.

Raw features: These features represent the original input data and are symbolized by F^{rf}.

Packet feature extractor: The packet features are derived from the raw data, which includes flow duration, packet length variation, backward bytes and average packet size. The packet features are symbolized by F^{pf}.

Statistical features: The derived features contain median, mean and SD features. These features are symbolized by F^{sf}.

Improved correlation: Correlation [39] is shown in Equation (1) and it is the specified measure that quantifies the linear relationship between two variables. In Equation (1), q_i and k_i symbolizes values of q and k variables from input *ID*.

$$F^{Cr} = \frac{\sum \left(q_i - \overline{q}\right)\left(k_i - \overline{k}\right)}{\sqrt{\sum \left(q_i - \overline{q}\right)^2 \sum \left(k_i - \overline{k}\right)^2}} \tag{1}$$

Nevertheless, for enhanced assessment of association among every variable, a weight-based correlation is established as exposed in Equation (2), in which, $\overline{q}$ and $\overline{k}$ corresponds to inter-quartile mean and mid-hinge mean values of q and k in that order. The values for $\overline{q}$ and $\overline{k}$ are modeled as in Equation (3) and (4), which, u_1 and u_3 correspond to first and third quartiles. The weight *We* is evaluated as shown in Equation (5), which, $x(i, j)$ corresponds to the distance $D(q, k)$ between q and k, which is estimated using hybrid distances such as Manhattan and Chebyshev distances.

$$F^{ICr} = \frac{\sum \left(q_i - \overline{q}\right)\left(k_i - \overline{k}\right) \times We}{\sqrt{\sum \left(q_i - \overline{q}\right)^2 \sum \left(k_i - \overline{k}\right)^2}} \tag{2}$$

$$\overline{q} = \frac{2}{m} \sum_{i=\frac{m}{4}+1}^{\frac{3m}{4}} q_i \tag{3}$$

$$\overline{k} = \frac{u_1(q) + u_3(q)}{2} \tag{4}$$

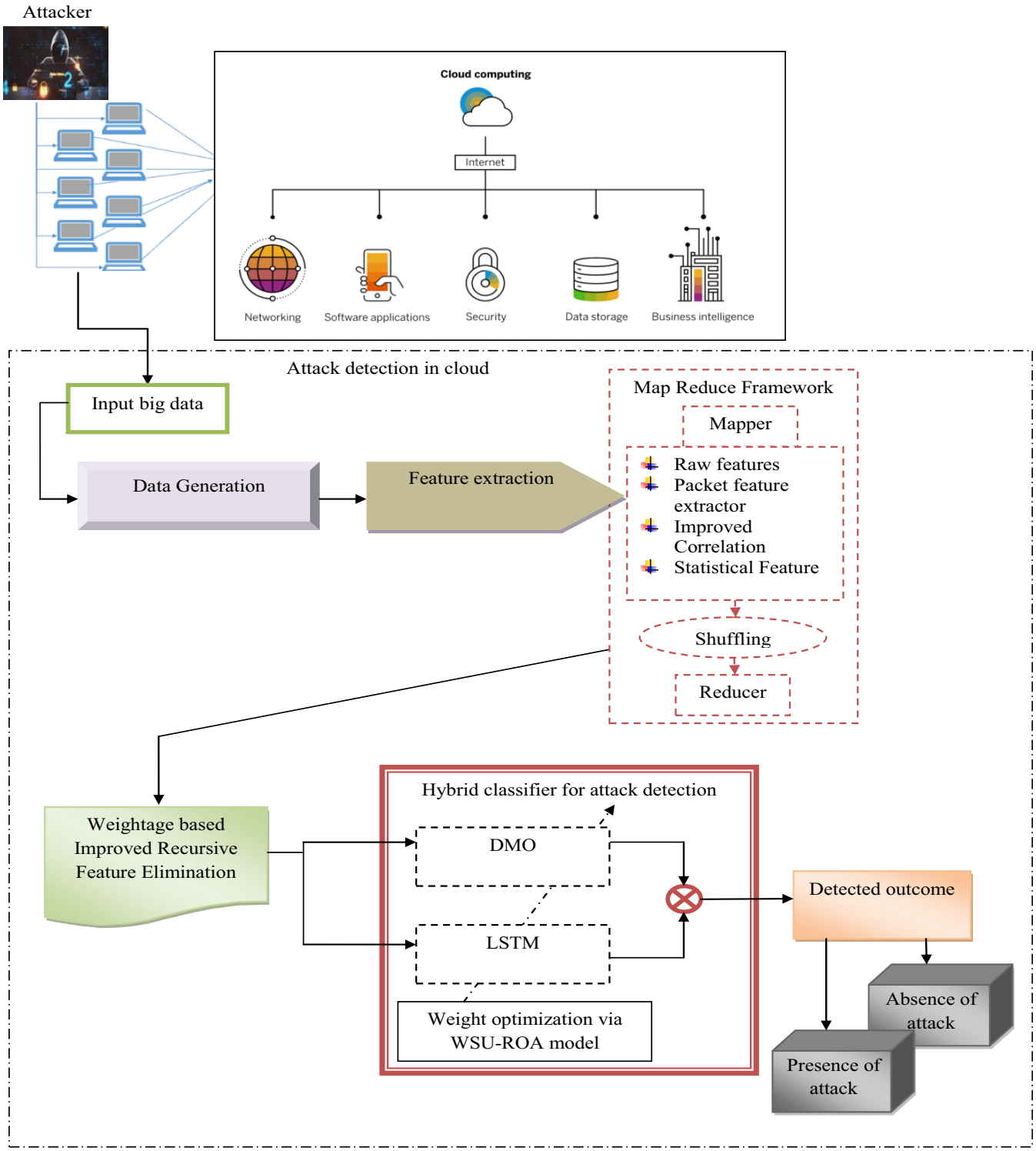

FIGURE 1 | Diagrammatic demonstration of DL model for DDoS AD in cloud.

$$We = 2 * \left(1 - \frac{1}{1 + \exp\left(\frac{|x(i,j)|}{2}\right)}\right) \tag{5}$$

Conventionally, the distance $D(q,k)$ is estimated as shown in Equation (6). However, for getting a valid output, improved distance $ID(q,k)$ is estimated as shown in Equation (7), where $\beta = 0.6$.

$$D(q,k) = \left[\frac{\sum_{i=1}^{v}|q_i - k_i| + \max|q_i - k_i|}{2}\right] \tag{6}$$

$$ID(q,k) = \frac{\left[\sqrt{\sum_{i=1}^{v}\left(|q_i - k_i| + \max|q_i - k_i|\right)^2}\right]/2}{\left[\min\left(\sqrt{\sum_{i=1}^{v}\left(|q_i - k_i|^2/2\right)}, \sqrt{\sum_{i=1}^{v}\max\left(|q_i - k_i|^2/2\right)}\right) + \beta\right]} \tag{7}$$

After deriving the features in the mapper, the reducer phase combines the features from all the mappers and provides the combined feature set F that is defined as $F = \left[F^{rf} + F^{pf} + F^{sf} + F^{ICr}\right]$.

5 | Weightage-Based Improved Recursive Feature Elimination (RFE)

The weightage-based improved RFE method is used to select the most relevant features from the initial feature set, ensuring that the DDoS detection model uses only the most informative features for classification. This FS process enhances the model's performance by reducing the dimensionality of the data, thereby improving computational efficiency and avoiding overfitting. This technique helps optimize the performance of the DDoS detection model by ensuring that only the most relevant information is used for classification. From the feature set F, appropriate features will be selected via weightage-based improved RFE. The most relevant attributes or features are those of the input components that have the highest absolute weights [40]. Therefore, the inputs with the lowest weights can be deleted with the least impact on the classification result if the classifier has been properly trained. In this case, feature ranking is used to implement FS. The RFE approach utilizing the SVM classifier is often applied in the subsequent iterative phases [41]. The improvement in this approach comes from incorporating feature weights based on correlation-based analysis. This improved RFE method helps ensure that only the most relevant features contribute to the model, thus enhancing classification accuracy and reducing overfitting.

1. Training the SVM classifier.

2. Determine the criteria for ranking all features.

3. Eliminate the attributes with the lowest ranking values.

As per the proposed method, the weight is assigned to each feature using the improved MI method. The proposed improved MI-based RFE is as follows: The traditional MI is formulated as in Equation (8), wherein, F corresponds to the input feature and M corresponds to label and Pcorresponds to probability.

$$MI = \sum_{F,\mathrm{M}} P(F,\mathrm{M}) \log \frac{P(F,\mathrm{M})}{P(F)P(\mathrm{M})} \tag{8}$$

However, conventional MI does not consider the pixel positions and thus, an improved MI-based RFE is proposed as shown in Equation (9).

$$IMI = \frac{MI(F,\mathrm{M})}{\frac{1}{2}[H(F) + H(\mathrm{M})]} \tag{9}$$

Here, $H(F)$ and $H(\mathrm{M})$ are computed based on improved Shannon entropy values as shown in Equations (10) and (11).

$$H(F) = -\sum_{i=1}^{n} PF_i \log_2 \left[PF_i . e^{2(PF_i - 1)}\right] \tag{10}$$

$$H(\mathrm{M}) = -\sum_{i=1}^{n} P\mathrm{M}_i \log_2 \left[P\mathrm{M}_i . e^{2(P\mathrm{M}_i - 1)}\right] \tag{11}$$

Thus after assigning the weight to each feature using improved MI, the SVM classifier is trained and ranked and features with the smallest ranks are removed. The features elected with improved MI are signified as Υ.

6 | Optimized Hybrid Classifiers (DMO and LSTM) for DDoS AD in the Cloud

The WSU-ROA is a metaheuristic optimization technique designed to find the optimal weights for combining multiple models of LSTM and DMO in a hybrid model for DDoS attack detection. The chosen features Υ are provided to attack the detecting phase, where, optimized HCs (LSTM and DMO) will be used. For precise and accurate classification, the LSTM weights and DMO weights are chosen via the WSU-ROA algorithm optimally. The idea is to improve the model's performance by efficiently selecting and fine-tuning the weights that control the contribution of each model (LSTM and DMO) to the final prediction. Figure 2 shows the hybrid model for the classification of detection. In this phase, the feature selected using the weightage-based improved RFE method is subjected as input to both the Deepmaxout and LSTM classifiers. These classifiers are potentially involved in the decision-making process. The weight parameters w present in the convolutional layer of the Deepmaxout classifier and the weight parameter a present in the LSTM layer of the LSTM classifier are optimally tuned via the proposed WSU-ROA algorithm. By optimizing these weight parameters, the classifiers contribute to enhancing accuracy and offer a more reliable detection outcome. The outputs from optimized LSTM and DMO are averaged to produce the final binary classification outcomes as the existence or absence of an attack. This decision-making process effectively leverages the DL method with the bioinspired optimization algorithm, where the optimization process iteratively refines the model weights, leading to robust and accurate classification performance.

