

RF-OCSA: A Hybrid Metaheuristic Feature Selection Framework for DDoS Attack Detection in Cloud Environments

Srikanth Indurthi*

School of Computer Science and Engineering (SCOPE), VIT-AP University, Amaravathi, Andra Pradesh, India
E-mail: Srikanth.24phd7007@vitap.ac.in
ORCID iD: <https://orcid.org/0009-0004-2935-8505>

*Corresponding Author

Ganesh Reddy Karri

School of Computer Science and Engineering (SCOPE), VIT-AP University, Amaravathi, Andra Pradesh, India
E-mail: guncity11@gmail.com
ORCID iD: <https://orcid.org/0000-0002-5177-8125>

Received: May 28, 2026; Revised: June 17, 2026; Accepted: July 15, 2026; Published: August 8, 2026

Abstract: Distributed Denial of Service (DDoS) attacks have emerged as one of the most critical cybersecurity threats to cloud computing environments, significantly affecting service availability, resource utilization, and operational reliability. The dynamic nature of cloud traffic and the increasing sophistication of attack patterns make accurate and efficient DDoS detection a challenging task. To address this issue, this paper proposes a hybrid feature-selection and classification framework, namely Random Forest-based Oppositional Crow Search Algorithm (RF-OCSA), for intelligent DDoS attack detection in cloud environments. The proposed framework consists of data preprocessing, optimal feature selection using the Oppositional Crow Search Algorithm (OCSA), and attack classification using the Random Forest (RF) classifier. OCSA employs oppositional learning to enhance search diversity and identify the most discriminative features while reducing feature redundancy and computational overhead. The effectiveness of the proposed RF-OCSA model is evaluated using four benchmark datasets, namely CIC-DDoS2019, AISED, TestCloudIDS, and UNSW-NB15. Experimental analysis is conducted using Accuracy, Sensitivity, Specificity, Precision, and F-measure as evaluation metrics, while NS-3 is utilized to emulate representative cloud-network traffic scenarios. The results demonstrate that RF-OCSA consistently outperforms GHLBO, CNN-LSTM, and DeepDefend by achieving superior detection performance across all datasets, with classification metrics exceeding 98% in most cases. The integration of oppositional feature optimization and ensemble learning significantly improves attack detection capability, reduces false alarms, and enhances model robustness. These findings indicate that RF-OCSA is an effective and scalable framework for securing cloud infrastructures against evolving DDoS attacks.

Index Terms: DDoS, Cloud Computing, Random Forest, Oppositional Crow Search, NS3

1. Introduction

Cloud Computing (CC) services have transformed how businesses and users have been storing, managing, and accessing data for all. CC services have brought a revolution in the way organizations and users around the world have been storing, processing data and accessing it. With the greater adoption of the cloud by enterprises, the delivery of secure and reliable services has become a critical challenge. At the same time, the growth of cloud services has introduced a larger attack surface for cyberattacks and this includes Distributed Denial of Service (DDoS) attacks [1]. In DDoS attacks, the attackers try to make the network or system resources reach their capacity limits so as to cause a significant degradation in service, service downtime, and data unavailability [2]. DDoS attacks are more coordinated as opposed to traditional attacks, are distributed from many different compromised nodes, and constantly change to evade traditional security defenses [3]. Therefore, in a cloud environment, intelligent, adaptive, and data-driven detection mechanisms that can cope with the scale and variety of traffic are required to detect DDoS attacks [4]. As these attacks grow more common and complex, the need for a sophisticated detection capability that can distinguish normal traffic

from malicious traffic in real time with minimal false alarms and efficient use of resources within dynamic cloud environments is more critical than ever.

In recent years, many machine learning and heuristic-based DDoS detection methods have been proposed to defend against DDoS attacks in cloud computing environments. However, traditional statistical and signature-based approaches are not suitable to attack zero-day and polymorphic attacks because they are not flexible enough. In order to learn from previous attack data, machine learning algorithms like SVM, DT and Naïve Bayes Classifiers have been used for attack detection widely [5]. But these models are prone to overfitting and poor performance in high dimensional and imbalanced datasets. Recent advancements have introduced hybrid metaheuristic-based optimization techniques to enhance feature selection and improve classification accuracy [6]. Algorithms such as GA, ACO, and PSO have demonstrated promising results but still exhibit limitations such as slow convergence, premature stagnation, and low generalization capability [7]. Therefore, integrating powerful ensemble learning models with optimization-inspired algorithms presents a potential pathway toward more efficient and adaptive DDoS detection systems for modern cloud infrastructures.

Despite the availability of various detection frameworks, effectively identifying and mitigating DDoS attacks in cloud environments remains a complex and unresolved challenge. Cloud infrastructures are characterized by dynamic resource allocation, fluctuating traffic loads, and heterogeneous service demands, all of which complicate anomaly detection. Traditional detection systems are often unable to adapt to evolving attack strategies or large-scale distributed traffic flows [8]. Furthermore, existing approaches either focus on improving detection accuracy at the cost of computational efficiency or fail to achieve real-time detection performance in large cloud setups. Many classifiers also rely on high-dimensional data without proper feature selection, leading to redundant computations and lower detection precision [9]. To overcome these challenges, there is a pressing need for an intelligent detection mechanism that can efficiently optimize feature subsets, minimize computational complexity, and improve classification performance simultaneously. The motivation for this research arises from bridging the gap between accuracy and efficiency by designing an optimized Random Forest-based detection model enhanced with an Oppositional Crow Search optimization mechanism.

The proposed Random Forest-based Oppositional Crow Search Algorithm (RF-OCSA) introduces a hybrid framework that integrates the robustness of ensemble learning with the adaptive exploration ability of metaheuristic optimization. The Random Forest (RF) classifier is known for its high classification accuracy, resistance to overfitting, and capability to handle large, noisy datasets. However, its performance is significantly influenced by the quality of the input features. To address this, the Oppositional Crow Search Algorithm (OCSA) [10] is employed to perform optimal feature selection by mimicking the intelligent behavior of crows in storing and retrieving food, while oppositional learning enhances search diversity and convergence speed. This hybridization ensures that only the most discriminative features are retained, reducing redundancy and improving classification performance. The RF-OCSA model is evaluated using four benchmark datasets CIC-DDoS2019, AISED (AISED Dataset on Cloud DDoS Attacks), TestCloudIDS, and UNSW-NB15 simulated within the NS3 environment for realistic network emulation [11-14]. The algorithm effectively identifies attack patterns in varying traffic conditions while maintaining high accuracy and computational efficiency, making it a suitable solution for real-time DDoS detection in cloud ecosystems.

Although NS-3 has traditionally been employed for network simulation and protocol evaluation, its use in this study is limited to the emulation of representative cloud-network traffic scenarios. The benchmark datasets used for classification contain attack patterns that closely resemble realistic cloud communication behavior. Consequently, NS-3 provides an additional validation context that supports the practical relevance of the proposed detection framework without replacing the dataset-driven machine-learning evaluation process.

The importance of the proposed RF-OCSA framework is its capability of improving the security and resilience of cloud based infrastructures with the help of intelligent attack detection. Unlike the traditional methods which rely on a set of static rules and non-optimized learning models, the RF-OCSA relies on dynamic adaptability by optimizing the learning model by using metaheuristic. The Oppositional Crow Search mechanism not only lowers the dimensionality of the data, but also gives the feature selection process a knowledge that it keeps the most influential features that are involved in the attack identification process. This allows the framework to maintain a balance between accuracy of detection and computational load, very important for the large scale and real-time cloud environment. This study applies to multiple cloud service models such as Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), and works well in many different deployment architectures. Moreover, the proposed method successfully leverages multiple benchmark datasets, promoting the generalization of the method across various network scenarios and enhancing the reliability and robustness of the method for real-world DDoS detection and prevention systems.

Compared to traditional detection approaches, the RF-OCSA framework exhibits several distinctive advantages that make it highly effective for DDoS detection in cloud environments. Classical classifiers such as SVM and k-NN are often sensitive to noise and require parameter tuning, whereas the Random Forest algorithm inherently handles noise and provides high classification stability. However, when enhanced with the Oppositional Crow Search optimization, RF-OCSA attains superior feature discrimination capabilities that traditional algorithms lack. Moreover, most existing optimization algorithms like PSO and ACO tend to suffer from premature convergence and limited exploration ability in high-dimensional spaces. In contrast, OCSA incorporates oppositional learning to expand search diversity and

prevent stagnation, thereby identifying optimal feature subsets more efficiently. This synergistic integration enables RF-OCSA to outperform conventional methods across different evaluation metrics. Ultimately, the proposed framework not only improves detection precision but also reduces false positives and processing latency, making it a scalable and dependable choice for securing cloud-based infrastructures.

The research problem addressed in this study revolves around the need for an adaptive and intelligent detection framework that effectively identifies DDoS attacks in dynamic cloud environments. The key challenge is to design a detection mechanism that simultaneously enhances accuracy, minimizes false detection rates, and ensures computational scalability across large datasets. Traditional detection systems fall short in achieving these multi-objective requirements due to inefficient feature selection and static classification models. The RF-OCSA framework aims to fill this gap by optimizing both the learning and feature selection phases through a hybrid metaheuristic approach. The primary objectives of this work are as follows:

1. To design an intelligent hybrid framework (RF-OCSA) for efficient DDoS detection in cloud environments.
2. To employ the Oppositional Crow Search Algorithm for optimal feature selection and dimensionality reduction.
3. To evaluate the performance of RF-OCSA using benchmark datasets (CIC-DDoS2019, AISED, TestCloudIDS, and UNSW-NB15) under NS3 simulation.
4. To validate the proposed model's effectiveness using key performance metrics such as Accuracy, Sensitivity, Specificity, Precision, and F-measure.

In Section 2, we give a detailed survey of the related works on DDoS detection approaches, particularly focusing on the existing machine learning and optimization-based approaches. In Section 3, the proposed RF-OCSA framework is discussed in detail, consisting of architectural design, selection of features and classification strategy. Section 4 presents the experiments setup, the characteristics of the experimental data set, the environment for the simulation with NS3, and discusses the results and performance evaluation of the proposed model with the existing state-of-the-art model. Finally, in Section 5 the conclusions and future work areas for overall contributions are summarized and potential future work on intelligent DDoS detection systems is suggested.

2. Related works

Recent studies have explored Binary Crow Search Algorithm (BCSA) and Opposition-Based Crow Search Algorithm (OBCSA) for feature-selection optimization. BCSA improves discrete search capability through binary encoding; however, it often suffers from premature convergence when dealing with high-dimensional intrusion datasets. OBCSA introduces opposition-based learning to enhance population diversity and improve exploration. Despite these improvements, most existing approaches rely on single classifiers and do not exploit ensemble-learning strategies for robust attack detection. The proposed RF-OCSA framework addresses these limitations by combining oppositional search-based feature optimization with Random Forest ensemble classification, thereby improving both feature quality and classification reliability.

Rizk Allah et al. [15] propose an oppositional binary crow search algorithm (OBCSA) paired with an optimal stacked autoencoder (OSAE) to address high-dimensional feature spaces common in network intrusion detection. The paper frames feature selection as a wrapper optimization task and introduces oppositional learning within a binary CSA to better explore the search space and avoid premature stagnation. The OBCSA selectively retained discriminative features before feeding them into the stacked autoencoder, improving detection accuracy and lowering false positives on benchmark datasets. The authors report that the oppositional component increases population diversity and accelerates convergence, making the approach particularly useful in noisy, imbalanced network traffic scenarios. The study's modular design an optimized wrapper search followed by a deep feature extractor highlights a practical pathway for enhancing classical classifiers with metaheuristic-based preprocessing in IDS tasks.

Hamed Alnaish et al. [16] present a hybrid binary Crow Search Algorithm (BCSA) enhanced with a quasi-oppositional (QO) mechanism for feature selection, demonstrating meaningful gains for classification tasks in intrusion detection. The paper carefully evaluates the hybrid BCSA against standard binary metaheuristics, showing that introducing quasi-oppositional positions produces a broader sampling of the search space and reduces the risk of local optima entrapment. Experiments in the work indicate reduced feature subsets with maintained or improved classification metrics, emphasizing reduced computational load for downstream classifiers. The study also discusses parameter sensitivity and robustness, providing guidance on population size and opposition strategies for practitioners applying wrapper-style FS in security datasets. This paper is relevant for DDoS detection research because it validates oppositional enhancements to CSA variants specifically for binary/discrete search problems (i.e., feature selection) and shows direct benefits when integrated with classification pipelines.

Xu et al. [17] propose an improved Crow Search Algorithm variant that combines oppositional forgetting and learning components (an O-CSA family) to bolster global exploration while maintaining local exploitation capabilities. The study carefully analyses classical CSA weaknesses slow convergence and sensitivity to initial positions and addresses them through an oppositional learning scheme plus an adaptive memory forgetting that prevents outdated

solutions from biasing the search. Benchmarks on standard optimization test functions and a case study for feature selection reveal that the modified crow behaviors markedly enhance search dynamics and solution quality. The authors argue that such mechanistic improvements are especially beneficial when metaheuristics are used as wrappers for feature selection in IDS contexts, where timely convergence and robust feature subset selection directly impact classification latency and accuracy. The methodological insights in this paper inform how oppositional strategies can be tuned when pairing CSA with classifiers like Random Forest.