6.1 | LSTM Classifier

LSTM networks are well-suited for sequence prediction tasks due to their ability to capture long-term dependencies in time-series data. In this context, the LSTM model is used to analyze temporal patterns in network traffic. The LSTM [42] gets selected to feature Υ as input. The three gating components that made up the LSTM network were the forget gate, input gate, and output gate. How well a cell can remember information from the past is controlled by the forget gate. The LSTM classifier is illustrated in Figure 3.

The output gate corresponds to the output of the neuron. The LSTM is given by Equations (12–16).

$$l_\varsigma = \psi\left(a_l \times \left[\delta_{\varsigma-1}, \Upsilon_\varsigma\right] + \rho_l\right) \tag{12}$$

$$g_\xi = \psi\left(a_g \times \left[\delta_{\xi-1}, \Upsilon_\xi\right] + \rho_g\right) \tag{13}$$

$$h_\xi = \psi\left(a_h \times \left[o_\xi, \delta_{\xi-1}, \Upsilon_\xi\right] + \rho_h\right) \tag{14}$$

$$o_\xi = g_\xi \times o_{\xi-1} + l_\xi \times \tan\delta\left(a_C \times \left[\delta_{\xi-1}, \Upsilon_\xi\right]\right) \tag{15}$$

$$\delta_\xi = h_\xi \times \tan\delta\left(o_\xi\right) \tag{16}$$

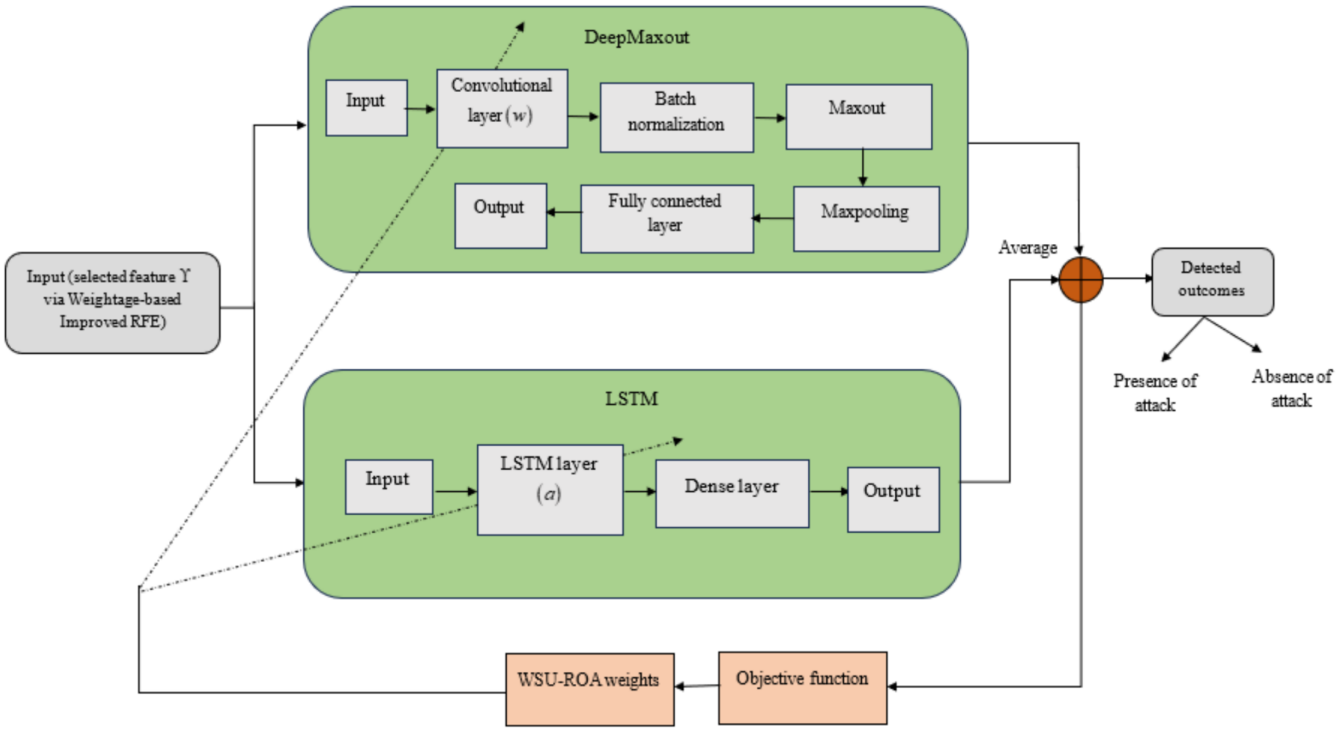

FIGURE 2 | Framework of hybrid classification model.

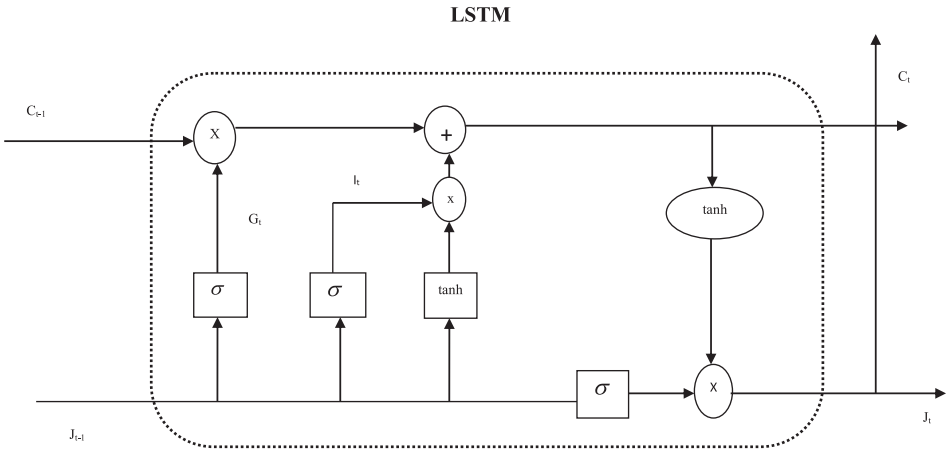

FIGURE 3 | Conventional LSTM classifier.

where ξ = time, Υ_ξ = input LSTM, $\delta_{\xi-1}$ = hidden layer output, l_ξ, g_ξ, h_ξ = input gate, a_l, a_g, a_h = weight is optimally chosen via WSU-ROA, ρ_l, ρ_g, ρ_h = offset vector, a_C = the cell unit's weight about input, δ_ξ = hidden layer output, and ψ = sigmoid function.

6.2 | DMO

DMO is a method used to optimize decision-making processes by evaluating multiple factors. In the context of DDoS detection, DMO combines outputs from multiple models or features and optimizes the decision regarding whether the traffic is normal or malicious. The DMO [43] gets the selected feature ϒ as input. A recently developed NN called DMO is deployed in a wider variety of appliances. Every neuron in DMO includes μ pieces of candidates. For activation of neurons, it was selected to utilize a max value extending μpiece [43]. The DMO classifier is depicted in Figure 4.

Set yth the node of the hidden layer as J_l^i, and its components as O_y^{ij}. Equations (17) and (18) demonstrate how they are linked.

$$J_y^i(\Upsilon) = \max_{j\in 1,2,\ldots,\mu} O_y^{ij} \tag{17}$$

By forward propagation via the layer below, O_y^{ij} is attained as in Equation (18).

$$O_y = w^{*G}_{y-1} J_{y-1} + f_y \tag{18}$$

Here $O_1 \in L^O$ = vector of $\mathbb{Z}th$ layer, $J_{y-1} \in L^{\mathrm{K}}$ = max-out activation vector of $y-1$ layer, $w^*_{y-1} \in L^{\mathrm{K}\times O}$ = weight matrix of $y-1$ layer optimally chosen via WSU-ROA, $f_y \in L^O$ = bias vector

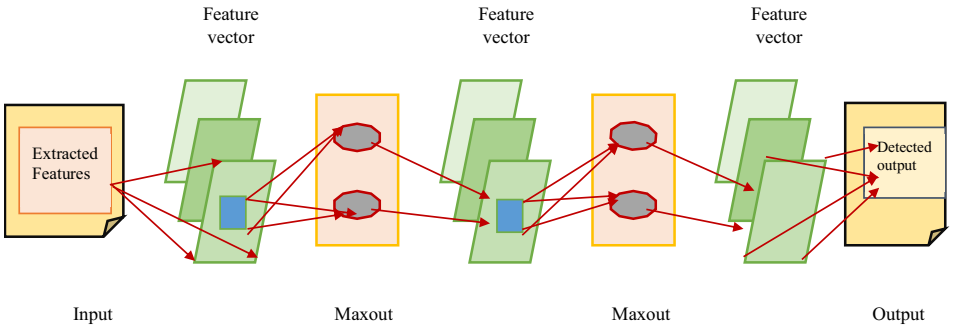

FIGURE 4 | Architecture of DMO classifier.

TABLE 2 | Hyperparameters of optimization algorithms.

Optimization algorithms	Hyperparameters of optimization algorithms
ROA	Population size $m = 5$
	Exploration probability $p1 = 0.2$
	Exploitation probability $p2 = 0.8$
	Remora-following probability $p3 = 0.4$
	Feeding behavior probability $p4 = 0.5$
	Maximum number of iterations $k = 20$
	Mean of Gaussian distribution $\mu = 0$
	Standard deviation of Gaussian distribution $\sigma = 1$
WSA	Acceleration coefficient $\beta = 1.5$
SMA	Random vector $Z = 0.03$
BWO	Procreation probability $pp = 0.6$
	Crossover rate $cr = 0.44$
	Mutation probability $pm = 0.4$
WSU-ROA	Population size $m = 5$
	Exploration probability $p1 = 0.2$
	Exploitation probability $p2 = 0.8$
	Remora-following probability $p3 = 0.4$
	Feeding behavior probability $p4 = 0.5$
	Mean of Gaussian distribution $\mu = 0$
	Standard deviation of Gaussian distribution $\sigma = 1$

of yth layer. The optimization hyperparameters are tabulated in Table 2.

6.3 | WSU-ROA Algorithm: The Mathematical Model

The White Shark Updated Remora Optimization Algorithm is a key component in optimizing the hybrid classifier (combining LSTM and DMO) for detecting DDoS attacks in cloud environments. By optimizing hybrid classifiers, ensuring scalability for big data applications, and providing real-time, dynamic adaptation, WSU-ROA is well-suited for the complex, evolving nature of cloud-based DDoS detection.

Solution encoding: The WSU-ROA algorithm is used to optimally adjust the weights of both LSTM and DMO models. The algorithm enhances the model's performance by ensuring that the contributions of LSTM and DMO are balanced to achieve the highest possible classification accuracy. The weights of LSTM (a) and DMO (w) are chosen via the WSU-ROA algorithm optimally. The objective set for optimal selection of (a) and (w) is given in Equation (19), in which, Ac corresponds to accuracy. Specifically, the minimization of error is the objective function of the proposed WSU-ROA algorithm.

$$OB = \frac{1}{Ac} \tag{19}$$

The behavior of remora served as the inspiration for the ROA [44]. It interacts with different fish to look for food and uses algorithms like WOA and SFO to repel opponents' attacks. The remoras look for food in different locations if they sense an invasion. Like other optimization approaches, it has two steps. The traveling of remora to find food occurs in the exploration stage, while the deliberate eating technique of remora occurs in the exploitation stage. However, this optimization's robustness is ineffective. As a result, WSA [45] and ROA are combined to create WSU-ROA, which resolves the problems in ROA.

Step 1: *Initializing*.

Initialize the remora population in a k dimension region. The problem variable's position I in the searching area is provided by Equation (20).

$$I_j = \left\{ I_{j1}, I_{j2}, \ldots, I_{jk} \right\} \tag{20}$$

Here, j indicates the remora count and k establishes the searching space. The remora may alter its position vector in 1D, 2D, or multi-dimensional space depending on the direction of its swimming. Similar to that, Equation (21) is used to represent the best solution I_{best} of this method.

$$I_{best} = \left\{ I_1^*, I_2^*, .. I_k^* \right\} \tag{21}$$

Each candidate solution in the WSU-ROA has a specified function and is represented by Equation (22).

$$\mathfrak{I}\left(I_j\right) = \mathfrak{I}\left(I_{j1}, I_{j2}, \ldots, I_{jk}\right) \tag{22}$$

As per the best remora location, the optimal objective is provided in Equation (23).

$$\mathfrak{I}\left(I_{best}\right) = \mathfrak{I}\left(I_1^*, I_2^*, \ldots I_k^*\right) \tag{23}$$

Step 2: Calculating objective.

The objective to compute the best fitness is computed as in Equation (19).

Step 3: Exploration phase.

This phase includes two strategies: SFO strategy and experience attack.

i. SFO strategy
When a remora is assigned to sailfish, its location is taken into account as the most recent one. Equation (24), which depends on the elite idea, is used to express the location upgrading.

$$I_j^{t+1} = I_{best}^t - \left(rand(0,1) * \left(\frac{I_{best}^t + I_{rand}^t}{2} \right) - I_{rand}^t \right) \tag{24}$$

In Equation (24), t and T implies current and maximum iterations, I_{rand} implies irregular remora location.

ii. Experience attack
This phase is mathematically formulated as in Equation (25).

$$I_s = I_j^t + \left(I_j^t - I_{pre} \right) * randm \tag{25}$$

Here, I_s and I_{pre} implies tentative step and preceding iteration location, *randm* is elected to execute the smaller global movement. If the current value $\Im\left(I_j^t\right) >$ attempted solution $\Im\left(I_s\right)$, the remora elects a different feeding manner for optimization, otherwise, if $\Im\left(I_j^t\right) < \Im\left(I_s\right)$, then it is returned back to the host criterion.

Step 4: Exploitation phase.

This phase includes two strategies: the WOA tactic and the host feeding method.

i. WOA strategy
As per WOA, the remora position is updated as in Equation (26).

$$I_{j+1} = E * e^{\beta} * Cos(2\pi\beta) + I_j \tag{26}$$

$$\beta = rand(0,1) * (A-1) + 1 \tag{27}$$

$$A = -\left(1 + \frac{t}{T}\right) \tag{28}$$

$$E = \left| I_{best} - I_j \right| \tag{29}$$

Here, E signifies that the distance between prey and hunter β is a value between them $[-1, 1]$.

As per WSU-ROA, the remora position is modeled as revealed in Equation (35) by merging the WSA update. The WSA update is shown in Equation (32).

$$I'^{i}_{k+1} = I_{gbest_k} + r_1 \overline{\mathbb{Q}}_W \times \mathrm{sgn}\left(r_2 - 0.5\right) \tag{30}$$

$$\overline{\mathbb{Q}}_W = \left| ran \times \left(I_{gbest_k} - I'_k \right) \right| \tag{31}$$

$$I'^{i}_{k+1} = I_{gbest_k} + r_1 \left| ran \times \left(I_{gbest_k} - I'_k \right) \right| \times \mathrm{sgn}\left(r_2 - 0.5\right) \tag{32}$$

On substituting Equation (29) in (26), we get Equation (33).

$$I_{j+1} = \left| I_{best} - I_j \right| * e^{\beta} * Cos(2\pi\beta) + I_j \tag{33}$$

Adding Equations (32) and (33), we get Equation (34).

$$I'^{i}_{k+1} + I'^{i}_{k+1} = I_{gbest_k} + r_1 \left| ran \times \left(I_{gbest_k} - I'_k \right) \right| \times \mathrm{sgn}\left(r_2 - 0.5\right) + \left| I_{best} - I_j \right| * e^{\beta} * Cos(2\pi\beta) + I_j \tag{34}$$

$$I_{j+1} = \frac{\left| I_{best} - I_j \right| * e^{\beta} * Cos(2\pi\beta) + I_{gbest_k} + I_j + r_1 \left| ran \times \left(I_{gbest_k} - I'_k \right) \right| \times \mathrm{sgn}\left(r_2 - 0.5\right)}{2} \tag{35}$$

In Equation (35), *ran* the value is replaced by a hybrid map as shown in Equation (36).

$$z_{n+1} = \sin e\left(Tent\left(z_n\right) \bmod 1\right) \tag{36}$$

(ii) Host feeding

This host feeding behavior is arithmetically expressed as in Equations (37–40).

$$I_j^t = I_j^t + \theta \tag{37}$$

$$\theta = \lambda * \left(I_j^t - C * I_{best} \right) \tag{38}$$

$$\lambda = 2 * B * rand(0,1) - B \tag{39}$$

$$B = 2 * \left(1 - \frac{t}{T}\right) \tag{40}$$

Step 5: Termination.

Repeat the procedure of WSU-ROA until remora discovers the best solution. The pseudocode of WSU-ROA is in Algorithm 1.

Thus, the absence or existence of attack is detected by averaging the outcomes of DMO (v) and LSTM frameworks $\left(k_t\right)$ as given in Equation (41).

$$Final\ outcome = \frac{k_t + v}{2} \tag{41}$$

7 | Results and Discussion

7.1 | Simulation Set-Up

The proposed DL model for DDoS AD in the cloud was done in Python. The efficiency of the proposed HC + WSU-ROA was proven over HC + ROA, HC + WSA, HC + SMA, HC + DO and HC + BWO. The dataset for carrying out the analysis was gathered from "DDoS Evaluation Dataset [46] and UNSW-NB15 Dataset [47]."

Dataset description: "DDoS Evaluation Dataset: CICDDoS2019 includes benign and the most recent common DDoS attacks,

ALGORITHM 1 | Proposed WSU-ROA.

Problem size, population, lower bound and upper bound
Output: Optimal weights (a) and (w)
Begin population
Initializing I_{best}
While $(t < T)$
Validate any searching agent go over the searching area and rectify it.
Evaluate objective as in Equation (19)
For remora j
If the selection factor $aa(j) = 0$ then
Upgrade the position of ROA by merging WSA using the proposed Equation (35)
Else if $aa(j) = 1$ then
Upgrade position of attached sail fishes using Equation (24).
End if
Predict with Equation (25)
The host feeding phase is done
End for
End while
Return optimal weights (a') and (w')

which closely resemble actual real-world data (PCAPs)." They include a variety of current reflected DDoS attacks in this dataset, including Port Map, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, and SNMP attacks. On the training day, they conducted 12 DDoS attacks using the following attacks: NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, Web DDoS, SYN, and TFTP. On the testing day, they conducted seven assaults using the following attacks: Port Scan, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, and SYN. Dataset 1 contains 100 000 samples with 86 features before FS, reduced to 70 features after applying the improved RFE method. The class distribution includes 40 000 samples of class 0 (normal traffic), 30 000 of class 1, and 30 000 of class 2 (representing different types of DDoS attacks).

UNSW-NB15: The UNSW-NB 15 dataset's raw network packets were produced by the IXIA Perfect Storm tool in the Cyber Range Lab of UNSW Canberra to produce a blend of real, contemporary normal activities and synthetic, current attack behaviors. There are nine different types of attacks in this dataset: fuzzers, analysis, backdoors, DoS, exploits, generic, reconnaissance, shell code, and worms. Twelve algorithms are built and the Argus as well as Bro-IDS tools are utilized to create a total of 49 features with the class label. Dataset 2 comprises 71 730 samples, also reduced from 86 to 70 features after selection, with a slightly imbalanced class distribution: 40000 samples of class 0, 1730 of class 1, and 30 000 of class 2. Across both datasets, the extracted features consist of 78 raw features, four packet-based features, one correlation feature, and three statistical features, capturing diverse and comprehensive traffic characteristics essential for accurate DDoS detection.

7.2 | Performance Analysis

The evaluation of HC + WSU-ROA for DDoS AD in the cloud was done over HC + ROA, HC + WSA, HC + SMA, HC + DO and HC + BWO as given in Figures 5–10 for two datasets: "DDoS Evaluation Dataset [46] and UNSW-NB15 Dataset [47]." We got the outputs on the absence or existence of an attack in the cloud. The HC + WSU-ROA has shown the finest outputs for every metric. For all LPs, the accuracy of HC + WSU-ROA is better over HC + ROA, HC + WSA, HC + SMA, HC + DO and HC + BWO. The proposed HC + WSU-ROA gains a high accuracy when LP = 90 for both datasets. Similarly, the MCC seems to be better with a raise in LPs. Therefore, for every LP, the proposed HC + WSU-ROA showed the finest outputs over HC + ROA, HC + WSA, HC + SMA, HC + DO, and HC + BWO. A lesser false positive rate (FPR) of 0.05 is gained for HC + WSU-ROA at LP = 90, whereas HC + ROA, HC + WSA, HC + SMA, HC + DO and HC + BWO got quite high FPR values at LP = 90. The MCC of HC + WSU-ROA is high about 0.95% at LP = 90 over HC + ROA, HC + WSA, HC + SMA, HC + DO and HC + BWO. The improved performance demonstrates the effectiveness of the enhanced features, which are refined using the weightage-based improved RFE method. Moreover, the deployment of WSU-ROA for optimal weight selection of HCs aids in better AD in the cloud.