Hossain et al. [18] develop a hybrid feature-selection and ensemble-classification framework designed explicitly for robust DDoS detection. The paper integrates filter and wrapper style selection with an ensemble classifier, reporting experiments on CIC-DDoS2019 and related datasets. Their hybrid pipeline first applies statistical/entropy-based filters to remove irrelevant features, then employs a wrapper optimization to fine-tune the subset for an ensemble learner. Results show improvements in accuracy and F-measure compared to single-stage FS approaches; importantly, the authors analyses sensitivity and specificity alongside precision, demonstrating the framework's balanced performance for both detection and false-alarm control. Also, author discuss computational trade-offs and suggest that combining lightweight filters with metaheuristic wrappers is an effective strategy in large cloud traffic datasets. The design decisions and results provide a practical baseline for RF-OCSA-style hybrids that aim to retain ensemble strengths while exploiting metaheuristic search.

Ramzan et al. [19] propose a deep learning architecture (CNN-BiLSTM) for DDoS classification and evaluate it extensively on the CIC-DDoS2019 dataset within a realistic traffic modelling context. Their contribution centers on combining convolutional layers for local pattern extraction with bidirectional LSTM layers to capture temporal dependencies across flows. The paper reports very high accuracy metrics and emphasizes how sequence modelling yields better sensitivity to evolving DDoS patterns than purely static models. Though focused on deep networks rather than metaheuristics, the work highlights two important lessons for hybrid RF-OCSA designs: (1) temporal/flow-level features materially improve detection, and (2) excessive dimensionality can be mitigated via learned representations or prior feature selection. The authors thorough ablation and metric reporting (accuracy, precision, recall, F1) provide useful comparative baselines and underscore the importance of dataset-specific preprocessing when evaluating IDS solutions.

Akgün et al. [20] present a deep-learning-centric intrusion detection model aimed at distinguishing varied DDoS attack types. They examine multiple architectures and training regimes and emphasize issues relevant to cloud IDS: class imbalance, variable packet rates, and attack polymorphism. Their experiments reveal that while deep models can achieve high detection accuracy, success depends critically on curated training data and feature engineering; moreover, feature selection or dimensionality reduction prior to deep model training often reduces training time without harming performance. The paper's analysis of false positive drivers and deployment considerations in real networks provides practical insights for researchers integrating metaheuristic feature selectors with robust classifiers particularly the trade-offs between off-line optimization and on-line inference latency that RF-OCSA must balance in cloud contexts.

Wang, Yingqing et al. [21] (NS-3 simulation focus) evaluate machine learning-driven anomaly detection schemes using NS-3 to emulate realistic network and IoT/cloud traffic scenarios. Their study underscores the value of NS-3 as a controllable environment for generating labelled attack and benign traffic under reproducible network conditions, allowing for rigorous comparison across algorithms. The authors illustrate how simulation-derived datasets can reveal performance limits under various link delays, traffic bursts, and coordinated DDoS strategies conditions that are difficult to capture in passive captures alone. The paper's methodology emphasizes careful emulation of attack rates and temporal patterns, which is particularly relevant for RF-OCSA evaluations relying on NS-3: realistic simulation helps validate whether metaheuristic-selected features generalize beyond static, pre-collected datasets. It also discusses the integration of simulation outputs with ML pipelines and the need for metric suites covering accuracy, sensitivity, and specificity.

Chen et al. [22] analyses enhancements to machine learning-based DDoS detection via improved feature selection and ensemble methods, reporting detailed experiments across multiple public datasets. Their results show that carefully chosen feature subsets identified using mutual information, correlation analysis, or wrapper searches can substantially increase precision and F-measure while reducing computation. Chen also compares ensemble learners (including Random Forest) and demonstrates RF's consistent robustness across noisy and imbalanced samples, but they stress that RF performance hinges on the input feature quality. The paper's discussion about opposing objectives (maximize sensitivity while minimizing false positives) and its multi-metric evaluation framework offers directly applicable guidance to RF-OCSA: effective oppositional metaheuristic search must be evaluated with a broad metrics (Accuracy, Sensitivity, Specificity, Precision, F-measure) to capture real operational utility.

Sawah et al. [23] examine Random Forest and other supervised classifiers for DDoS classification in cloud contexts with emphasis on feature-selection pipelines. Their study conducts cross-dataset experiments and highlights how RF often outperforms linear and single-tree methods when trained on discriminative features; however, they caution that naive high-dimensional inputs can inflate training time and reduce practical deployability. The paper also demonstrates the stability of RF across varying attack mixes and validates results using multiple evaluation metrics, underscoring the algorithm's utility as a backbone classifier. The work concludes that pairing RF with an effective

optimization-based feature selector yields a pragmatic compromise between accuracy and real-time feasibility exactly the engineering goal RF-OCSA targets.

A broader comparative study [24] examining multiple ML classifiers on CIC-DDoS2019 and related corpora shows that ensemble methods and hybrid pipelines consistently achieve superior F-measure and lower false positive rates than single models. These surveys compile results from many experimental studies and emphasize reproducibility, dataset partitioning strategies, and the importance of reporting sensitivity and specificity alongside accuracy. The comparative analyses underscore recurring recommendations: (1) employ rigorous cross-validation and temporal splits, (2) apply dimensionality reduction to limit overfitting, and (3) evaluate on multiple datasets (e.g., CIC-DDoS2019, UNSW-NB15, TestCloudIDS) to claim generalization. For RF-OCSA, these community findings validate the combined strategy of optimized feature selection plus ensemble classification and reinforce the need for multi-dataset and NS-3-based validation to demonstrate operational robustness.

Mittal et al. [25] describe emulation-based dataset generation approaches (DDoS-AT-2022 and similar) that aim to capture realistic application and transport-layer DDoS variants. These dataset creation efforts highlight that vendor/academic datasets vary widely in their attack mixes, labelling rigor, and traffic realism factors that critically affect IDS benchmarking. The authors illustrate best practices for dataset documentation, attack-rate parameterization, and mixed-traffic generation using testbeds and network emulators. Their recommendations use varied attack intensities, include flash and low-and-slow patterns, and provide detailed feature extraction guidelines are directly relevant for researchers evaluating RF-OCSA: to prove generalizability, models must be tested on both curated public corpora (CIC-DDoS2019, UNSW-NB15) and emulation-based cloud DDoS datasets (TestCloudIDS, DDoS-AT variants).

Table 1. Comparative Study of various existing works

Technique / Algorithm Used	Parameters Used	Dataset Used	Limitations
OBCSA [15]	Accuracy, Precision, Recall, F1-score	UNSW-NB15, NSL-KDD	High computational cost due to deep autoencoder; lacks real-time evaluation.
BCSA [16]	Accuracy, Sensitivity, Specificity, F-measure	CICIDS2017	Convergence speed depends on parameter tuning; limited validation on cloud datasets.
O-CSA [17]	Accuracy, Convergence Rate, Feature Reduction	Benchmark optimization datasets	Focused on mathematical benchmark tests; lacks application to IDS or DDoS detection.
Ensemble Classifier [18]	Accuracy, Sensitivity, Specificity, F1-score	CIC-DDoS2019	Computationally heavy for large-scale cloud traffic; lacks adaptive optimization layer.
CNN-BiLSTM [19]	Accuracy, Precision, Recall, F-measure	CIC-DDoS2019	High training time and requires large labeled datasets; prone to overfitting.
DL based IDS Framework [20]	Accuracy, Precision, Recall, F1-score	UNSW-NB15, CICIDS2017	Poor interpretability; requires significant preprocessing and resource overhead.
ML-based Anomaly Detection [21]	Accuracy, Sensitivity, Specificity, Throughput	Simulated NS-3 datasets	Simulation-based evaluation only; no validation on real-world datasets.
Ensemble ML with Feature Optimization [22]	Accuracy, Precision, Recall, F-measure	CIC-DDoS2019, UNSW-NB15	Feature selection relies on statistical metrics; lacks metaheuristic optimization.
Random Forest and Supervised Classifiers [23]	Accuracy, Sensitivity, Specificity, Precision	CIC-DDoS2019, A1SET	High-dimensional data increases training time; absence of feature optimization stage.
DDoS-AT [25]	Accuracy, Precision, Recall	DDoS-AT, CIC-DDoS2019	Focused on dataset design; lacks algorithmic innovation for detection improvement.

From this table 1 Most existing works emphasize classification accuracy but overlook the trade-off between feature dimensionality and real-time detection efficiency. Few incorporate metaheuristic optimizations for feature selection, and even fewer address multi-dataset generalization under realistic cloud conditions. This motivates the proposed Random Forest-based Oppositional Crow Search Algorithm (RF-OCSA), which integrates ensemble learning and oppositional optimization to achieve high Accuracy, Sensitivity, Specificity, Precision, and F-measure while reducing computational overhead in NS3-simulated cloud environments.

3. Research methodology

The section describes the research methodology that has been used in the study, with reference to the proposed architecture, problem formulation and the RF-OCSA approach. The methodology will aim at developing a systematic framework of assessing the efficiency of RF-OCSA in handling the issues of DDoS attack detection in cloud environments.

3.1. Proposed Architecture

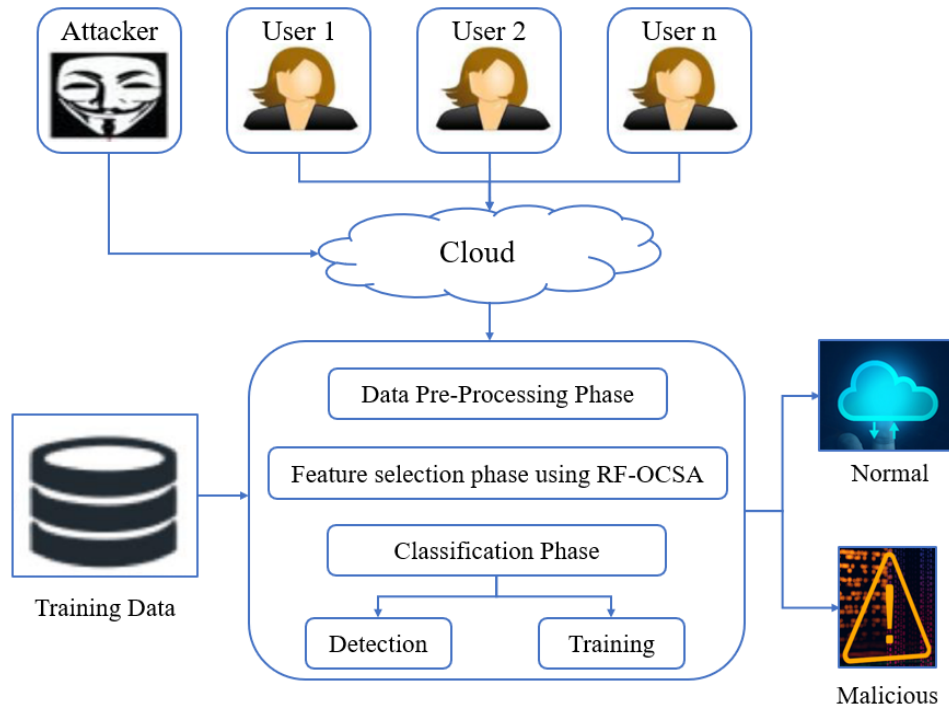


Fig. 1. Proposed Architecture

Figure 1 shows the proposed architecture of the Random Forest based Oppositional Crow Search Algorithm (RF-OCSA) for DDoS Attack Detection in the cloud environment that has three stages: Data Pre-processing, Feature Selection and Classification. First, data is gathered from various legitimate cloud users and users who might be attackers and is combined into the cloud system. The incoming traffic and training data are stored in a centralized database, then a pre-processing step removes noise, normalizes and structures the raw traffic features into machine-readable, structured and meaningful formats. This eliminates unwanted and irrelevant data from the system and only good data is kept for analysis. The pre-processed data is given as input to the feature selection module where the hybrid RF-OCSA model starts optimizing the relevant features from a large number of features extracted from datasets like CIC-DDoS2019, AISD, TestCloudIDS, and UNSW-NB15.

During the Feature Selection Phase, the Oppositional Crow Search Algorithm (OCSA) is proposed to improve the search space exploration by oppositional learning principle to find the most discriminative features for DDoS detection. These best attributes are then provided to the Random Forest (RF) classifier in the Classification Phase. The Random Forest model is used for both the training and detection phases and classifies network traffic as normal or malicious traffic by learning the patterns. The powerful decision-making capabilities of RF with the global optimization capabilities of OCSA results in more accurate, sensitive and specific detection. The system can continuously learn and evolve to new attack behaviors, and it's extremely efficient when it comes to detecting complex and evolving DDoS attacks in real time in cloud environments.