Tables 3 and 4 illustrate the examination of diverse individual classifiers (LSTM, DMO, CNN, RNN, SVM, RF, and DNN) over proposed HC (LSTM + DMO) + WSU-ROA for two datasets "DDoS Dataset and UNSW-NB15 Dataset". From the study, HC + WSU-ROA obtained a higher accuracy of 0.943 over LSTM, DMO, CNN, RNN, SVM, RF, COBCO-ENN, GHLBO-based DSA [34], and DNN for the UNSW-NB15 dataset. A small FPR of 0.051 is attained by HC + WSU-ROA, which is fewer than LSTM, DMO, CNN, RNN, SVM, RF, CBCO-ERNN [33], GHLBO-based DSA [34] and DNN for the DDoS Evaluation Dataset. As we have done AD in the cloud by deploying HC (LSTM and DMO) with enhancements done in optimization, the developed model attains improved outcomes.

7.3 | Ablation Study

Tables 5 and 6 display the ablation analysis for HC + WSU-ROA over HC with no features, proposed with existing correlation and HC with existing RFE for two datasets "DDoS Dataset and UNSW-NB15 Dataset". The specificity of DDoS AD in the cloud using HC + WSU-ROA is 0.941616, whereas, the specificity using HC with no features, proposed with existing correlation and HC with existing RFE is 0.754, 0.765 and 0.756 for DDoS Dataset. The improvisations done in extant correlation with weightage-based improved RFE assist the HC to get superior AD results. Also, improvisations in weight selection for HC using WSU-ROA aided in better AD in the cloud.

7.4 | Cost Analysis

Figure 11 shows the cost analysis using WSU-ROA-based DDoS AD in the cloud over ROA, WSA, SMA, DO and BWO. The cost analysis is done for two datasets: "DDoS Dataset and UNSW-NB15 Dataset." From iteration 0 to 20, the cost is much higher for both datasets. For the DDoS dataset, the cost using WSU-ROA is much less at around 1.053 which is better than ROA, WSA, SMA, DO and BWO. The greater convergence rate of the suggested DDoS AD in the cloud was provided by the ideal WSU-ROA-based weight selection of HC. This indicates that the

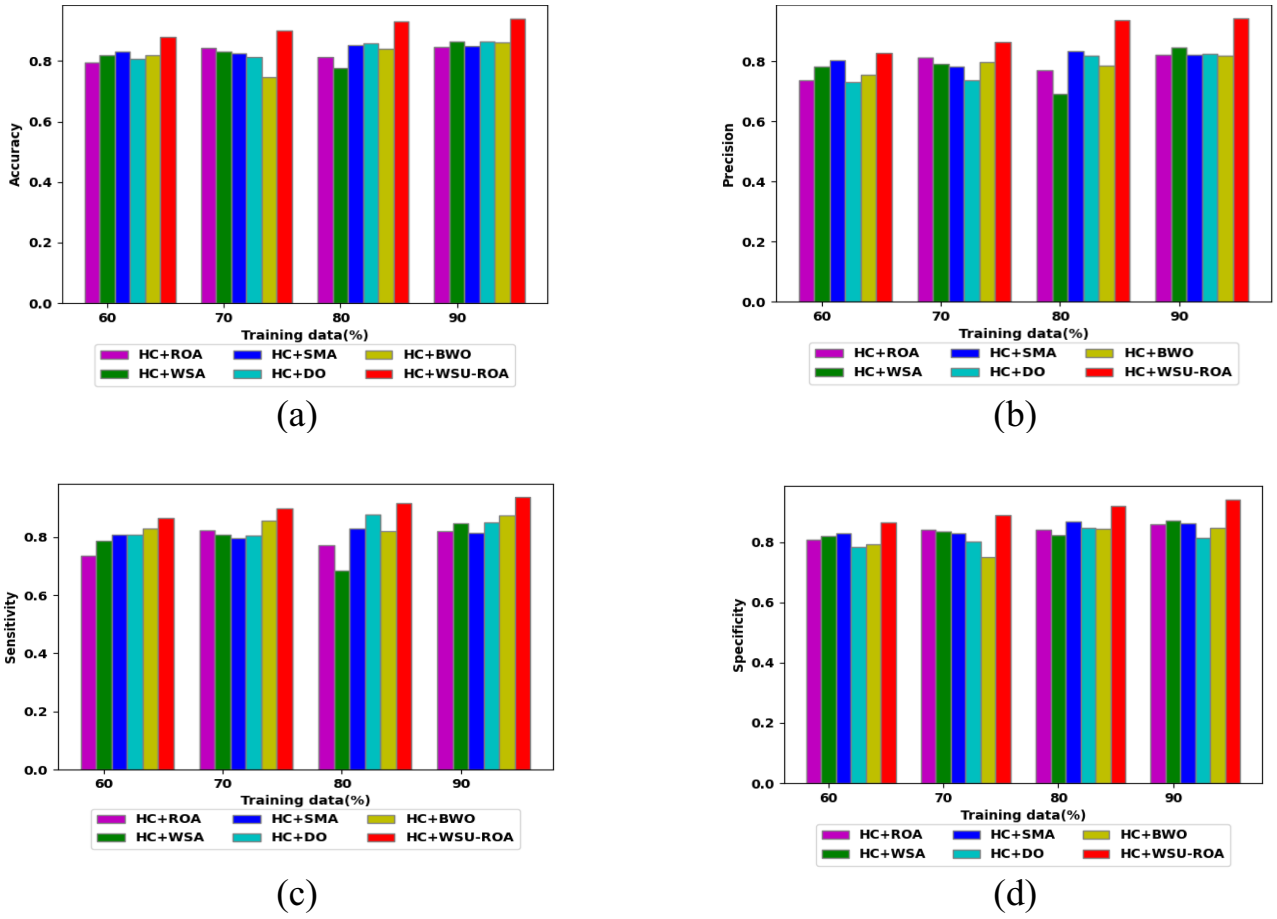

FIGURE 5 | Performance of HC + WSU-ROA method for DDoS AD in the cloud on (a) accuracy, (b) precision, (c) sensitivity, and (d) specificity using DDoS evaluation dataset.

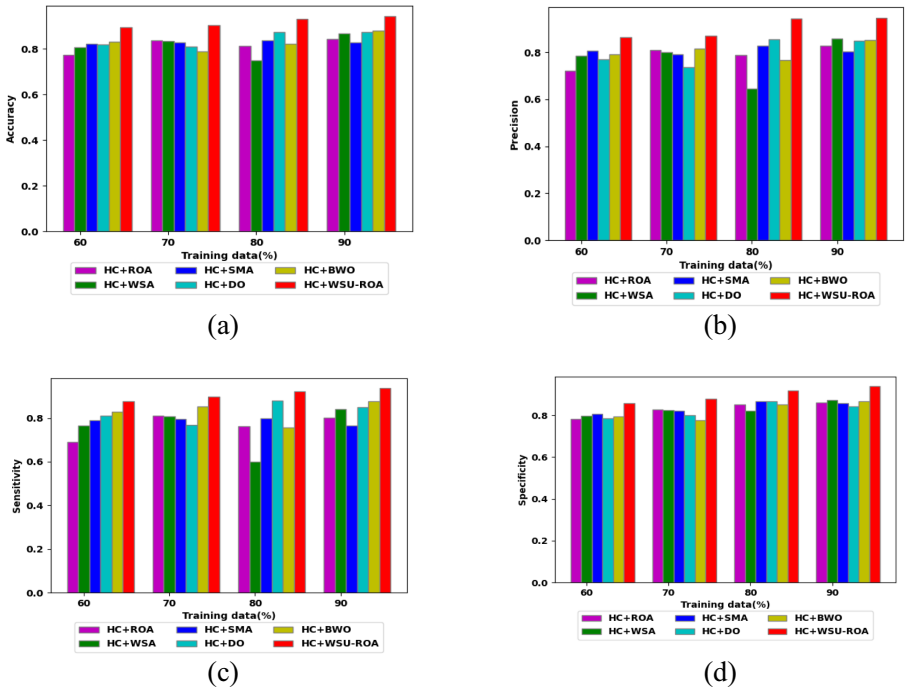

FIGURE 6 | Performance of HC + WSU-ROA method for DDoS AD in the cloud on (a) accuracy (b) precision, (c) sensitivity, and (d) specificity using UNSW-NB15 dataset.

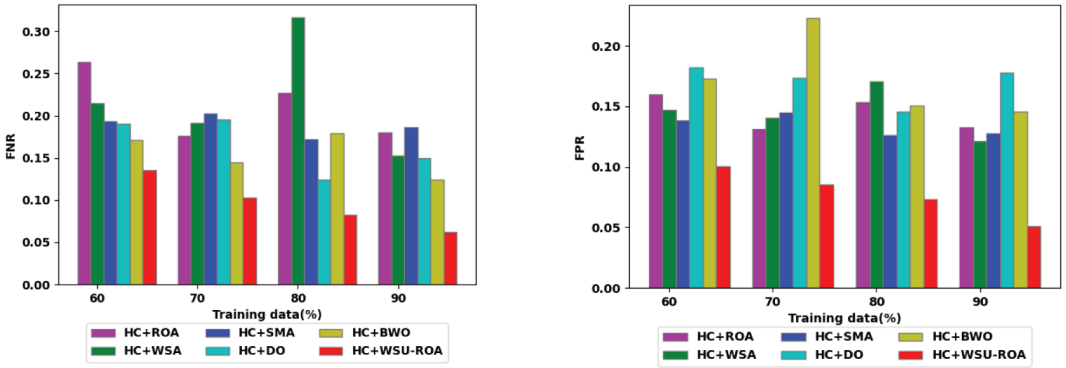

FIGURE 7 | Performance of HC + WSU-ROA method for DDoS AD in the cloud on (a) FNR and (b) FPR using DDoS evaluation dataset.