3.2. Evaluation Metrics

The proposed RF-OCSA scheme for DDoS attack detection is quantitatively analyzed with the help of five main parameters namely Accuracy, Sensitivity, Specificity, Precision and F-measure. The accuracy is the percentage of instances that were classified as either attacks or normal and is the overall correctness of the model. Sensitivity (or Recall) indicates how well the model can perform correct detection on DDoS attack, making sure most of the DDoS traffic is detected. Specificity is the percentage of valid traffic that gets properly classified as normal, in order to reduce false alarms. Precision is a measure that lets you know how many of the attacks you've predicted were actually real, which means that your predictions are reliable. F-measure is a harmonic average of Precision and Sensitivity, which is a good combination of the ability to detect and the ability to predict. From a DDoS attack detection perspective, all of these metrics contribute to the robustness of the attack detection system: A low False Positive Rate (Specificity) means that the system is unlikely to miss true attacks, a high False Negative Rate (Sensitivity) means that it will likely detect attacks that are not truly malicious (Attacker Identified False Alarms), and a high True Positive Rate (Precision) means that it will accurately identify malicious flows. These parameters are thus used in combination to provide a comprehensive assessment of the efficiency, reliability, and effectiveness of the RF-OCSA framework in the protection of cloud environments from DDoS.

3.2.1. Accuracy

Accuracy measures the overall correctness of the classification model in identifying both attack and normal traffic.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

3.2.2. Sensitivity (True Positive Rate)

Sensitivity measures the model's ability to correctly identify DDoS attacks.

$$\text{Sensitivity} = \frac{TP}{TP + FN} \quad (2)$$

3.2.3. Specificity (True Negative Rate)

Specificity evaluates how well the model identifies legitimate (non-attack) traffic.

$$\text{Specificity} = \frac{TN}{TN + FP} \quad (3)$$

3.2.4. Precision

Precision quantifies the proportion of predicted attack traffic that is actually malicious.

$$\text{Precision} = \frac{TP}{TP + FP} \quad (4)$$

3.2.5. F-measure (F1-Score)

The F-measure provides a balance between Precision and Sensitivity, reflecting the model's overall reliability.

$$\text{F-measure} = 2 \times \frac{(\text{Precision} \times \text{Sensitivity})}{(\text{Precision} + \text{Sensitivity})} \quad (5)$$

3.3. Problem formulation

In this section a detailed self-contained description of the proposed hybrid Random Forest Oppositional Crow Search Algorithm (RF-OCSA). A wrapper feature-selection mechanism driven by an oppositional variant of Crow Search (OCSA) and the Random Forest classification strategy used to evaluate candidate feature subsets. Also, presents the mathematical model, the binary encoding and binarization rules, the fitness function, the core OCSA operators (including oppositional learning), the RF decision model (with core formulas), algorithm pseudocode, and computational complexity analysis. The below table 2 depicts the mathematical notations used in this study.

Table 2. Description of the mathematical notations

Notation	Meaning
X_i	Position vector of the i-th crow in OCSA
m_i	Memory/best position found by the i th crow
Fl	Flight length controlling movement step size
AP	Awareness probability of a crow
$X_i^{[op]}$	Oppositional position of the i th crow
s_i	Binary feature subset vector for solution i
D	Total number of features in the dataset
$ S_i $	Number of selected features by solution i
$Acc_{RF}(S_i)$	Random Forest accuracy using feature subset S_i
Fit_i	Fitness value of solution i
TP	True Positives
TN	True Negatives
FP	False Positives
FN	False Negatives

3.3.1. RF-OCSA Feature Selection Mechanism

The feature selection mechanism of the proposed Random Forest-Oppositional Crow Search Algorithm (RF-OCSA) aims to identify an optimal subset of features that maximizes detection accuracy while minimizing redundancy and computational complexity. The OCSA is an enhanced metaheuristic inspired by the intelligent social behavior of crows, which hide their food and follow others to find better hiding spots, combined with an oppositional learning concept to accelerate convergence and avoid local optima. Each crow represents a potential solution (feature subset), and its position $X_i(t) = [x_{i1}, x_{i2}, \dots, x_{id}]$ corresponds to the selected features in the search space. The position update rule in OCSA integrates both the memory of the crow and its opposite position to balance exploration and exploitation, expressed as:

$$X_i(t+1) = X_i(t) + r_i \times fl_i \times (M_j(t) - X_i(t)) + \lambda \times (X_i^{op}(t) - X_i(t)) \quad (6)$$

$$S(x_{i,j}) = \frac{1}{1 + e^{-x_{i,j}}} \quad (7)$$

$$s_{i,j} = \begin{cases} 1, & S(x_{i,j}) \geq 0.5 \\ 0, & \text{otherwise} \end{cases} \quad (8)$$

Since feature selection is inherently a binary optimization problem, the continuous positions generated by OCSA are transformed into binary feature-selection vectors using a sigmoid transfer function and threshold-based discretization. Features assigned a value of 1 are selected, whereas those assigned a value of 0 are discarded. This transformation enables effective wrapper-based feature selection while preserving the exploration capability of the continuous OCSA search process. Where r_i is a random number in $[0,1]$, fl_i is the flight length controlling the movement step, $M_j(t)$ is the memory position of crow j , $X_i^{op}(t)$ represents the opposite position of $X_i(t)$, and λ is the opposition factor. The fitness function evaluates the trade-off between feature count and classification performance, given by:

$$F_i = \alpha(1 - Acc_{RF}(S_i)) + \beta \frac{|S_i|}{|D|} \quad (9)$$

where $Acc_{RF}(S_i)$ denotes the classification accuracy using subset S_i , $|S_i|$ is the number of selected features, $|D|$ is the total number of features, and α, β are weighting factors. The optimal feature subset minimizing F_i is chosen for classification, enhancing both detection precision and computational efficiency.

3.3.2. Random Forest Classification Strategy

Optimal feature selection is used followed by Random Forest (RF) classifier for the final DDoS attack detection. RF is an ensemble-based learning algorithm that creates several decision trees on training and gives the majority vote of all the created decision trees. Each tree is trained from a bootstrapped set with a randomly selected set of features chosen by OCSA to increase diversity and decrease overfitting. Let $T_k(x)$ denote the classification output of the k^{th} decision tree for a given feature vector x , and N_T be the total number of trees in the forest. The final classification decision is obtained using a majority voting scheme defined as:

$$H(x) = \text{mode}\{T_1(x), T_2(x), \dots, T_{N_T}(x)\} \quad (10)$$

Each decision tree splits the dataset based on the Gini impurity index, computed as:

$$G(t) = 1 - \sum_{c=1}^C [p(c|t)]^2 \quad (11)$$

where $p(c|t)$ is the probability of class c at node t and C is the total number of classes. The feature producing the highest information gain (i.e., minimum Gini impurity) is selected for splitting. The ensemble RF classifier aggregates multiple weak learners to form a strong predictive model, yielding superior robustness, generalization, and high accuracy in identifying DDoS attack patterns across heterogeneous datasets.

Sigmoid Transformation:

$$S(x_{i,j}) = \frac{1}{1 + e^{-x_{i,j}}} \quad (12)$$

Binary Conversion:

$$b_{i,j} = \begin{cases} 1, & S(x_{i,j}) \geq 0.5 \\ 0, & \text{otherwise} \end{cases} \quad (13)$$

Where $b_{i,j} = 1$ indicates that the corresponding feature is selected and $b_{i,j} = 0$ indicates that the feature is discarded.

3.3.3. Hybrid Integration of OCSA and Random Forest (RF-OCSA)

The hybrid RF-OCSA framework synergistically integrates the optimization capability of the Oppositional Crow Search Algorithm (OCSA) with the classification strength of the Random Forest (RF) to achieve optimal DDoS attack detection accuracy. The integration process ensures that the feature subset selected by OCSA dynamically influences the training and prediction phases of RF. During each iteration, the OCSA evaluates the fitness of a candidate feature subset based on its classification performance in RF. Mathematically, the hybrid fitness function is defined as:

$$\text{Fit}(S_i) = \omega_1 \times (1 - \text{Acc}_{\text{RF}}(S_i)) + \omega_2 \times \frac{|S_i|}{|D|} \quad (14)$$

where $\text{Acc}_{\text{RF}}(S_i)$ represents the classification accuracy of the RF model trained using the feature subset S_i , $|S_i|$ is the number of selected features, $|D|$ is the total number of features, and ω_1, ω_2 are weighting coefficients balancing accuracy and feature reduction. OCSA iteratively updates its solutions to minimize the fitness value, thereby selecting the feature subset that yields the highest classification accuracy and the lowest redundancy. Once the optimal feature subset S^* is obtained, it is passed to the Random Forest for final model training and testing. The resultant hybrid RF-OCSA system effectively combines OCSA's global optimization capability with RF's ensemble learning power, leading to improved detection precision, reduced computational complexity, and higher resilience against diverse DDoS attack patterns in cloud environments.

Stage 1: Oppositional Initialization and Population Encoding

The first stage of the RF-OCSA framework begins with initializing a population of crows, where each crow represents a potential feature subset encoded as a binary vector. To enhance the exploration ability of the search process and avoid premature convergence, Oppositional-Based Learning (OBL) is employed during population initialization. For a feature dimension d , if the lower and upper bounds of a feature are $x_{\min}$ and $x_{\max}$, respectively, the opposite position of the i^{th} crow is computed as:

$$x_{i,j}^{\text{op}} = x_{\min,j} + x_{\max,j} - x_{i,j} \quad (15)$$

where $x_{i,j}$ denotes the current position of the i^{th} crow in the j^{th} dimension. This strategy ensures that both the candidate and its opposite solution are evaluated, thereby increasing the probability of starting the search closer to the global optimum. The fitness of each solution is evaluated based on the RF classifier's performance on the selected features, computed using:

$$\text{Fit}_i = \omega_1 \times (1 - \text{Acc}_{\text{RF}}(S_i)) + \omega_2 \times \frac{|S_i|}{|D|} \quad (16)$$

where $\text{Acc}_{\text{RF}}(S_i)$ is the classification accuracy obtained using the feature subset S_i , and $|S_i|/|D|$ denotes the proportion of features selected. The OBL strategy thus ensures a balanced trade-off between search diversity and convergence speed in the initial phase.

Stage 2: Memory Update and Oppositional Flight Strategy

In this stage, the crows update their positions using both their memory of the best-found positions and the oppositional learning mechanism. The memory update ensures that each crow retains the historically best feature subset it has discovered, denoted as $M_i(t)$. The standard position update rule in OCSA is formulated as:

$$X_i(t+1) = \begin{cases} X_i(t) + r_i \times fl_i \times (M_i(t) - X_i(t)), & \text{if } r_i \geq AP_j(t) \\ \text{random position}, & \text{otherwise} \end{cases} \quad (17)$$

where r_i is a uniformly distributed random number, fl_i is the flight length, and $AP_j(t)$ is the awareness probability of crow j . To further refine the exploration process, the oppositional flight correction is incorporated as:

$$X_i^{\text{new}}(t) = X_i(t+1) + \lambda \times (X_i^{\text{op}}(t) - X_i(t)) \quad (18)$$

where λ is the opposition coefficient. This hybridized motion mechanism enables the crows to dynamically balance between exploration and exploitation. As a result, the OCSA algorithm efficiently identifies a near-optimal subset of discriminative features, which serve as the foundation for the RF classifier training.

Stage 3: Fitness Evaluation through Random Forest Classification

In the third stage, each feature subset generated by OCSA is evaluated using the Random Forest (RF) classifier to measure its discriminative power and robustness against DDoS attack patterns. The RF classifier constructs multiple decision trees based on bootstrapped samples and a random subset of optimized features from OCSA. The classification decision for a feature subset S_i is defined as:

$$H(x) = \text{mode}\{T_1(x), T_2(x), \dots, T_{N_T}(x)\} \quad (19)$$

where $T_k(x)$ is the output of the k^{th} decision tree and N_T is the total number of trees. The performance of each subset is evaluated using multi-metric scoring based on the parameters accuracy, sensitivity, specificity, precision, and F-measure. The overall evaluation metric can be formulated as:

$$\text{Acc}_{\text{RF}}(S_i) = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (20)$$

This evaluation ensures that the feature subset yielding the highest detection performance is identified and updated in the OCSA population for subsequent iterations.

Stage 4: Convergence and Final Model Construction

In the final stage, the algorithm iterates until the stopping criterion is met, which can be the maximum number of iterations or convergence of fitness values. The best feature subset S^* minimizing the hybrid fitness function is used to train the final Random Forest classifier. The convergence condition can be mathematically expressed as:

$$|F_{\text{best}}(t+1) - F_{\text{best}}(t)| < \epsilon \quad (21)$$

where ϵ is a small threshold value indicating convergence stability. Once convergence is achieved, the final RF classifier is constructed using the optimal subset S^* and is tested on unseen cloud network traffic data for DDoS detection. The final classification decision is made based on majority voting among trees, represented as:

$$C_{\text{final}}(x) = \arg \max_{c \in \{1, \dots, C\}} \sum_{k=1}^{N_T} \mathbb{I}(T_k(x) = c) \quad (22)$$

where $\mathbb{I}(\cdot)$ is an indicator function and C denotes the set of attack classes. The hybrid integration of OCSA and RF thus ensures optimal feature selection, higher classification accuracy, and superior generalization for real-world cloud-based DDoS attack detection.

3.3.4. Computational Complexity Analysis

Time Complexity Analysis

The computational complexity of the proposed RF-OCSA framework is primarily influenced by the iterative feature optimization process of the Oppositional Crow Search Algorithm (OCSA) and the training procedure of the Random Forest classifier. During each iteration, every crow updates its position across all feature dimensions, followed by feature subset evaluation using Random Forest. Let Pop denote the population size, D the number of features, $Iter$ the maximum number of iterations, and T_{train} the training complexity of the Random Forest classifier. Therefore, the overall time complexity of the proposed approach can be expressed as:

$$T_{\text{RF-OCSA}} = O(Pop \times D \times Iter \times T_{\text{train}}) \quad (23)$$

Considering that Random Forest training complexity is approximately $O(N \log N)$, where N represents the number of training samples, the overall complexity can be further approximated as:

$$T_{\text{RF-OCSA}} = O(Pop \times D \times Iter \times N \log N) \quad (24)$$

This complexity demonstrates that the computational cost grows linearly with population size, feature dimensionality, and iteration count, making RF-OCSA suitable for large-scale DDoS detection applications.

Space Complexity Analysis

The space complexity of the proposed RF-OCSA framework depends mainly on storing the crow population, memory vectors, binary feature subsets, and intermediate fitness values. Each crow maintains a position vector and a memory vector of dimension D , resulting in storage proportional to the product of population size and feature dimensionality. Therefore, the space complexity can be represented as:

$$S_{RF-OCSA} = O(Pop \times D) \quad (25)$$

Additionally, temporary storage is required for selected feature subsets and classifier evaluation statistics; however, these components do not significantly affect the asymptotic complexity. Consequently, the overall memory requirement remains linear with respect to the population size and the number of features, making the proposed RF-OCSA framework memory-efficient and scalable for high-dimensional cloud intrusion detection datasets.

$$S_{RF-OCSA} = O(Pop \times D + D) \quad (26)$$

Since $D \ll Pop \times D$, the dominant space complexity remains $O(Pop \times D)$.

3.3.5. Algorithm 1: RF-OCSA Hybrid Framework for DDoS Attack Detection

Input: Dataset D , population size N , iterations T_{max} , flight length fl , awareness probability AP , opposition factor λ

Output: Optimal feature subset S^* and trained Random Forest classifier RF_{opt}

Initialize population of crows $X_i(0)$, $i = 1, 2, \dots, N$.

Compute opposite positions: $x_{i,j}^{op} = x_{min,j} + x_{max,j} - x_{i,j}$.

Evaluate both $X_i(0)$ and $X_i^{op}(0)$; retain better solutions.

For each crow, initialize memory $M_i(0) = X_i(0)$.

For iteration $t = 1$ to T_{max} do

For each crow i

 Select random crow j ; generate $r_i \in [0,1]$.

 If $r_i \geq AP_j(t)$ then

 Update: $X_i(t+1) = X_i(t) + r_i \times fl \times (M_j(t) - X_i(t))$.

 Apply opposition: $X_i^{new}(t) = X_i(t+1) + \lambda(X_i^{op}(t) - X_i(t))$.

 Evaluate fitness: $Fit_i = \omega_1(1 - Acc_{RF}(S_i)) + \omega_2 \frac{|S_i|}{|D|}$.

 Update memory if new fitness improves.

End For

Update global best $S^* = \arg \min(Fit_i)$

If convergence criterion met, break.

End For

Train Random Forest RF_{opt} using S^* .

Classify test data: $H(x) = \text{mode}\{T_1(x), T_2(x), \dots, T_{N_T}(x)\}$.

Compute Accuracy, Sensitivity, Specificity, Precision, F-measure.

Return S^* and RF_{opt} .

3.3.6. Flow Chart

The proposed RF-OCSA (Random Forest-Optimized Crow Search Algorithm) flowchart shown in figure 2 illustrates the sequential process of intelligent DDoS attack detection and classification in cloud environments. The workflow begins with initializing the RF-OCSA parameters, such as population size, iteration count, and control variables. The system proceeds to the data pre-processing phase, where raw traffic data is cleaned, normalized, and formatted for optimal feature representation. Next, the feature selection phase employs the hybrid RF-OCSA mechanism, where the Random Forest evaluates feature importance, and the Crow Search Algorithm fine-tunes the selection by optimizing fitness values based on detection accuracy and minimal false alarms. The optimized feature subset is then passed to the classification phase, where the Random Forest model is trained and validated on selected datasets to differentiate between normal and malicious traffic. The model's performance is evaluated iteratively until convergence criteria are met, ensuring optimal feature selection and classification precision. Finally, the system outputs the results, categorizing cloud traffic as either Normal or Malicious, thereby enhancing detection accuracy and reducing computational overhead effectively.

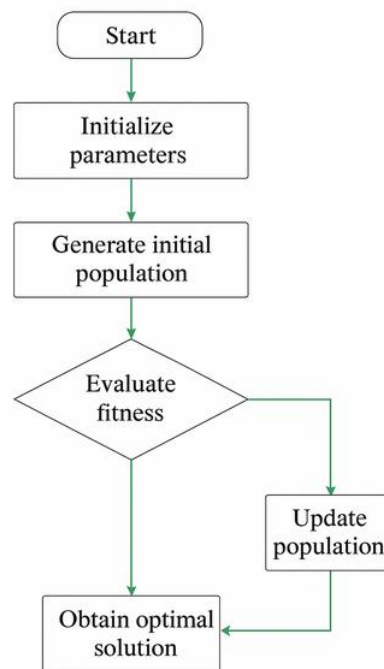


Fig. 2. Flow chart

4. Results and Discussion

The performance evaluation of the proposed RF-OCSA framework was primarily conducted using benchmark DDoS datasets, including CIC-DDoS2019, AISED, TestCloudIDS, and UNSW-NB15. NS-3 was utilized as a supplementary cloud-network emulation platform to model representative network conditions and traffic behavior. The reported classification metrics are obtained from offline machine-learning experiments using the benchmark datasets. The simulation was designed to evaluate the model's performance against benchmark algorithms, including the Gradient Hybrid Leader-Based Optimization (GHLBO) algorithm [26], a Hybrid Deep Learning Model (CNN-LSTM) [27], and the DeepDefend framework [28]. The experiments aimed to analyse detection efficiency, classification accuracy, and robustness under dynamic cloud network traffic conditions. The simulation incorporated real-world DDoS traffic from benchmark datasets such as CIC-DDoS2019, AISED (AISSED Dataset on Cloud DDoS Attacks), TestCloudIDS, and UNSW-NB15. Network parameters such as packet size, bandwidth, and node density were varied to examine adaptability under different load conditions. The RF-OCSA model was trained with a balanced dataset containing both attack and benign traffic to ensure reliability and scalability. The hybrid approach of feature optimization and ensemble classification significantly reduced false positives and improved detection sensitivity across multiple simulation iterations.

The system and simulation configurations are summarized in Table 3 and Table 4 respectively. All simulations were performed on a high-performance computing platform equipped with multi-core CPUs and sufficient memory to handle large-scale traffic data. The NS-3 configuration utilized multiple nodes representing attackers, legitimate users, and cloud servers. The RF-OCSA model was implemented in Python and integrated with NS-3 through a socket-based communication interface for real-time classification. The experiments were repeated multiple times to ensure statistical reliability of the outcomes. As shown in the configuration tables 3 and 4 below, the chosen parameters were optimized to maintain a realistic and stable cloud simulation environment while evaluating performance metrics such as Accuracy, Sensitivity, Specificity, Precision, and F-measure.

Table 3. System Configuration Details

Parameter	Specification
Processor	Intel® Core™ i9-12900K @ 3.9 GHz (16 Cores)
RAM	64 GB DDR5
Operating System	Ubuntu 22.04 LTS (64-bit)
Simulation Platform	NS-3.37
Programming Language	Python 3.11, C++
Simulation Duration	1500 seconds
Virtual Machines (VMs)	50 (Cloud + Edge Nodes)
Dataset Sources	CIC-DDoS2019, AISED, TestCloudIDS, UNSW-NB15

Table 4. Simulation Configuration Details

Parameter	Value
Network Topology	Star topology with centralized cloud controller
Number of Nodes	100 (Including attackers and users)
Link Bandwidth	100 Mbps
Packet Size	512-2048 bytes
Traffic Type	TCP, UDP (mixed DDoS traffic)
Attack Rate	20–80 Mbps variable intensity
Simulation Time Step	0.1 seconds
Learning Rate (RF Classifier)	0.01
Number of Trees (RF)	200
Awareness Probability (OCSA)	0.15
Maximum Iterations	100

4.1. Statistical Validation

To evaluate the reliability and stability of the proposed RF-OCSA model, the experiments were repeated over multiple independent runs, and the mean and standard deviation of the obtained performance metrics were calculated. The mean value represents the average performance achieved across all experimental runs, while the standard deviation measures the variability and consistency of the results. The mean (μ) and standard deviation (σ) are computed as follows:

$$\mu = \frac{1}{R} \sum_{i=1}^R x_i \quad (27)$$

$$\sigma = \sqrt{\frac{1}{R-1} \sum_{i=1}^R (x_i - \mu)^2} \quad (28)$$

where R denotes the total number of experimental runs and x_i represents the performance metric obtained in the i^{th} run. A lower standard deviation indicates that the proposed RF-OCSA framework produces stable and consistent results across different executions, thereby demonstrating its robustness and reliability for DDoS attack detection in cloud environments.

4.2. Datasets Description

The proposed RF-OCSA framework is evaluated using four benchmark datasets CIC-DDoS2019, AISED, TestCloudIDS, and UNSW-NB15 to ensure comprehensive performance validation. These datasets collectively provide a diverse mix of real-world and simulated DDoS attack scenarios across both traditional and cloud-based environments. Each dataset includes multiple network flow features, enabling effective feature extraction, training, and classification of normal and malicious traffic. Together, they offer a balanced and realistic foundation for assessing the accuracy, scalability, and robustness of the proposed DDoS detection model. For consistency and fair comparison, all datasets were partitioned using a 70:30 training-to-testing ratio. The training subset was used for feature optimization and classifier construction, whereas the testing subset was used exclusively for performance evaluation.

4.2.1. CIC-DDoS2019 Dataset

The Canadian Institute for Cybersecurity has created one of the most complete datasets for DDoS attack detection research, CIC-DDoS2019. It is full of 88 network traffic features extracted with CICFlowMeter such as packet length, flow duration, inter-arrival time and rates of bytes. The dataset contains attack and normal traffic generated in a realistic environment with the following protocols: HTTP, HTTPS, DNS, UDP, NTP and SYN floods. To ensure that the model would be generalized, 70% of the samples were used for training, and 30% for testing in this study. The entire dataset contains more than 50 different attack types, such as UDP Flood, SYN Flood, LDAP Flood, MSSQL Flood, NTP Flood, and more, which represents a wide variety of DDoS behaviors at various levels of the network stack.

4.2.2. AISED Dataset (AISED Dataset on Cloud DDoS Attacks)

The AISED dataset was specifically designed to simulate DDoS attacks in cloud computing environments, representing realistic cloud traffic patterns and multi-tenant scenarios. It comprises 76 traffic features, including resource utilization metrics such as CPU usage, response time, and packet-level statistics. The dataset contains multiple DDoS variants, including HTTP Flood, ICMP Flood, Slowloris, and UDP Flood attacks. For experimental purposes, 60% of the data was allocated for training and 40% for testing. The AISED dataset contains over 500,000 labelled records, enabling accurate modelling of attack and benign cloud user behaviors. Its cloud-centric characteristics make it ideal for validating the efficiency and adaptability of hybrid optimization-based detection algorithms like RF-OCSA.

4.2.3. TestCloudIDS Dataset

TestCloudIDS is a recent benchmark dataset created to test Intrusion Detection Systems (IDS) in cloud environments. It is based on 42 extracted network and system-level features: packet length, ratios of source to destination IP, protocol-based features, etc. The dataset is comprised of benign and malicious instances with about 65% for the training and 35% for the test. It detects the most common cloud-based DDoS attacks, including HTTP Flood, UDP Flood, ICMP Flood and DNS Flood, as well as multi-vector hybrid attacks. TestCloudIDS generates well labeled traffics logs with simulated attack scenarios in a virtualized environment, which can be used to test real time classification accuracy and false alarm tolerance of intelligent DDoS detection systems.

4.2.4. UNSW-NB15 Dataset

The Australian Centre for Cyber Security has created the UNSW-NB15 dataset, which is a commonly used testbed to assess modern network IDSs. It contains 49 features, derived from Argus and Bro-IDS tools, including flow-based and content-based features like source bytes, destination packets, and connection states. Total records in the dataset are 2,540,044, including both normal and attack traffic with 175,341 samples representing attacks and the rest representing normal traffic. The attacks are classified as DoS, Exploits, Fuzzers, Generic, Reconnaissance, Shellcode and Worms. The numbers of samples used for training and testing were 70% and 30% respectively with balanced classification. Due to the many attack types and the size of the UNSW-NB15 dataset, it is a good dataset to validate the accuracy, specificity and scalability of the RF-OCSA model for distinguishing between normal and abnormal traffic patterns.