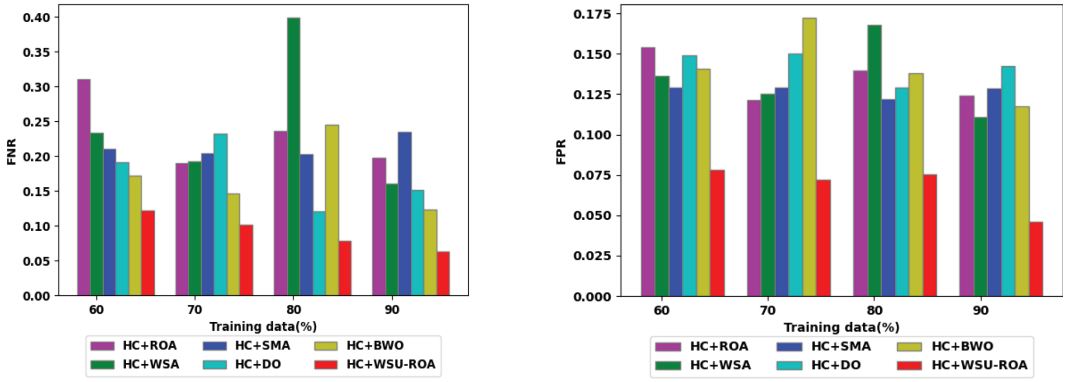

FIGURE 8 | Performance of HC + WSU-ROA method for DDoS AD in cloud on (a) FNR and (b) FPR using UNSW-NB15 Dataset.

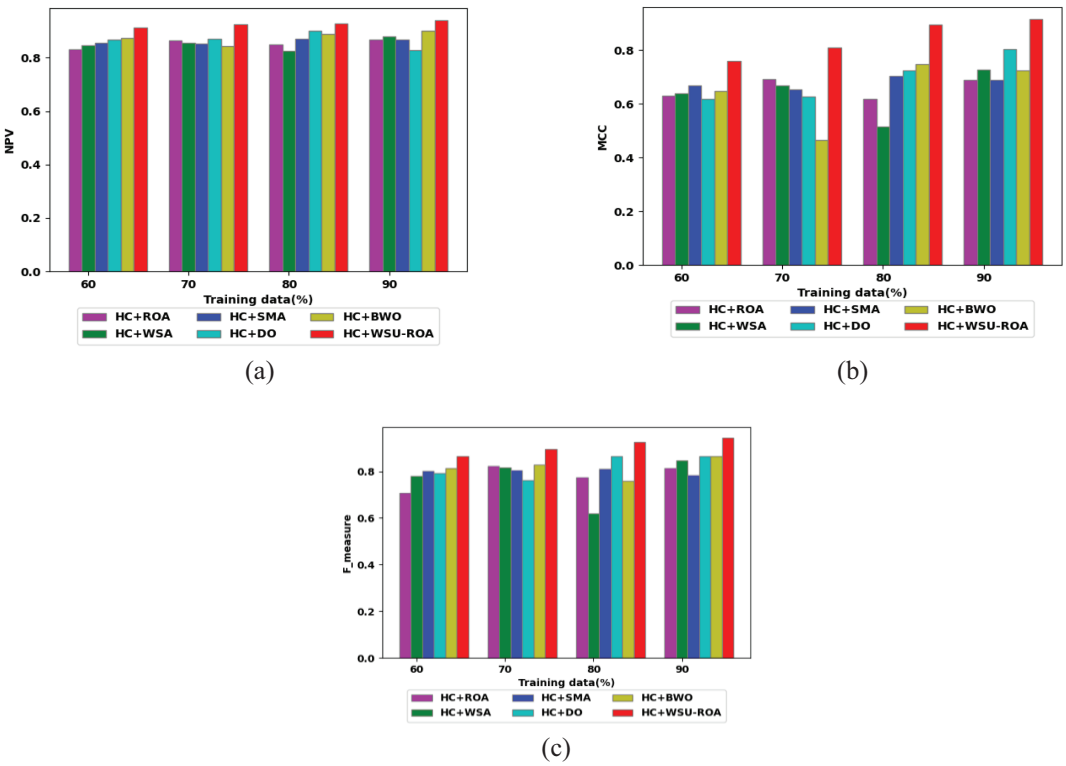

FIGURE 9 | Performance of HC + WSU-ROA method for DDoS AD in cloud on (a) NPV, (b) MCC, and (c) F measure using DDoS dataset.

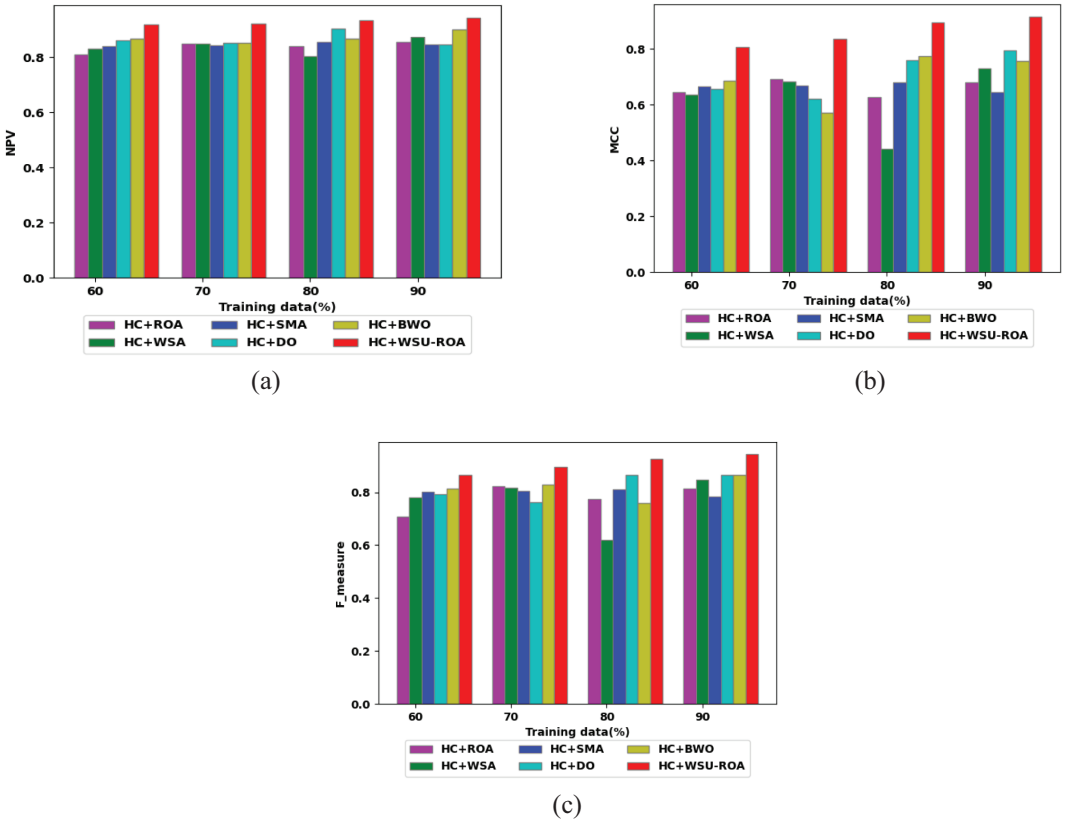

FIGURE 10 | Performance of HC + WSU-ROA method for DDoS AD in the cloud on (a) NPV, (b) MCC, and (c) F measure using UNSW-NB15 dataset.

TABLE 3 | Assessment of diverse classifiers using DDoS dataset.

Methods	Sensitivity	Specificity	Accuracy	Precision	F_measure	MCC	NPV	FPR	FNR
Proposed	0.937477	0.941616	0.939813	0.94345	0.944036	0.915004	0.939973	0.050884	0.062523
LSTM	0.83143	0.887529	0.871835	0.782396	0.806168	0.643895	0.849141	0.112471	0.16857
Deepmaxout	0.757371	0.843603	0.812528	0.759672	0.75852	0.812846	0.791671	0.156397	0.242629
CNN	0.838162	0.90119	0.893386	0.780883	0.808509	0.681085	0.828151	0.09881	0.161838
RNN	0.829019	0.834429	0.808485	0.805767	0.817228	0.555119	0.832753	0.165571	0.170981
SVM	0.884832	0.925759	0.921788	0.760402	0.817912	0.860693	0.840546	0.074241	0.115168
RandomForest	0.89795	0.889644	0.898717	0.77746	0.833373	0.796246	0.840058	0.110356	0.10205
DNN	0.865973	0.916835	0.911645	0.776404	0.818746	0.697053	0.879346	0.083165	0.134027
CBCO-ERNN	0.892496	0.900846	0.901937	0.883595	0.888023	0.823113	0.914308	0.099154	0.107504
GHLBO-based DSA	0.903741	0.911038	0.911406	0.898559	0.901142	0.846085	0.920724	0.088962	0.096259

WSU-ROA method is more efficient in utilizing computational resources, leading to faster and more efficient DDoS attack detection. The reduced cost reflects not only lower processing time but also the better convergence rate achieved through the optimized weight selection process in the hybrid classifier.

7.5 | Statistical Study

Table 7 demonstrates an evaluation of statistical study presented HC + WSU-ROA-based DDoS AD in the cloud over classifiers. For Dataset 1, the proposed model achieves the highest mean accuracy (0.9132) with a low standard deviation (0.0239), indicating both strong and consistent performance. Competing models such as Hybrid HHO-PSO-LSTM [36] (mean is 0.8938) and HybGBS [35] (mean is 0.8916) also perform well but slightly trail the proposed approach. Similar trends are observed in Dataset 2, where the HC + WSU-ROA model again secures the highest mean accuracy (0.9193) and lowest standard deviation (0.01998) among all methods, demonstrating excellent generalization and robustness. Traditional models like SVM, Random Forest, and DNN show competitive but lower performance with higher variability, while deep learning methods like LSTM, CNN, and RNN exhibit greater fluctuations and lower mean accuracies.

TABLE 4 | Assessment on diverse classifiers using UNSW-NB15 dataset.

Methods	Sensitivity	Specificity	Accuracy	Precision	F_measure	MCC	NPV	FPR	FNR
Proposed	0.9368	0.939116	0.943766	0.946422	0.943968	0.915516	0.9437	0.045884	0.0632
LSTM	0.842162	0.864498	0.872455	0.734737	0.78479	0.66413	0.85131	0.135502	0.157838
Deepmaxout	0.745046	0.825314	0.798474	0.772977	0.758754	0.794657	0.815347	0.174686	0.254954
CNN	0.803834	0.925535	0.886946	0.746916	0.77433	0.638233	0.847223	0.074465	0.196166
RNN	0.840949	0.837965	0.848907	0.843024	0.841985	0.546345	0.797705	0.162035	0.159051
SVM	0.90344	0.875661	0.891345	0.817863	0.858524	0.785552	0.893315	0.124339	0.09656
RandomForest	0.871966	0.906469	0.909512	0.761791	0.813164	0.770302	0.859576	0.093531	0.128034
DNN	0.885888	0.850786	0.88436	0.817509	0.850326	0.734718	0.876669	0.149214	0.114112
CBCO-ERNN	0.884535	0.884358	0.900007	0.887012	0.885772	0.824814	0.910003	0.115642	0.115465
GHLBO-based DSA	0.897601	0.898048	0.910947	0.901864	0.899728	0.847489	0.918428	0.101952	0.102399

TABLE 5 | Ablation study on HC + WSU-ROA method for DDoS AD in cloud using DDoS dataset.