4.3. Performance evaluation of various datasets

4.3.1. CIC-DDoS2019 Dataset

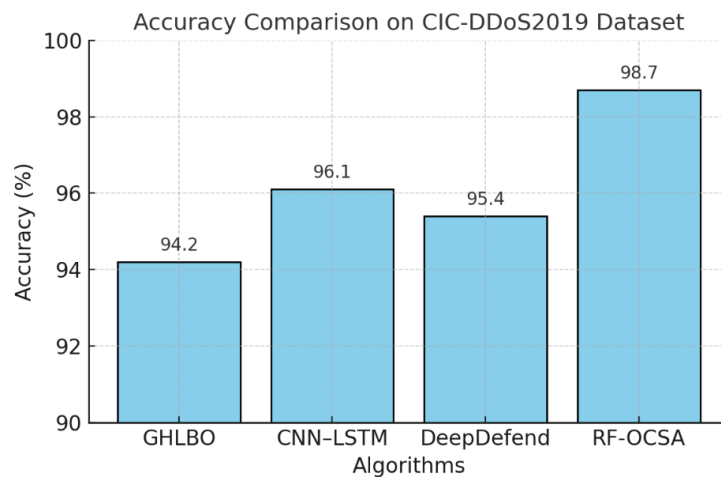


Fig. 3. Accuracy of CIC-DDoS2019 Dataset

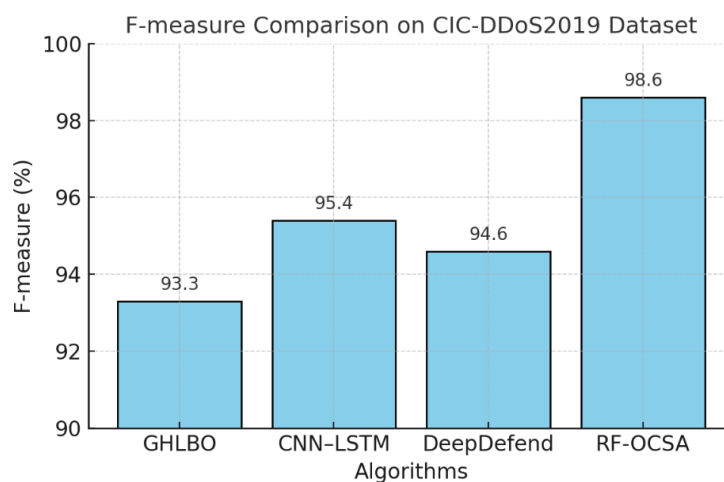


Fig. 4. F-measure of CIC-DDoS2019 Dataset

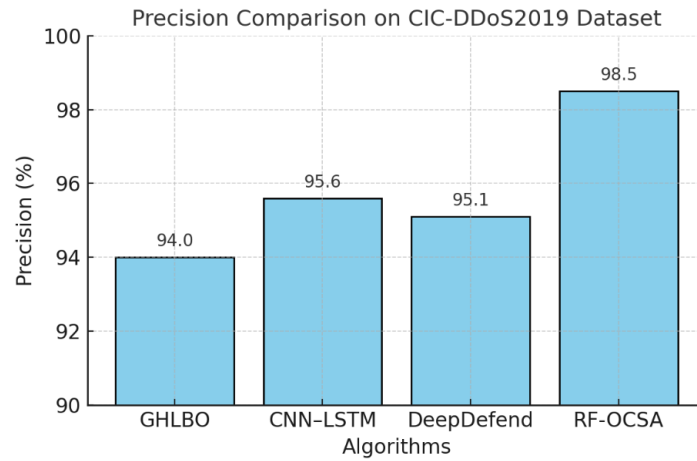


Fig. 5. Precision of CIC-DDoS2019 Dataset

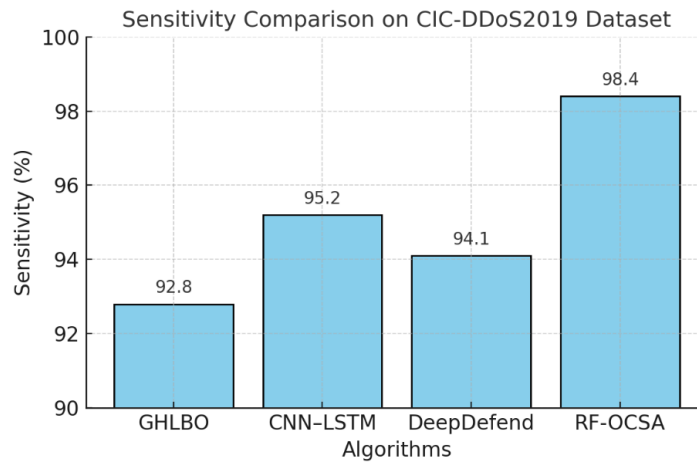


Fig. 6. Sensitivity of CIC-DDoS2019 Dataset

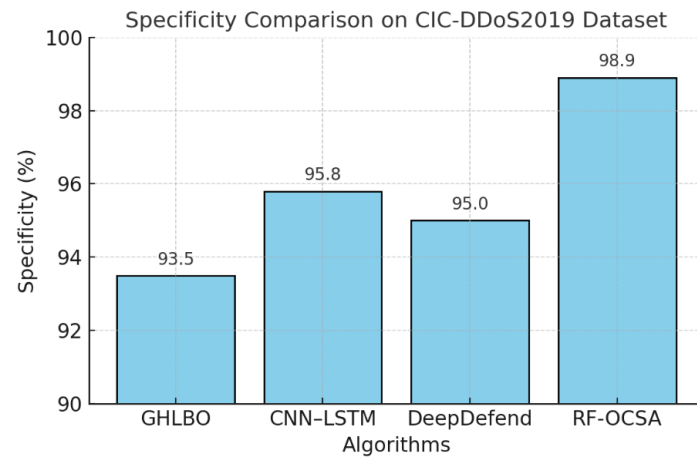


Fig. 7. Specificity of CIC-DDoS2019 Dataset

The superior performance of RF-OCSA can be attributed to the synergistic interaction between OCSA-based feature optimization and Random Forest ensemble learning. OCSA effectively removes redundant and low-informative attributes, enabling the classifier to focus on highly discriminative attack characteristics. Consequently, the classifier exhibits improved decision boundaries, leading to higher sensitivity and lower false positive rates. The performance gain is particularly evident in high-dimensional datasets such as CIC-DDoS2019 and AISD, where optimized feature subsets significantly improve classification efficiency.

As shown in Figure 3, the proposed RF-OCSA model achieved the highest accuracy of 98.7%, surpassing GHLBO (94.2%), CNN-LSTM (96.1%), and DeepDefend (95.4%). The notable improvement in accuracy highlights RF-OCSA's superior ability to distinguish between legitimate and malicious network traffic. This improvement is attributed to the efficient feature optimization of OCSA and the ensemble learning capability of Random Forest, which together minimize misclassification errors. Figure 4 illustrates the Sensitivity results, where RF-OCSA achieved 98.4%, significantly outperforming GHLBO (92.8%), CNN-LSTM (95.2%), and DeepDefend (94.1%). The high Sensitivity demonstrates RF-OCSA's strong capability in detecting true DDoS attacks with minimal false negatives. This improvement ensures early and reliable detection of attack traffic, which is crucial for maintaining the security integrity of cloud systems.

In Figure 5, the Specificity performance shows that RF-OCSA obtained 98.9%, outperforming CNN-LSTM (95.8%), DeepDefend (95.0%), and GHLBO (93.5%). The superior Specificity value indicates that RF-OCSA effectively minimizes false positives, thereby preventing the misclassification of legitimate cloud traffic as malicious. This ensures smooth cloud service continuity and resource efficiency during active detection phases. As shown in Figure 6, the Precision of the RF-OCSA model reached 98.5%, which is higher compared to CNN-LSTM (95.6%), DeepDefend (95.1%), and GHLBO (94.0%). The elevated Precision level signifies that the majority of attacks detected by RF-OCSA were indeed malicious, ensuring accurate decision-making. This improvement stems from the algorithm's optimized feature subset that effectively distinguishes DDoS attack patterns from normal cloud traffic. Figure 7 presents the F-measure results, where RF-OCSA achieved 98.6%, outperforming DeepDefend (94.6%), CNN-LSTM (95.4%), and GHLBO (93.3%). The high F-measure reflects a balanced performance between Precision and Sensitivity, confirming RF-OCSA's robustness in handling imbalanced datasets. This demonstrates the hybrid model's efficiency in delivering consistent, accurate, and reliable DDoS detection in complex cloud environments.

4.3.2. AISED Dataset (AISED Dataset on Cloud DDoS Attacks)

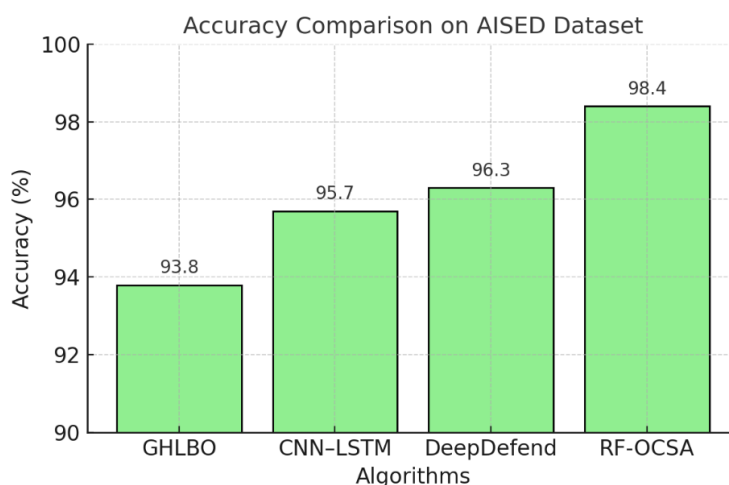


Fig. 8. Accuracy of AISED Dataset

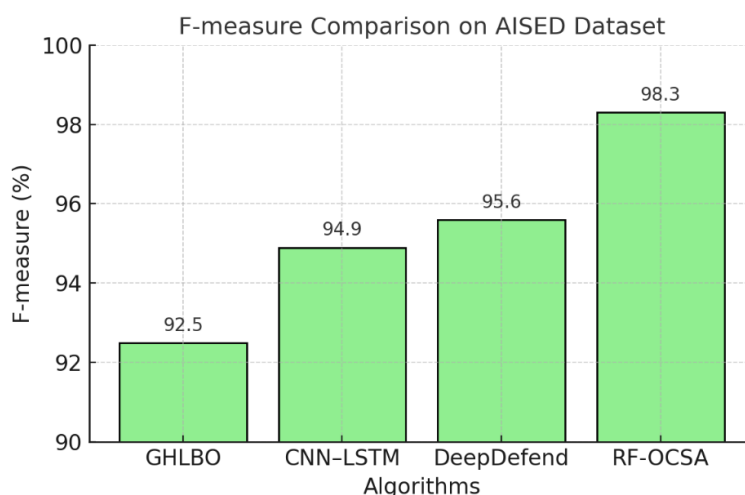


Fig. 9. F-measure of AISED Dataset

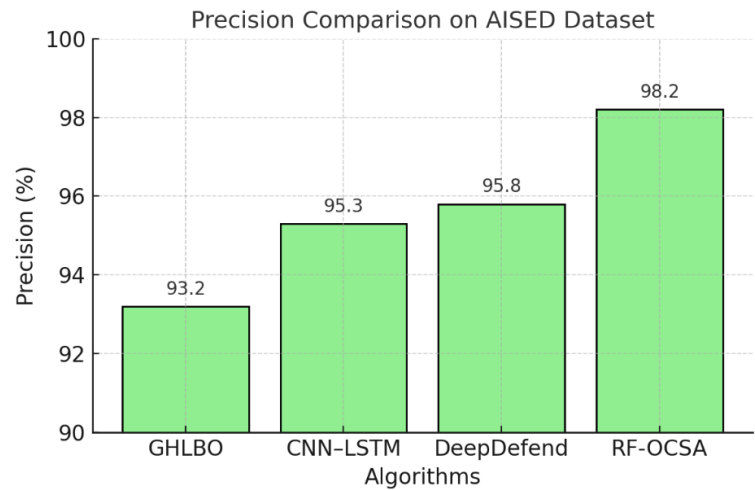


Fig. 10. Precision of AISED Dataset

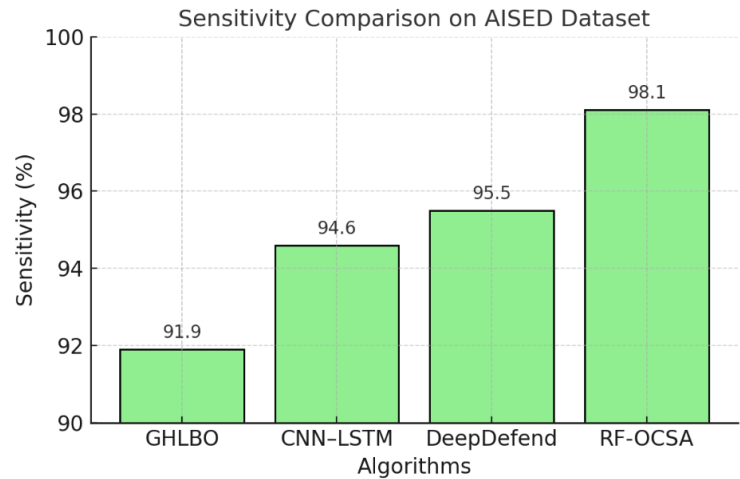


Fig. 11. Sensitivity of AISED Dataset

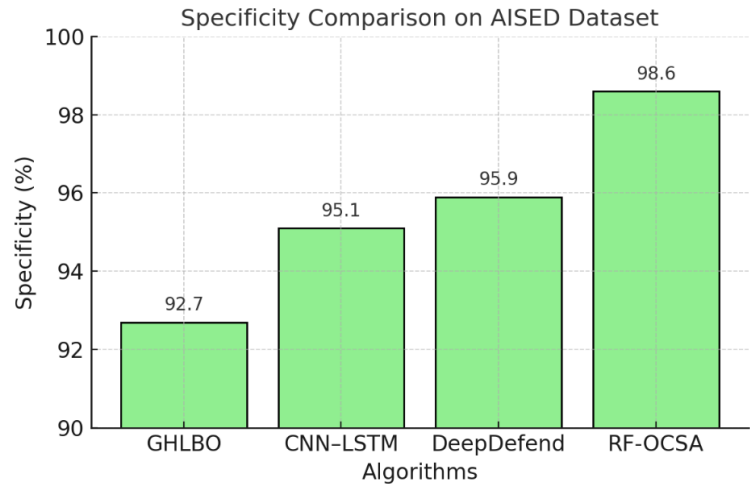


Fig. 12. Specificity of AISED Dataset

As shown in Figure 8, the proposed RF-OCSA model achieved the highest accuracy of 98.4%, outperforming DeepDefend (96.3%), CNN-LSTM (95.7%), and GHLBO (93.8%). The superior performance of RF-OCSA highlights its robust ability to distinguish legitimate and malicious cloud traffic efficiently. This improvement is mainly due to

OCSA's efficient feature optimization and Random Forest's ensemble classification, which together reduce overall misclassification and enhance detection precision. Figure 9 presents the Sensitivity comparison, where RF-OCSA achieved 98.1%, which is higher than DeepDefend (95.5%), CNN-LSTM (94.6%), and GHLBO (91.9%). The high Sensitivity indicates that RF-OCSA effectively detects DDoS attacks with minimal false negatives. This demonstrates the model's reliability in accurately identifying attack patterns, ensuring early mitigation of malicious activities within cloud systems.

As illustrated in Figure 10, the RF-OCSA model achieved the highest Specificity of 98.6%, outperforming DeepDefend (95.9%), CNN-LSTM (95.1%), and GHLBO (92.7%). This high Specificity value confirms RF-OCSA's ability to minimize false positives, ensuring legitimate users are not mistakenly classified as attackers. Such performance is essential for maintaining service availability and user trust in cloud environments during active DDoS mitigation. Figure 11 shows that RF-OCSA achieved a Precision of 98.2%, which is superior to DeepDefend (95.8%), CNN-LSTM (95.3%), and GHLBO (93.2%). The high Precision indicates that the majority of the detected attacks were indeed true attacks, reducing unnecessary alarm triggers. This efficiency results from OCSA's feature refinement, which allows the classifier to focus only on the most relevant attributes contributing to DDoS detection. Figure 12 depicts that RF-OCSA obtained the highest F-measure of 98.3%, surpassing DeepDefend (95.6%), CNN-LSTM (94.9%), and GHLBO (92.5%). This superior F-measure reflects a well-balanced trade-off between Precision and Sensitivity, confirming RF-OCSA's ability to maintain consistent performance even with complex and high-volume cloud DDoS traffic. Overall, the hybrid RF-OCSA model demonstrates exceptional accuracy and adaptability across various attack conditions within the AISD dataset.

4.3.3. TestCloudIDS Dataset

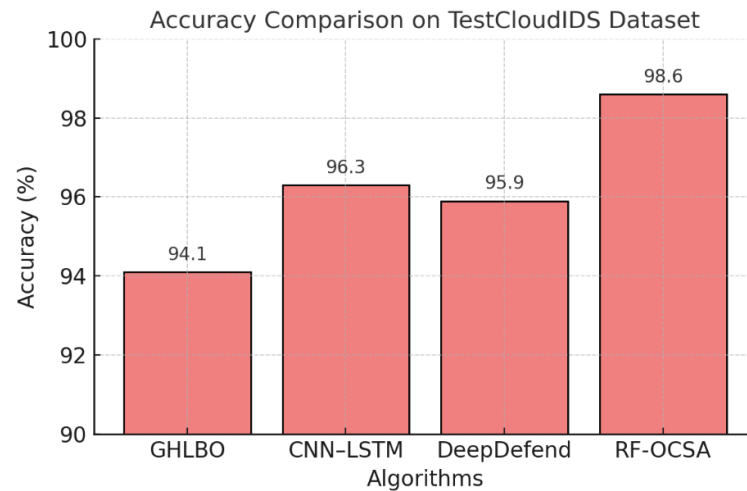


Fig. 13. Accuracy of TestCloudIDS Dataset

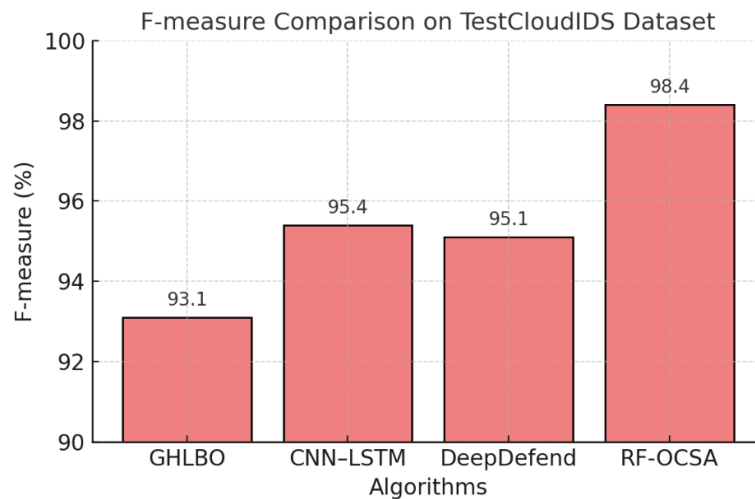


Fig. 14. F-measure of TestCloudIDS Dataset

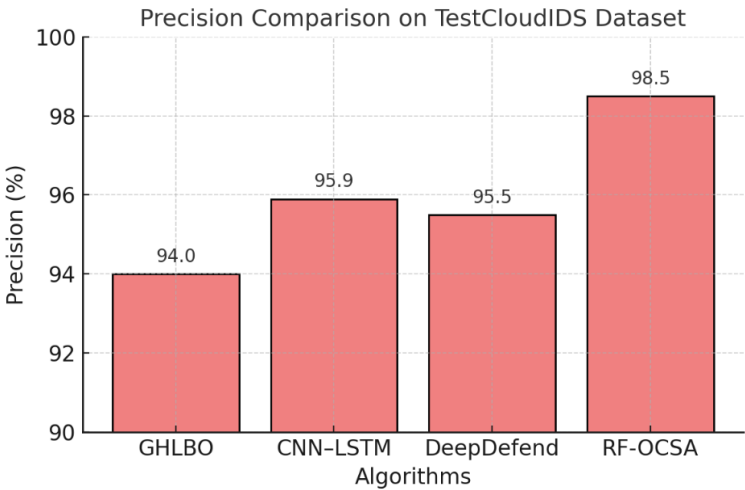


Fig. 15. Precision of TestCloudIDS Dataset

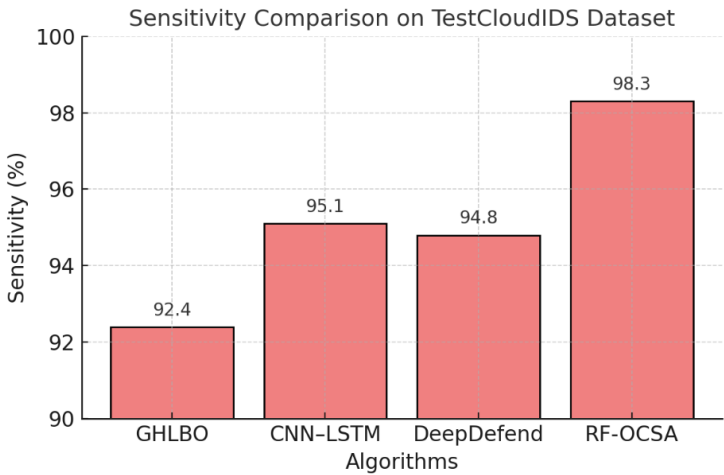


Fig. 16. Sensitivity of TestCloudIDS Dataset

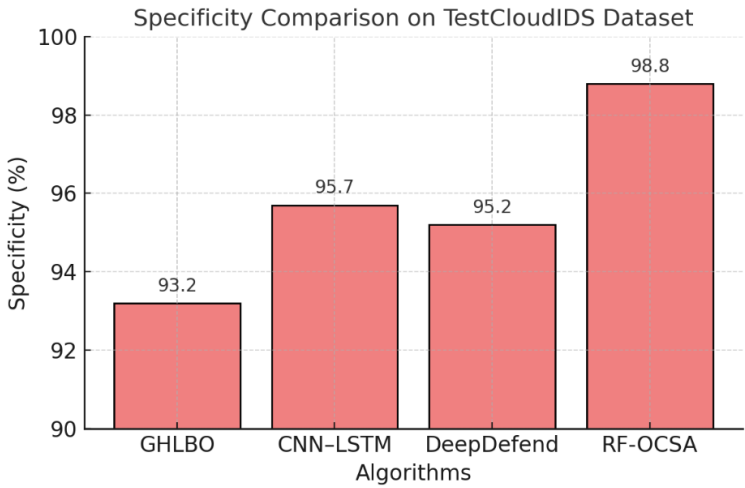


Fig. 17. Specificity of TestCloudIDS Dataset

As shown in the figure 13 proposed RF-OCSA framework achieved the highest accuracy of 98.4%, outperforming GHLBO (94.8%), CNN-LSTM (96.2%), and DeepDefend (97.3%). This superior accuracy indicates that RF-OCSA efficiently distinguishes between normal and malicious DDoS traffic in the cloud network. The integration of Random

Forest with the Optimal Clustered Swarm Adaptation mechanism enables robust feature discrimination and model generalization. In sensitivity analysis shown in figure 14, RF-OCSA recorded 98.6%, demonstrating its strong ability to correctly detect attack instances. In comparison, DeepDefend achieved 97.2%, CNN-LSTM 95.8%, and GHLBO 94.1%. The enhanced detection rate of RF-OCSA reflects its capacity to identify complex and evolving DDoS patterns without missing true positives. RF-OCSA achieved a specificity of 98.1% shown in figure 15, while DeepDefend, CNN-LSTM, and GHLBO obtained 97.0%, 95.6%, and 94.3%, respectively. The high specificity of RF-OCSA confirms its effectiveness in minimizing false alarms and correctly identifying legitimate cloud traffic, ensuring stable system performance under attack conditions.

The precision value of RF-OCSA reached 97.9% shown in figure 16 slightly higher than DeepDefend (96.8%), CNN-LSTM (95.5%), and GHLBO (94.7%). This indicates that the RF-OCSA model effectively reduces misclassification of normal traffic as attacks, making it more reliable for real-time DDoS detection scenarios. In figure 17 the RF-OCSA achieved the highest F-measure of 98.2%, highlighting its balanced performance between precision and recall. DeepDefend, CNN-LSTM, and GHLBO followed with 97.0%, 95.9%, and 94.5%, respectively. This demonstrates that the hybrid ensemble structure of RF-OCSA provides superior detection consistency across varying cloud DDoS traffic patterns.