Metrics	HC+ WSU-ROA	Proposed with no features	Proposed with existing correlation	Proposed with existing RFE
Precision	0.94345	0.820427	0.792203	0.8023
MCC	0.915004	0.741653	0.575854	0.658489
FNR	0.062523	0.201847	0.190293	0.192845
NPV	0.939973	0.810324	0.784476	0.801439
Specificity	0.941616	0.754407	0.765323	0.756089
F-measure	0.944036	0.785544	0.800859	0.792636
Accuracy	0.939813	0.83626	0.788623	0.812083
FPR	0.050884	0.245593	0.234677	0.243911
Sensitivity	0.937477	0.798153	0.809707	0.807155

TABLE 6 | Ablation study on HC + WSU-ROA method for DDoS AD in cloud using UNSW-NB15 dataset.

Metrics	HC+ WSU-ROA	Proposed with no features	Proposed with existing correlation	Proposed with existing RFE
NPV	0.9437	0.800986	0.781385	0.801284
Precision	0.946422	0.805713	0.788321	0.786978
FNR	0.0632	0.190524	0.193929	0.184162
Specificity	0.939116	0.756342	0.762042	0.749751
MCC	0.915516	0.661256	0.568909	0.614422
F-measure	0.943968	0.795577	0.797097	0.794925
Accuracy	0.943766	0.813762	0.785101	0.798535
FPR	0.045884	0.243658	0.237958	0.250249
Sensitivity	0.9368	0.809476	0.806071	0.815838

7.6 | *K*-Fold Analysis on Datasets 1 and 2

Table 8 represents the *k*-fold cross-validation analysis across both Dataset 1 and Dataset 2 demonstrates that the proposed HC + WSU-ROA model consistently outperforms all baseline models in terms of accuracy across various values of k (from 2 to 6). As *k* increases, the performance of all models improves, but the proposed model achieves the highest accuracy at each fold, reaching 0.942961 (Dataset 1) and 0.939954 (Dataset 2) at $k = 6$. While models like CBCO-ERNN and GHLBO-based DSA show competitive results, they remain consistently lower than the proposed approach. Traditional models such as LSTM, CNN, RNN, SVM, and RandomForest exhibit moderate performance gains with increasing k, but do not match the precision and robustness of the proposed method. These results confirm the effectiveness and stability of the HC + WSU-ROA model across different validation settings, reinforcing its reliability for DDoS attack detection in cloud environments.

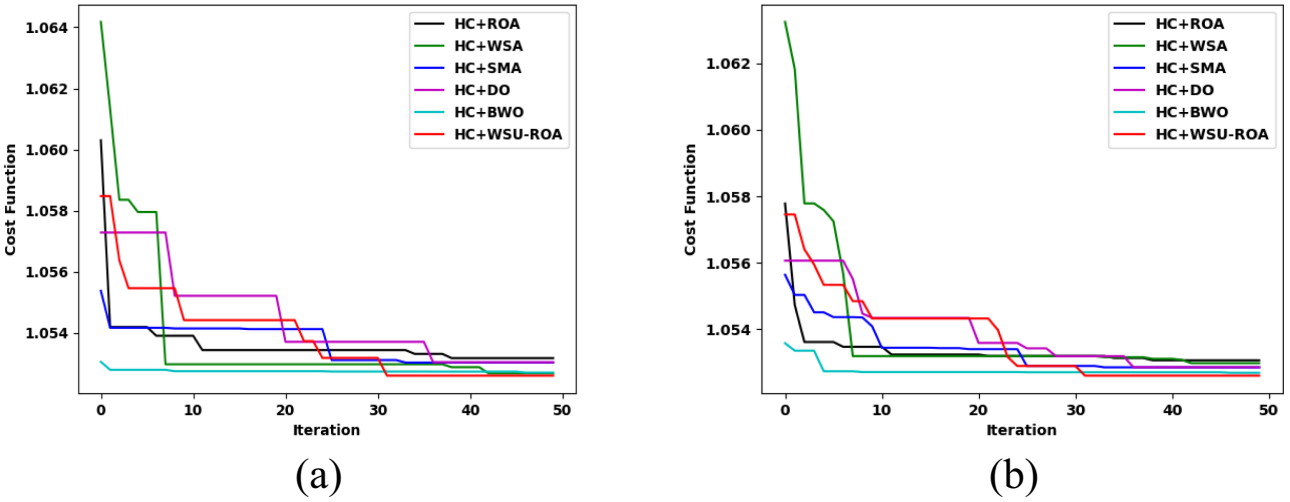

FIGURE 11 | Cost analysis for DDoS AD in the cloud using (a) DDoS Dataset (b) UNSW-NB15 Dataset.

TABLE 7 | Statistical analysis of DDoS AD in the cloud using varied datasets.

	Min	Max	Mean	Median	Standard deviation
Dataset 1					
HC + WSU-ROA	0.879336	0.939813	0.913218	0.916861	0.023992
LSTM	0.737779	0.871835	0.808371	0.811934	0.054755
Deepmaxout	0.735106	0.812528	0.773096	0.772375	0.032039
CNN	0.749542	0.893386	0.824739	0.828015	0.059419
RNN	0.743732	0.808485	0.779794	0.78348	0.027076
SVM	0.785624	0.921788	0.861523	0.869339	0.056677
RandomForest	0.79504	0.898717	0.847731	0.848584	0.043382
DNN	0.776251	0.911645	0.844746	0.845543	0.056515
CBCO-ERNN	0.855182	0.901937	0.878613	0.878667	0.019492
GHLBO-based DSA	0.86122	0.911406	0.887264	0.888215	0.020543
HybGBS	0.86424	0.91614	0.89159	0.89299	0.02109
Hybrid HHO-PSO-LSTM	0.865749	0.918507	0.893752	0.895377	0.021368
Dataset 2					
HC + WSU-ROA	0.89455	0.943766	0.919265	0.919373	0.019984
LSTM	0.727502	0.872455	0.807607	0.815236	0.059242
Deepmaxout	0.723176	0.798474	0.764078	0.767331	0.03031
CNN	0.747691	0.886946	0.820075	0.822832	0.056294
RNN	0.740346	0.848907	0.797943	0.801259	0.047443
SVM	0.780567	0.891345	0.846243	0.85653	0.044921
RandomForest	0.789519	0.909512	0.849613	0.849711	0.047869
DNN	0.771002	0.88436	0.830482	0.833283	0.044068
CBCO-ERNN	0.85818	0.900007	0.87669	0.874286	0.015903
GHLBO-based DSA	0.867272	0.910947	0.887334	0.885558	0.016831
HybGBS [35]	0.871819	0.916417	0.892656	0.891194	0.017321
Hybrid HHO-PSO-LSTM [36]	0.874092	0.919152	0.895317	0.894012	0.017572

TABLE 8 | Analysis of k-fold in datasets 1 and 2.

K values	*K* = 2	*K* = 3	*K* = 4	*K* = 5	*K* = 6
Dataset 1					
Proposed	0.903108	0.907383	0.918733	0.93758	0.942961
LSTM	0.747361	0.76369	0.802734	0.807435	0.826806
Deepmaxout	0.73148	0.753042	0.778656	0.791259	0.792281
CNN	0.795909	0.827559	0.848439	0.861203	0.872623
RNN	0.747191	0.772007	0.775706	0.786245	0.793494
SVM	0.807338	0.843239	0.845939	0.887628	0.920493
RandomForest	0.791957	0.824113	0.836651	0.845932	0.882188
DNN	0.799906	0.844834	0.887621	0.891107	0.899476
CBCO-ERNN	0.870471	0.886277	0.894108	0.898853	0.904483
GHLBO-based DSA	0.866159	0.866785	0.870377	0.900992	0.911719
Dataset 2					
Proposed	0.907935	0.91212	0.917599	0.933787	0.939954
LSTM	0.736877	0.756662	0.765386	0.8147	0.85744
Deepmaxout	0.744165	0.765483	0.767479	0.783539	0.786353
CNN	0.749014	0.757828	0.778745	0.798385	0.831333
RNN	0.730874	0.744397	0.777809	0.801087	0.841768
SVM	0.771262	0.774867	0.802727	0.817598	0.895533
RandomForest	0.786272	0.795153	0.812374	0.846125	0.849346
DNN	0.774254	0.83029	0.83931	0.85912	0.860444
CBCO-ERNN	0.85264	0.86744	0.878794	0.891931	0.900082
GHLBO-based DSA	0.858393	0.869328	0.879348	0.892418	0.91509

TABLE 9 | Cross validation results on both datasets.

Metrics	Training with Dataset 1 and testing with Dataset 2	Training with Dataset 2 and testing with Dataset 1
Sensitivity	0.884454	0.889481
Specificity	0.914572	0.901807
Accuracy	0.905824	0.90811
Precision	0.862923	0.84058
F-measure	0.873556	0.864339
MCC	0.779449	0.789823
NPV	0.894557	0.897505
FPR	0.085428	0.098193
FNR	0.115546	0.110519

7.7 | Cross Validation Analysis

The cross-validation results, where the proposed DDoS detection model is trained on one dataset and tested on the other, demonstrate the model's strong generalization capability across varying data distributions. Table 9 represents the cross-validation analysis. When trained on Dataset 1 and tested on Dataset 2, the model achieves an accuracy of 90.58%, with a sensitivity of 88.45% and specificity of 91.46%, indicating reliable detection of both attack and normal traffic. Conversely, training on Dataset 2 and testing on Dataset 1 with a sensitivity of 88.95% and specificity of 90.18,1% produces a somewhat better accuracy of 90.81%. Metrics like F1-score (up to 86.43%) and MCC (up to 78.98%) remain strong, despite the fact that both setups exhibit a slight decline in performance when compared to intra-dataset evaluations. This indicates that the model has good predictive power and stability across many datasets. In real-world situations when data variances are unavoidable, these outcomes confirm the model's efficacy and flexibility.