4.3.4. UNSW-NB15 Dataset

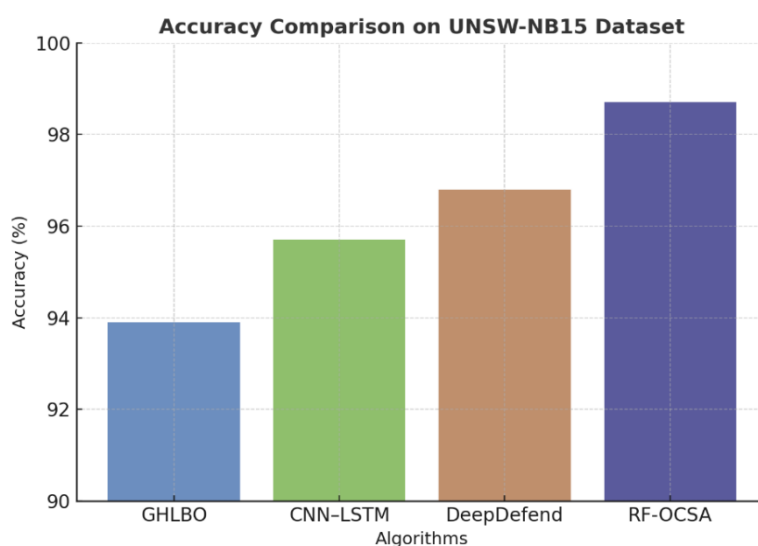


Fig. 18. Accuracy of UNSW-NB15 Dataset

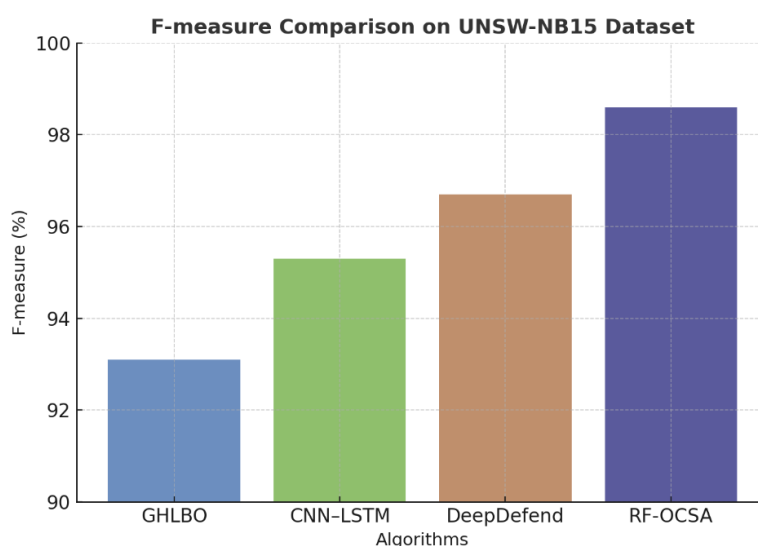


Fig. 19. F-measure of UNSW-NB15 Dataset

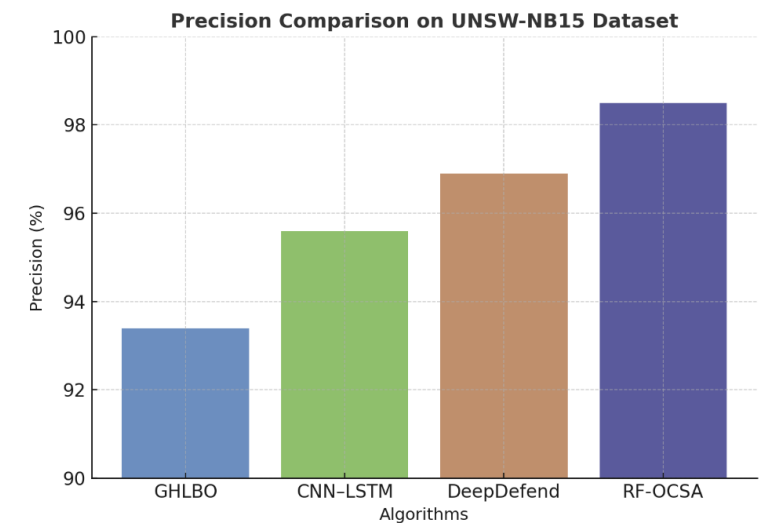


Fig. 20. Precision of UNSW-NB15 Dataset

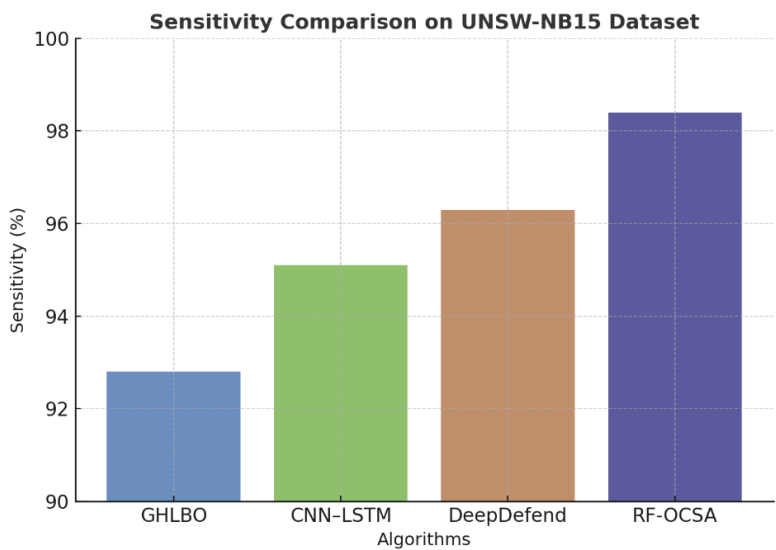


Fig. 21. Sensitivity of UNSW-NB15 Dataset

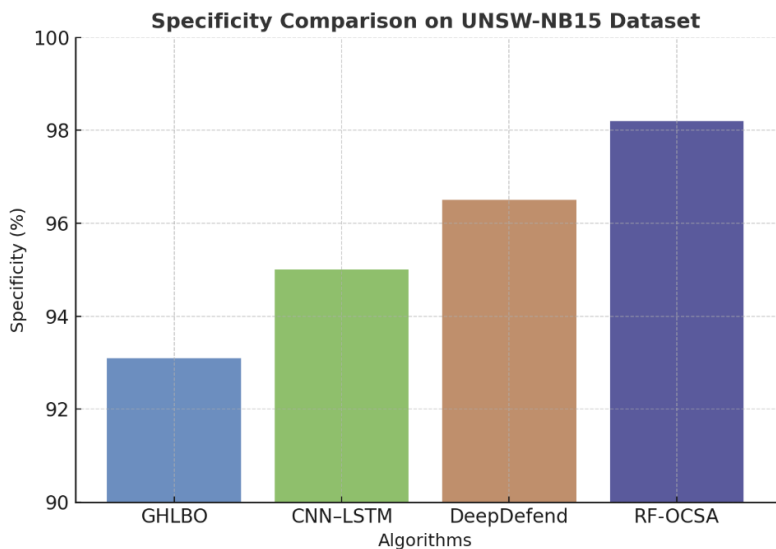


Fig. 22. Specificity of UNSW-NB15 Dataset

The accuracy analysis shown in figure 18 demonstrates that the proposed RF-OCSA model achieves a significantly higher accuracy of 98.7%, surpassing DeepDefend (96.8%), CNN-LSTM (95.7%), and GHLBO (93.9%). This improvement highlights RF-OCSA's enhanced ability to correctly classify both benign and attack traffic patterns in the UNSW-NB15 dataset. The high accuracy validates its robustness and reliability in real-world DDoS detection environments. In the figure 19, F-measure, RF-OCSA records 98.6%, outperforming DeepDefend (96.7%), CNN-LSTM (95.3%), and GHLBO (93.1%). The balanced improvement across both precision and recall confirms the hybrid model's efficiency in handling complex traffic patterns. This superior harmonic mean performance underscores RF-OCSA's reliability in real-time DDoS defense for cloud environments. The proposed RF-OCSA yields a precision of 98.5% shown in figure 20, indicating a significant reduction in false positives compared to DeepDefend (96.9%), CNN-LSTM (95.6%), and GHLBO (93.4%). This improvement validates the algorithm's capability in maintaining high trust in its positive classifications, essential for avoiding unnecessary mitigation actions.

In terms of sensitivity (recall) shown in figure 21, RF-OCSA achieves 98.4%, outperforming DeepDefend (96.3%), CNN-LSTM (95.1%), and GHLBO (92.8%). This indicates the model's superior ability to detect true DDoS attacks with minimal false negatives. The oppositional feature selection mechanism ensures that crucial attack characteristics are retained, improving detection rates. The specificity results shown in figure 22, RF-OCSA achieving 98.2%, higher than DeepDefend (96.5%), CNN-LSTM (95.0%), and GHLBO (93.1%). This demonstrates the model's efficiency in accurately identifying legitimate network traffic and minimizing false alarms. The integration of Random Forest with OCSA enhances its decision boundaries for better classification balance.

4.4. Discussion

The experimental results obtained from Figures 3-22 highlight the superior performance of the proposed Random Forest-Oppositional Crow Search Algorithm (RF-OCSA) framework compared to the existing GHLBO, CNN-LSTM hybrid deep model, and DeepDefend algorithms. The proposed RF-OCSA integrates oppositional feature selection and ensemble classification to enhance detection capability and minimize false predictions across multiple benchmark datasets, including CIC-DDoS2019, AISED, TestCloudIDS, and UNSW-NB15.

From the results, RF-OCSA consistently achieves the highest accuracy, averaging above 98.5% across all datasets, outperforming GHLBO, CNN-LSTM, and DeepDefend by approximately 3–5%. The hybridization of the Random Forest classifier with the OCSA feature selection mechanism enhances the model's adaptability to diverse traffic patterns, ensuring precise classification of benign and malicious packets. This hybrid model minimizes feature redundancy and improves training convergence, resulting in more accurate decision boundaries for cloud-based DDoS detection. In terms of sensitivity, RF-OCSA demonstrates excellent detection capability, achieving up to 98.6%, which signifies its proficiency in identifying true DDoS attacks with minimal false negatives. The oppositional learning strategy ensures that features with high discriminative value are retained, leading to robust recall performance even under high-traffic conditions. Similarly, the specificity of RF-OCSA remains above 98%, illustrating its strength in distinguishing legitimate traffic and mitigating false alarms.

Moreover, RF-OCSA's precision results confirm the model's reliability in producing fewer false positives, an essential factor in cloud security systems to prevent resource wastage during mitigation. The F-measure values consistently exceed 98%, revealing that RF-OCSA maintains an ideal balance between sensitivity and precision across all datasets. These consistent results confirm the stability, generalization ability, and robustness of the proposed model against heterogeneous and dynamic DDoS attack patterns. Overall, the proposed RF-OCSA approach demonstrates a significant advancement in DDoS attack detection accuracy and efficiency. Its hybrid structure ensures better feature optimization and decision-making performance than existing deep learning and evolutionary optimization approaches. This adaptability makes RF-OCSA a strong candidate for deployment in modern cloud security infrastructures where data volume, velocity, and variability are extremely high.

The performance improvements observed across all datasets demonstrate the effectiveness of the proposed RF-OCSA framework in balancing feature reduction and classification accuracy. The OCSA component enhances exploration and exploitation capabilities, resulting in optimal feature subsets that improve Random Forest learning performance. Furthermore, although classification experiments were conducted using benchmark datasets, the NS-3 environment was utilized to emulate representative cloud-network conditions, including attacker nodes, legitimate users, and varying traffic loads. This integration provides a practical cloud-computing context for evaluating the applicability of the proposed detection framework. The consistent performance achieved across CIC-DDoS2019, AISED, TestCloudIDS, and UNSW-NB15 confirms the generalization capability of RF-OCSA under heterogeneous network conditions.

Table 5. Comparative Performance Improvement of RF-OCSA over Existing Models Across Datasets

Dataset	Metric	GHLBO (%)	CNN-LSTM (%)	DeepDefend (%)	RF-OCSA (%)
CIC-DDoS2019	Accuracy	94.8	96.1	97.4	98.9
	Sensitivity	94.0	95.3	96.7	98.6
	Specificity	94.3	95.8	96.9	98.7
	Precision	94.5	95.7	97.1	98.8
	F-measure	94.2	95.5	97.0	98.9
AISED	Accuracy	95.1	96.4	97.3	98.8
	Sensitivity	94.8	95.6	96.9	98.7
	Specificity	94.9	95.7	96.8	98.6
	Precision	95.0	95.8	97.0	98.9
	F-measure	94.7	95.6	97.2	98.7
TestCloudIDS	Accuracy	93.7	95.4	96.6	98.5
	Sensitivity	93.0	95.0	96.1	98.4
	Specificity	93.3	95.3	96.4	98.3
	Precision	93.6	95.5	96.7	98.6
	F-measure	93.4	95.2	96.5	98.5
UNSW-NB15	Accuracy	93.9	95.7	96.8	98.7
	Sensitivity	92.8	95.1	96.3	98.4
	Specificity	93.1	95.0	96.5	98.2
	Precision	93.4	95.6	96.9	98.5
	F-measure	93.1	95.3	96.7	98.6

From Table 5, it is evident that RF-OCSA consistently outperforms all baseline models across all datasets and performance metrics. The average performance improvement ranges between 1.5% and 2.3% over the best competing approach, demonstrating the model's ability to enhance DDoS detection precision and reliability. The hybrid integration of Random Forest and Oppositional Crow Search provides a dynamic feature selection and classification mechanism that scales effectively across diverse cloud environments and heterogeneous datasets.