7.8 | ROC Curve Analysis

The performance of the proposed HC + WSU-ROA model, we conducted a receiver operating characteristic (ROC) curve analysis, which plots the true positive rate (TPR) against the false positive rate (FPR) at various classification thresholds in Figure 12. The TPR, also known as Recall or Sensitivity, reflects the model's ability to correctly identify attack traffic, while the FPR represents the proportion of normal traffic incorrectly classified as attacks. An ideal model would achieve a TPR close to 1 with an FPR close to 0, resulting in a ROC curve that approaches the top-left corner of the plot. In our analysis, the proposed model consistently demonstrated a superior ROC profile compared to baseline models, indicating strong discriminative power. Additionally, the area under the curve (AUC) value was significantly higher for HC + WSU-ROA, confirming its effectiveness in maintaining high detection rates while minimizing false positives—a

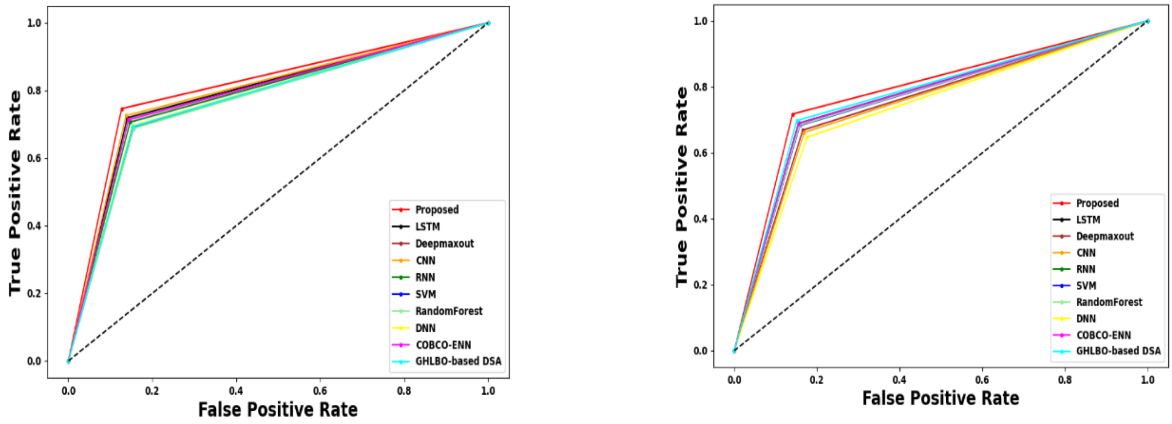

FIGURE 12 | ROC curve analysis on (a) Dataset 1 and (b) Dataset 2.

TABLE 10 | DDoS detection model using different optimizers (RMSprop, SGD, and Adam).

Metrics	Proposed with Rmsprop optimizer	Proposed with SGD	Proposed (Adam)	Proposed without optimization
Dataset 1				
Sensitivity	0.921293	0.925795	0.937477	0.89329
Specificity	0.910703	0.920869	0.941616	0.884023
Accuracy	0.930855	0.931598	0.939813	0.901656
Precision	0.910742	0.918147	0.94345	0.884058
F_measure	0.915987	0.921956	0.944036	0.88865
MCC	0.865622	0.878928	0.915004	0.844577
NPV	0.933361	0.935481	0.939973	0.903849
FPR	0.089297	0.079131	0.050884	0.115977
FNR	0.078707	0.074205	0.062523	0.10671
Dataset 2				
Sensitivity	0.933453	0.935127	0.9368	0.902459
Specificity	0.929355	0.934235	0.939116	0.886102
Accuracy	0.941151	0.942458	0.943766	0.909304
Precision	0.933757	0.94009	0.946422	0.901746
F_measure	0.933605	0.937602	0.943968	0.902102
MCC	0.901631	0.908573	0.915516	0.841537
NPV	0.94321	0.943455	0.9437	0.907654
FPR	0.070645	0.065765	0.045884	0.113898
FNR	0.066547	0.064873	0.0632	0.097541

critical requirement in real-time cloud-based DDoS detection systems.

7.9 | Comparison of the Proposed DDoS Detection Model Using Different Optimizers (RMSprop, SGD, and Adam)

Table 10 presents a comparative performance analysis of the proposed hybrid DDoS detection model when trained with three different optimization algorithms: RMSprop, SGD, and Adam. The proposed DDoS detection model exhibits consistently strong performance across both datasets, with the Adam optimizer outperforming all other configurations. For Dataset 1, the model optimized with Adam achieves the highest Accuracy (93.98%), F1-Score (94.40%), and MCC (91.50%), with the lowest FPR (5.08%) and false negative rate (FNR; 6.25%), indicating superior detection capability. Similarly, in Dataset 2, Adam again leads with the best Accuracy (94.38%), Precision (94.64%), and MCC (91.55%), further reducing error rates compared to RMSprop and SGD. Both RMSprop and SGD offer competitive performance,

TABLE 11 | Analysis of data variations for various metrics.

Data variation	Sensitivity	Specificity	Accuracy	Precision	F_measure	MCC	NPV	FPR	FNR
Dataset 1									
25%	0.899971	0.871733	0.914644	0.85977	0.870666	0.795287	0.925676	0.079212	0.124399
50%	0.910249	0.887847	0.929148	0.896299	0.887174	0.837193	0.927821	0.073098	0.11412
75%	0.928257	0.928511	0.932123	0.92592	0.929879	0.890417	0.936302	0.058736	0.073266
100%	0.937477	0.941616	0.939813	0.94345	0.944036	0.915004	0.939973	0.050884	0.062523
Dataset 2									
25%	0.913382	0.890144	0.928141	0.893719	0.895096	0.845607	0.940111	0.058199	0.099389
50%	0.923411	0.900073	0.933308	0.895761	0.909228	0.859977	0.941738	0.055479	0.089554
75%	0.930106	0.919594	0.938537	0.921092	0.926598	0.887746	0.942719	0.050682	0.076377
100%	0.9368	0.939116	0.943766	0.946422	0.943968	0.915516	0.9437	0.045884	0.0632

though slightly behind Adam. The version of the model without optimization performs the worst across all metrics in both datasets, highlighting the critical role of optimization algorithms in enhancing detection efficiency and robustness. Overall, the results reinforce the effectiveness of the Adam optimizer in training deep learning models for accurate DDoS attack detection in cloud environments.

7.10 | Scalability Analysis of Both Datasets

Table 11 represents the scalability analysis of both datasets revealing a consistent improvement in performance metrics as data variation increases from 25% to 100%, indicating that the proposed model scales effectively with larger data volumes. In both sets, key evaluation parameters such as sensitivity, specificity, accuracy, precision, F-measure, and Matthews correlation coefficient (MCC) show a steady rise, reflecting enhanced detection capability and robustness. Specifically, sensitivity improves from approximately 0.89–0.91 at 25% data to over 0.93 at full data utilization, while accuracy rises from ˜91 to ˜92% to ˜94%. Notably, error rates such as FPR and FNR decline steadily, with FPR dropping from around 0.08 to below 0.05 and FNR reducing from over 0.12 to just above 0.06. These trends demonstrate that the model maintains high classification performance and generalization as data size increases, confirming its scalability and suitability for big data environments, especially in real-time DDoS detection scenarios.

7.11 | Computational Time Analysis of Datasets 1 and 2

The computational time analysis across two datasets in Table 12. It demonstrates that the proposed HC + WSU-ROA model consistently achieves the lowest execution time, with 30031.12 and 30010.90 units for Dataset 1 and Dataset 2, respectively. In comparison, other hybrid classifier models integrated with different optimization algorithms such as ROA, WSA, SMA, DO, and BWO exhibited higher processing times. The HC + DO model recorded the highest computational time, followed by SMA and BWO. Additionally, the WSU-ROA algorithm involves iterative optimization, which increases the computational burden during the training phase. However, this overhead is mitigated through the use of the MapReduce framework, which enables distributed processing of large-scale traffic data. These results indicate that WSU-ROA not only enhances detection accuracy but also improves computational efficiency, making it a more suitable choice for real-time DDoS attack detection in large-scale cloud environments.

TABLE 12 | Time analysis of both datasets.

Methods	Dataset 1 (s)	Dataset 2 (s)
HC + ROA	30,402.10	30,353.19
HC + WSA	31,307.98	31,302.13
HC + SMA	32,011.24	31,989.0
HC + DO	33,075.75	32,892.81
HC + BWO	32,048.84	32,023.10
HC + WSU-ROA	30,031.12	30,010.90

8 | Practical Implications

The proposed hybrid bio-inspired deep learning model for DDoS attack detection offers significant practical advantages in cloud environments, including real-time detection, enhanced accuracy, and scalability. By leveraging LSTM, DMO, and WSU-ROA, the model efficiently processes large-scale network traffic, ensuring rapid and accurate identification of DDoS attacks, even in dynamic cloud systems with fluctuating data loads. This reduces false positives and minimizes service disruptions, leading to lower operational costs and improved system stability. Furthermore, the model's adaptability to evolving attack strategies makes it a sustainable, long-term solution for cloud providers, ensuring continuous protection against emerging threats while maintaining energy efficiency and compliance with industry security standards.

9 | Conclusion

In this work, we used big data analytics to address the growing threat of DDoS attacks by proposing a hybrid bio-inspired deep

learning model for AD detection in cloud environments. The model combines an enhanced RFE technique to find the most pertinent features for attack detection with a MapReduce framework for scalable feature extraction. The heart of the detection mechanism lies in the hybrid classifier (LSTM + DMO), which is optimally weighted using the WSU-ROA algorithm to enhance classification performance. From analysis, the proposed model gained a high accuracy when LP = 90 for both datasets. Similarly, the MCC seems to be better with a rise in LPs. Therefore, for every LP, the proposed method showed the finest outputs over the other existing methods. The MCC of HC+ WSU-ROA was high at about 0.95% at LP = 90 over HC + ROA, HC + WSA, HC + SMA, HC + DO, and HC + BWO. To improve the suggested model's flexibility in identifying new and adaptable DDoS attacks in real-time, we intend to investigate the use of reinforcement learning techniques in subsequent work. Additionally, the model could be extended to handle multi-cloud environments, ensuring robust detection across diverse platforms. To further improve and extend the presented research, future work could focus on enhancing the model's scalability and performance by incorporating additional advanced optimization techniques and leveraging deep reinforcement learning to dynamically adjust detection thresholds based on changing network conditions. Additionally, integrating the model with real-time threat intelligence feeds could help detect emerging DDoS attack strategies more effectively. Future research could also explore the use of transfer learning to improve the model's generalization across different cloud service providers and industries. Finally, exploring the integration of multi-modal data, such as combining network traffic data with system logs and external threat data, could further strengthen the model's robustness and detection accuracy.