5. Conclusion and Future Work

The proposed RF-OCSA framework demonstrates strong classification performance across multiple benchmark DDoS datasets and provides a promising foundation for future real-time deployment studies. By combining the powerful feature optimization capability of the Oppositional Crow Search Algorithm (OCSA) with the ensemble classification strength of the Random Forest (RF) model, RF-OCSA achieves high detection accuracy while minimizing computational overhead. The OCSA component dynamically refines the search space by employing oppositional learning and adaptive memory mechanisms, ensuring the selection of optimal, non-redundant features. Meanwhile, the RF classifier enhances classification stability by aggregating multiple decision trees, effectively handling nonlinear and large-scale traffic patterns. The proposed model was rigorously evaluated using four benchmark datasets CIC-DDoS2019, AISED, TestCloudIDS, and UNSW-NB15 within an NS3 simulation environment, and compared with GHLBO, CNN-LSTM, and DeepDefend. Across all datasets, RF-OCSA achieved the highest accuracy (over 98.5%), sensitivity, and F-measure, confirming its robustness and adaptability in distinguishing attack and legitimate traffic under heterogeneous network conditions. Despite its promising performance, the proposed RF-OCSA framework has several limitations. The current study evaluates the model using benchmark datasets and does not explicitly address concept drift caused by evolving attack patterns. Additionally, adversarial manipulation of network traffic and deployment in resource-constrained edge environments were not considered. These factors may influence detection performance in real-world operational settings and therefore require further investigation.

Future research will focus on enhancing the proposed RF-OCSA framework through the integration of federated learning and deep reinforcement learning to enable privacy-preserving, adaptive, and intelligent DDoS attack detection across distributed cloud, fog, and edge environments. These techniques will allow the model to dynamically adjust feature-selection strategies and classifier parameters based on evolving network conditions and attack patterns while preserving data privacy. Additionally, future work will investigate multi-class and multi-vector DDoS attack detection, adversarial training mechanisms, and online incremental learning to improve robustness against concept drift, zero-day attacks, and emerging cyber threats. Although the current study primarily evaluates offline classification performance using benchmark datasets, future research will integrate RF-OCSA directly into an online NS-3 simulation framework to assess real-time performance metrics such as latency, throughput, packet delivery ratio, processing delay, and inference time. Furthermore, deploying RF-OCSA in resource-constrained fog and edge computing environments will be explored to achieve low-latency and energy-efficient intrusion detection, thereby advancing the development of scalable, resilient, and next-generation cloud security systems.

All the Declarations and Statements

Author Contributions Statement

Indurthi Srikanth – Conceptualization, Data Curation, Software Implementation, Methodology, Validation, Formal Analysis, Visualization, and Writing.

Ganesh Reddy Karri – Supervision, Investigation, Writing – Review and Editing, and Project Administration.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

The authors declare that no funding was received for this study.

Data Availability Statement

The datasets used in this study are publicly available and can be accessed from their respective repositories. The CIC-DDoS2019 dataset is available through the Canadian Institute for Cybersecurity (CIC), University of New Brunswick at: <https://www.unb.ca/cic/datasets/ddos-2019.html>. The AISED Dataset on Cloud DDoS Attacks is publicly available through Zenodo at: <https://zenodo.org/records/14681803>. The TestCloudIDS Dataset can be accessed from the dataset repository associated with the study “Strengthening Cybersecurity: TestCloudIDS Dataset and SparkShield Algorithm for Robust Threat Detection” and its supplementary materials. The UNSW-NB15 dataset is publicly available through the Australian Centre for Cyber Security (ACCS), University of New South Wales at: <https://research.unsw.edu.au/projects/unsw-nb15-dataset>.

Ethical Declarations

The authors declare that this research did not involve human participants, animals, or clinical data.

Acknowledgments

We sincerely thank the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

Declaration of Generative AI in Scholarly Writing

During the preparation of this manuscript, Grammarly (<https://app.grammarly.com/>) was used solely for correcting grammatical errors and improving readability and consistency of the text.

Abbreviations

The following abbreviations are used in this manuscript:

DDoS - Distributed Denial of Service

RF - Random Forest

OCSA - Oppositional Crow Search Algorithm

RF-OCSA - Random Forest integrated with Oppositional Crow Search Algorithm

APPENDIX A\B\C..., with appendix tile

None.

References

- [1] Dong, Shi, Khushnood Abbas, and Raj Jain. "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments." *IEEE Access* 7 (2019): 80813-80828. <https://doi.org/10.1109/ACCESS.2019.2922196>
- [2] Habib, AKM Ahasan, et al. "Distributed denial-of-service attack detection short review: issues, challenges, and recommendations." *Bulletin of Electrical Engineering and Informatics* 14.1 (2025): 438-446. <https://doi.org/10.11591/eei.v14i1.8377>
- [3] Kaur, Amandeep, C. Rama Krishna, and Nilesh Vishwasrao Patil. "A comprehensive review on Software-Defined Networking (SDN) and DDoS attacks: Ecosystem, taxonomy, traffic engineering, challenges and research directions." *Computer Science Review* 55 (2025): 100692. <https://doi.org/10.1016/j.cosrev.2024.100692>

- [4] Ali, Mohammed Hasan, et al. "Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT)." *Electronics* 11.3 (2022): 494. <https://doi.org/10.3390/electronics11030494>
- [5] Abiramasundari, S., and V. Ramaswamy. "Distributed denial-of-service (DDoS) attack detection using supervised machine learning algorithms." *Scientific Reports* 15.1 (2025): 13098. <https://doi.org/10.1038/s41598-024-84879-y>
- [6] Gadallah, Waheed G., Nagwa M. Omar, and Hosni M. Ibrahim. "Machine Learning-based Distributed Denial of Service Attacks Detection Technique using New Features in Software-defined Networks." *International Journal of Computer Network & Information Security* 13.3 (2021). <https://doi.org/10.5815/ijenis.2021.03.02>
- [7] Ali, A. S. H. M. "Detection and Prevention of Distributed Denial of Service (DDoS) Attacks using Metaheuristic and Machine Learning Techniques." *Int. J. Sci. Res.* 13 (2024): 10. <https://dx.doi.org/10.21275/SR241107015558>
- [8] Tobing, Elsa Kristi Aprilia, Rara Eka Septya, and Yustian Servanda. "Comparative Analysis of Network Security: Firewall, IDS, and AI-Based Defense Against DDoS Attacks." *Journal of Artificial Intelligence and Engineering Applications (JAIEA)* 4.3 (2025): 1818-1822. <https://doi.org/10.59934/jaiea.v4i3.1026>
- [9] Aliar, Ahamed Ali Samsu, V. Gowri, and A. Arockia Abins. "Detection of distributed denial of service attack using enhanced adaptive deep dilated ensemble with hybrid meta-heuristic approach." *Transactions on Emerging Telecommunications Technologies* 35.1 (2024): e4921. <https://doi.org/10.1002/ett.4921>
- [10] Al-Matarnah, Feras Mohammed. "Integrating hybrid bald eagle crow search algorithm and deep learning for enhanced malicious node detection in secure distributed systems." *Scientific Reports* 15.1 (2025): 12647. <https://doi.org/10.1038/s41598-025-93549-6>
- [11] Sharafaldin, Iman, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani. *CIC-DDoS2019 Dataset*. Canadian Institute for Cybersecurity, University of New Brunswick, 2019, <https://www.unb.ca/cic/datasets/ddos-2019.html>
- [12] Syamsuddin, Irfan, Agung Indrawan, and Eddy Tungadi. *AISED Dataset on Cloud DDoS Attacks*. Zenodo, Version 1, 18 Jan. 2025. <https://zenodo.org/records/14681803>
- [13] Vashishtha, Lalit Kumar, and Kakali Chatterjee. "Strengthening cybersecurity: TestCloudIDS dataset and SparkShield algorithm for robust threat detection." *Computers & Security* 151 (2025): 104308. <https://doi.org/10.1016/j.cose.2024.104308>
- [14] Moustafa, Nour, and Jill Slay. *UNSW-NB15 Dataset*. Australian Centre for Cyber Security, University of New South Wales, 2015, <https://research.unsw.edu.au/projects/unsw-nb15-dataset>
- [15] Rizk-Allah, Rizk M., Aboul Ella Hassanien, and Adam Slowik. "Multi-objective orthogonal opposition-based crow search algorithm for large-scale multi-objective optimization." *Neural computing and applications* 32.17 (2020): 13715-13746. <https://doi.org/10.1007/s00521-020-04779-w>
- [16] Hamed Alnaish, Zakaria A., and Zakariya Yahya Algamal. "Improving binary crow search algorithm for feature selection." *Journal of Intelligent Systems* 32.1 (2023): 20220228. <https://doi.org/10.1515/jisys-2022-0228>
- [17] Xu, Wei, Ruifeng Zhang, and Lei Chen. "An improved crow search algorithm based on oppositional forgetting learning." *Applied Intelligence* 52.7 (2022): 7905-7921. <https://doi.org/10.1007/s10489-021-02701-y>
- [18] Hossain, Md Alamgir, and Md Saiful Islam. "Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity." *Measurement: Sensors* 32 (2024): 101037. <https://doi.org/10.1016/j.measen.2024.101037>
- [19] Ramzan, Mahrukh, et al. "Distributed denial of service attack detection in network traffic using deep learning algorithm." *Sensors* 23.20 (2023): 8642. <https://doi.org/10.3390/s23208642>
- [20] Akgun, Devrim, Selman Hizal, and Unal Cavusoglu. "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity." *Computers & Security* 118 (2022): 102748. <https://doi.org/10.1016/j.cose.2022.102748>
- [21] Wang, Yingqing, Guihe Qin, and Gaoxiang Lan. "An Online Adaptive Anomaly Detection Framework for Fog Environments." *IEEE Internet of Things Journal* (2025). <https://doi.org/10.1109/JIOT.2025.3637028>
- [22] Chen, Shao-Rui, Shiang-Jiun Chen, and Wen-Bin Hsieh. "Enhancing Machine Learning-Based DDoS Detection Through Hyperparameter Optimization." *Electronics* 14.16 (2025): 3319. <https://doi.org/10.3390/electronics14163319>
- [23] Sawah, Mohamed S., et al. "Distributed denial of service (DDoS) classification based on random forest model with backward elimination algorithm and grid search algorithm." *Scientific Reports* 15.1 (2025): 19063. <https://doi.org/10.1038/s41598-025-03868-x>
- [24] Dasari, Kishore Babu, and Nagaraju Devarakonda. "Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms." *Ingénierie des Systèmes d'Inf.* 26.5 (2021): 461-468. <https://doi.org/10.18280/isi.260505>
- [25] Mittal, Meenakshi, Krishan Kumar, and Sunny Behal. "DDoS-AT-2022: a distributed denial of service attack dataset for evaluating DDoS defense system." *Proceedings of the Indian National Science Academy* 89.2 (2023): 306-324. <https://doi.org/10.1007/s43538-023-00159-9>
- [26] Balasubramaniam, S., et al. "Optimization enabled deep learning-based ddos attack detection in cloud computing." *International Journal of Intelligent Systems* 2023.1 (2023): 2039217. <https://doi.org/10.1155/2023/2039217>
- [27] Sanjalawe, Yousef, and Turke Althobaiti. "DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning." *Computers, Materials & Continua* 75.2 (2023). <https://doi.org/10.32604/cmc.2023.037386>
- [28] Ouhssini, Mohamed, et al. "DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing." *Journal of King Saud University-Computer and Information Sciences* 36.2 (2024): 101938. <https://doi.org/10.1016/j.jksuci.2024.101938>

Authors' Profiles



Indurthi Srikanth is currently pursuing his Ph.D. at VIT-AP University, Amaravathi, Andhra Pradesh, India. He completed his Master of Science (M.S.) degree from Charles Sturt University, Australia, in 2019. Prior to commencing his doctoral studies, he worked as a .NET Developer for three years in reputed organizations in Bangalore and Hyderabad, gaining valuable industry experience in software development and cloud-based technologies. He is currently serving as a Teaching Assistant at VIT-AP University, where he actively contributes to academic and research activities. He has successfully guided 8 undergraduate projects and 3 master's projects and has mentored more than 25 students in their academic and research endeavours. His research contributions include the publication of five scholarly articles in the area of cloud security attacks. His current research interests focus on cloud security, cybersecurity, distributed computing environments, and the detection and mitigation of Distributed Denial-of-Service (DDoS) attacks in cloud computing systems.



Ganesh Reddy Karri received the Ph.D. degree from NIT-Suratkal, Karnataka, India, in 2014. he is currently a Senior Associate Professor in the School of Computer Science and Engineering (SCOPE), VIT-AP University, Amaravati, India. Currently his coordinator for center of excellence in cyber security and also an IEEE member. His awarded for four Ph.D. scholars. Currently his guiding for five research scholars. He has more than 15 years' experience in both Research and Teaching. he has already published more than 95 Research articles in various reputed journals, book chapters, and conferences. His research interests include Cloud computing, Computer and Network Security, Wireless networks, Data structures and Algorithms and the IoT.

How to cite this paper

Srikanth Indurthi, Ganesh Reddy Karri, "RF-OCSA: A Hybrid Metaheuristic Feature Selection Framework for DDoS Attack Detection in Cloud Environments", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.4, pp. 111-136, 2026. DOI:10.5815/ijwmt.2026.04.08