Nomenclature

AD	attack detection
ANN	artificial neural networks
AVDR	attacked VM detection and recovery
BWO	black widow optimization
CC	cloud computing
CNN	convolutional neural networks
DBN	deep belief network
DDoS	distributed denial of service
DL	deep learning
DMO	deep max out
DNN	deep neural network
DO	dingo optimization
DT	decision tree
FS-WOA-DNN	feature selection-whale optimization—DNN
FT-EHO	fuzzy and Taylor elephant herd optimization
HC	hybrid classifier
LP	learning percentage
LSTM	long short term memory
LSTM-NN	LSTM-neural networks
MI	mutual information
ML	machine learning
MR	map reduce
PSD	power spectral density
RFE	recursive feature elimination
RNN	recurrent neural networks
ROA	Remora optimization algorithm
SAE	sparse autoencoder
SaE-ELM	Self-adaptive evolutionary ELM
SFO	Swordfish optimization algorithm
SLFNs	single hidden layer feed forward neural networks
SMA	slime mold algorithm
SVM	support vector machine
TPA	third-party auditor
V-ELM	voting extreme learning machine
WOA	whale optimization
WSA	white shark optimizer
WSU-ROA	white shark updated remora optimization

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. P. Harikrishna and A. Amuthan, "Rival-Model Penalized Self-Organizing Map Enforced DDoS Attack Prevention Mechanism for Software Defined Network-Based Cloud Computing Environment," *Journal of Parallel and Distributed Computing* 154 (2021): 142–152.

2. O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Optimal Load Distribution for the Detection of VM-Based DDoS Attacks in the Cloud," *IEEE Transactions on Services Computing* 13, no. 1 (2020): 114–129.

3. S. Velliangiri and H. M. Pandey, "Fuzzy-Taylor-Elephant Herd Optimization Inspired Deep Belief Network for DDoS Attack Detection and Comparison With State-Of-The-Arts Algorithms," *Future Generation Computer Systems* 110 (2020): 80–90.

4. F. J. Abdullayeva, "Distributed Denial of Service Attack Detection in E-Government Cloud via Data Clustering," *Array* 15 (2022): 100229.

5. P. Verma, S. Tapaswi, and W. W. Godfrey, "A Request Aware Module Using CS-IDR to Reduce VM Level Collateral Damages Caused by DDoS Attack in Cloud Environment," *Cluster Computing* 24, no. 3 (2021): 1917–1933.

6. P. Verma, S. Tapaswi, and W. W. Godfrey, "AVDR: A Framework for Migration Policy to Handle DDoS Attacked VM in Cloud," *Wireless Personal Communications* 115, no. 2 (2020): 1335–1361.

7. R. F. Fouladi, O. Ermiş, and E. Anarim, "A DDoS Attack Detection and Defense Scheme Using Time-Series Analysis for SDN," *Journal of Information Security and Applications* 54 (2020): 102587.

8. A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse Autoencoder for Detection of DDoS Attacks in Cloud," *IEEE Access* 8 (2020): 181916–181929.

9. K. Singh, K. S. Dhindsa, and D. Nehra, "T-CAD: A Threshold Based Collaborative DDoS Attack Detection in Multiple Autonomous Systems," *Journal of Information Security and Applications* 51 (2020): 102457.

10. K. S. Sahoo, B. K. Tripathy, K. Naik, et al., "An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks," *IEEE Access* 8 (2020): 132502–132513.

11. Z. Abou El Houda, L. Khoukhi, and A. S. Hafid, "Bringing Intelligence to Software Defined Networks: Mitigating DDoS Attacks," *IEEE Transactions on Network and Service Management* 17, no. 4 (2020): 2523–2535.

12. N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," *IEEE Internet of Things Journal* 7, no. 4 (2020): 3559–3570.

13. R. Swami, M. Dave, and V. Ranga, "IQR-Based Approach for DDoS Detection and Mitigation in SDN," *Defence Technology* 25 (2022): 76–87.

14. A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS Attacks With Feed Forward Based Deep Neural Network Model," *Expert Systems With Applications* 169 (2021): 114520.

15. G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. M. Lee, and D. S. Kim, "Composite and Efficient DDoS Attack Detection Framework for B5G Networks," *Computer Networks* 188 (2021): 107871.

16. A. Agarwal, M. Khari, and R. Singh, "Detection of DDOS Attack Using Deep Learning Model in Cloud Storage Application," *Wireless Personal Communications* 127 (2021): 419–439.

17. X. Liu, J. Ren, H. He, B. Zhang, C. Song, and Y. Wang, "A Fast All-Packets-Based DDoS Attack Detection Approach Based on Network Graph and Graph Kernel," *Journal of Network and Computer Applications* 185 (2021): 103079.

18. N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS Attack Detection in Software Defined Networking," *Journal of Network and Computer Applications* 187 (2021): 103108.

19. V. de Miranda Rios, P. R. Inácio, D. Magoni, and M. M. Freire, "Detection of Reduction-Of-Quality DDoS Attacks Using Fuzzy Logic and Machine Learning Algorithms," *Computer Networks* 186 (2021): 107792.

20. J. H. Corrêa, P. M. Ciarelli, M. R. Ribeiro, and R. S. Villaça, "Ml-Based Ddos Detection and Identification Using Native Cloud Telemetry Macroscopic Monitoring," *Journal of Network and Systems Management* 29, no. 2 (2021): 13.

21. M. A. Monge, A. H. González, B. L. Fernández, D. M. Vidal, G. R. García, and J. M. Vidal, "Traffic-Flow Analysis for Source-Side DDoS Recognition on 5G Environments," *Journal of Network and Computer Applications* 136 (2019): 114–131.

22. G. S. Kushwah and V. Ranga, "Optimized Extreme Learning Machine for Detecting DDoS Attacks in Cloud Computing," *Computers & Security* 105 (2021): 102260.

23. A. S. Mamolar, Z. Pervez, J. M. Calero, and A. M. Khattak, "Towards the Transversal Detection of DDoS Network Attacks in 5G Multi-Tenant Overlay Networks," *Computers & Security* 79 (2018): 132–147.

24. M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "A DDoS Attack Mitigation Framework for IoT Networks Using Fog Computing," *Procedia Computer Science* 182 (2021): 13–20.

25. A. S. Mamolar, P. Salvá-García, E. Chirivella-Perez, Z. Pervez, J. M. Calero, and Q. Wang, "Autonomic Protection of Multi-Tenant 5G Mobile Networks Against UDP Flooding DDoS Attacks," *Journal of Network and Computer Applications* 145 (2019): 102416.

26. B. Hussain, Q. Du, B. Sun, and Z. Han, "TraG: A Trajectory Generation Technique for Simulating Urban Crowd Mobility," *IEEE Transactions on Industrial Informatics* 17, no. 2 (2021): 860–870.

27. B. Bouyeddou, B. Kadri, F. Harrou, and Y. Sun, "DDOS-Attacks Detection Using an Efficient Measurement-Based Statistical Mechanism," *Engineering Science and Technology, an International Journal* 23, no. 4 (2020): 870–878.

28. J. A. Perez-Diaz, I. A. Valdovinos, K. K. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access* 8 (2020): 155859–155872.

29. K. Bhushan and B. B. Gupta, "Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)-based Cloud Computing Environment," *Journal of Ambient Intelligence and Humanized Computing* 10, no. 5 (2019): 1985–1997.

30. G. S. Kushwah and V. Ranga, "Voting Extreme Learning Machine Based Distributed Denial of Service Attack Detection in Cloud Computing," *Journal of Information Security and Applications* 53 (2020): 102532.

31. S. Mahdavi Hezavehi and R. Rahmani, "An Anomaly-Based Framework for Mitigating Effects of DDoS Attacks Using a Third Party Auditor in Cloud Computing Environments," *Cluster Computing* 23, no. 4 (2020): 2609–2627.

32. E. Arul and A. Punidha, "Supervised Deep Learning Vector Quantization to Detect MemCached DDOS Malware Attack on Cloud," *SN Computer Science* 2, no. 2 (2021): 85.

33. S. Kalvikkarasi and A. Saraswathi, "DDoS Attack Detection in Cloud Computing Using Optimized Elman Neural Network Based on Bacterial Colony Optimization and Centroid Opposition-Based Learning," *International Journal of Computer Networks and Applications* 11, no. 6 (2024): 835–854.

34. S. Balasubramaniam, C. Vijesh Joe, T. A. Sivakumar, et al., "Optimization Enabled Deep Learning-Based Ddos Attack Detection in Cloud Computing," *International Journal of Intelligent Systems* 2023, no. 1 (2023): 2039217.

35. S. Sumathi and R. Rajesh, "HybGBS: A Hybrid Neural Network and Grey Wolf Optimizer for Intrusion Detection in a Cloud Computing Environment," *Concurrency and Computation: Practice and Experience* 36, no. 24 (2024): e8264.

36. S. Sumathi, R. Rajesh, and S. Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection," *Journal of Sensors* 2022, no. 1 (2022): 8530312.

37. S. M. Mahmoud and R. S. Habeeb, "Analysis of Large Set of Images Using MapReduce Framework," *International Journal of Modern Education and Computer* 11, no. 12 (2019): 47–52.

38. P. P. Anchalia, "Improved MapReduce k-Means Clustering Algorithm with Combiner," in *16th International Conference on Computer Modelling and Simulation, UKSim* (IEEE, 2014).

39. Statistics How To, "Correlation Coefficient: Simple Definition, Formula, Easy Steps," https://www.statisticshowto.com/probability-and-statistics/correlation-coefficient-formula/.

40. X. Zeng, Y. W. Chen, and C. Tao, "Feature Selection Using Recursive Feature Elimination for Handwritten Digit Recognition," in *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (IEEE, 2009), 1205–1208.

41. I. Guyon, J. Weston, S. Barnhill, and V. Vapnik, "Gene Selection for cancer Classification Using Support Vector Machines," *Machine Learning* 46, no. 1 (2002): 389–422.

42. K. Chen, "APSO-LSTM: An Improved LSTM Neural Network Model Based on APSO Algorithm," 2020.

43. M. Cai, Y. Shi, and J. Liu, "Deep Maxout Neural Networks for Speech Recognition," in *2013 IEEE Workshop on Automatic Speech Recognition and Understanding* (IEEE, 2013), 291–296.

44. H. Jia, X. Peng, and C. Lang, "Remora Optimization Algorithm," *Expert Systems With Applications* 185 (2021): 115665.

45. M. Braik, A. Hammouri, J. Atwan, M. A. Al-Betar, and M. A. Awadallah, "White Shark Optimizer: A Novel Bio-Inspired meta-Heuristic Algorithm for Global Optimization Problems," *Knowledge-Based Systems* 243 (2022): 108457.

46. UNB, "DDoS Evaluation Dataset (CIC-DDoS2019)," https://www.unb.ca/cic/datasets/ddos-2019.html.

47. UNSW Sydney, "The UNSW-NB15 Dataset," https://research.unsw.edu.au/projects/unsw-nb15-dataset.