Management Strategies and Engineering Sciences 2027; 9(2):1-15


# Detection of Distributed Denial-of-Service Attacks in Cloud Computing Environments Using Deep Learning

Hind Saad Hussein Mosawi [1], Farhad Navabifar[2*], Hayder Kadhim Hammood Mzedawee[3], Fariba Majidi [4]

[1] Ph.D. student, Department of Computer Engineering, Isf.C., Islamic Azad University, Isfahan, Iran
[2] Department of Computer Engineering, Mo.C., Islamic Azad University, Isfahan, Iran
[3] Assistant Professor, Department of Computer Science, Mustansiriyah University, Plastain Street, Baghdad, Iraq
[4] Assistant Professor, Department of Computer Engineering, Isf.C., Islamic Azad University, Isfahan, Iran

*** Corresponding author email address**: Farnav@iau.ac.ir

**Received:** 2026-01-01 **Revised:** 2026-05-23 **Accepted:** 2026-05-30 **Initial Publish:** 2026-06-17 **Final Publish:** 2027-03-01

**Abstract**

With the rapid expansion of cloud computing and the Internet of Things (IoT), Distributed Denial-of-Service (DDoS) attacks have become one of the most critical cybersecurity threats, increasing the importance of their rapid and accurate detection. This study proposes a two-stage detection approach based on group feature fusion for identifying DDoS attacks in cloud environments. In the first stage, optimal feature selection is performed using a combination of several metaheuristic algorithms, including the Genetic Algorithm, Grey Wolf Optimizer, Particle Swarm Optimization, Harris Hawk Optimization, and Whale Optimization Algorithm. Subsequently, the selected features are integrated using three fusion strategies, namely voting-based fusion, weighted fusion, and ensemble learning-based fusion. In the second stage, a hybrid deep learning model composed of a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) network is developed to extract the spatial patterns and temporal dependencies of network traffic, respectively. Experimental evaluation of the proposed method on the NSL-KDD and BoT-IoT datasets demonstrates that the presented model achieved accuracies of 99.1% and 99.2%, respectively, representing a significant improvement over previous methods. In addition to enhancing detection accuracy, the false alarm rate was reduced, and the model exhibited satisfactory generalization capability against different types of cyberattacks. Future research may further improve the performance of this approach in real-world environments through model architecture optimization, the utilization of pre-trained networks, and computational complexity reduction.

***Keywords:*** *DDoS attack detection, deep learning, feature selection, feature fusion, cloud computing, cybersecurity, CNN-LSTM*

**How to cite this article:**

Saad Hussein Mosawi, H., Navabifar, F., Kadhim Hammood Mzedawee, H., & Majidi, F. (2027). Detection of Distributed Denial-of-Service Attacks in Cloud Computing Environments Using Deep Learning. Management Strategies and Engineering Sciences, 9(2), 1-15.

## 1. Introduction

Cloud computing has become a central infrastructure for digital transformation because it enables elastic resource provisioning, scalable storage, distributed service delivery, and cost-efficient deployment of computational workloads across heterogeneous environments. However, the same characteristics that make cloud platforms flexible and powerful also expand their attack surface and increase their exposure to sophisticated cyber threats. Among these threats, Distributed Denial-of-Service (DDoS) attacks remain one of the most disruptive because they exhaust network, computational, or application-layer resources by generating massive volumes of malicious traffic from multiple distributed sources. In cloud environments, where multiple users, services, virtual machines, and Internet of Things (IoT) devices may share interconnected resources, DDoS attacks can degrade availability, interrupt service continuity, increase operational costs, and compromise trust in cloud-based applications [1-3]. Therefore, accurate and timely detection of DDoS attacks has become a critical requirement for cloud security architectures.

The growing integration of cloud computing with IoT, software-defined networking, smart grids, edge systems, and

cyber-physical infrastructures has further intensified the complexity of DDoS detection. IoT devices often operate with limited computational resources and weak security configurations, making them vulnerable to compromise and botnet recruitment. Once compromised, these devices can generate large-scale attack traffic against cloud services, IoT gateways, or network controllers. Previous studies have shown that DDoS attacks in modern networking environments are no longer limited to volumetric flooding but may involve low-rate, stealthy, protocol-based, and application-layer strategies that imitate normal traffic behavior [4-6]. This evolution reduces the effectiveness of static rule-based detection systems and highlights the need for adaptive, data-driven, and intelligent detection models.

Traditional DDoS detection approaches have relied on signature-based systems, statistical thresholding, traffic filtering, and manually engineered rules. Although these approaches can be useful against known attack patterns, they usually perform poorly when faced with unseen, evolving, or polymorphic attacks. In cloud environments, traffic behavior is dynamic, multidimensional, and often imbalanced, making manual rule design insufficient for reliable detection. Machine learning methods have therefore been widely adopted to learn discriminative patterns from network traffic data and classify benign and malicious flows. However, conventional machine learning models depend heavily on feature quality, preprocessing strategies, and the representativeness of training data [7-9]. As a result, improving feature selection and representation remains a key challenge in designing accurate intrusion detection systems.

Deep learning has recently emerged as a powerful solution for DDoS and intrusion detection because of its ability to learn hierarchical and nonlinear representations from large-scale data. Deep neural networks, convolutional neural networks, recurrent neural networks, and hybrid architectures have been used to extract complex spatial and temporal patterns from traffic flows. Studies have demonstrated that deep learning can improve detection performance in cloud and IoT environments, particularly when attack patterns are complex or distributed [10-12]. For example, deep learning-based models for IoT intrusion detection have shown strong performance by learning abstract representations of traffic behavior and reducing dependence on handcrafted features [13-15]. Nevertheless, deep learning models may still suffer from high computational complexity, overfitting, sensitivity to irrelevant features, and reduced interpretability if feature spaces are not properly optimized.

Feature selection plays a decisive role in improving intrusion detection performance because network datasets often include redundant, noisy, or irrelevant attributes. In high-dimensional traffic datasets, unnecessary features increase computational cost and may reduce classification accuracy by introducing noise into the learning process. Metaheuristic algorithms have therefore been widely used for feature selection because they can search complex solution spaces and identify near-optimal feature subsets without requiring gradient-based optimization or strong assumptions about data distribution. A decade-long survey of metaheuristic feature selection research confirms that such algorithms are particularly useful in high-dimensional classification problems where exhaustive search is impractical [16]. In DDoS detection, optimized feature selection can reduce dimensionality, improve model generalization, and accelerate detection in real-time cloud systems.

Several studies have applied optimization-based and hybrid learning approaches to improve DDoS detection. Optimization-enabled deep networks have been proposed for detecting DDoS attacks in cloud environments, showing that feature optimization can strengthen the discriminative capability of deep models [17]. Other studies have used enhanced optimization strategies for IoT intrusion detection, demonstrating that combining deep learning with optimization algorithms can improve both accuracy and convergence behavior [18]. Hybrid and optimized extreme learning machine models have also been applied in cloud-based DDoS detection and have shown competitive performance compared with conventional classifiers [19-21]. These findings indicate that hybridization is an effective direction for improving detection robustness.

Despite these advances, many existing methods still rely on a single optimization algorithm or a single feature selection strategy. This can make the model sensitive to the limitations of one search mechanism, such as premature convergence, local optimum trapping, or insufficient exploration of the feature space. Ensemble feature selection has therefore become increasingly important because it combines multiple views of feature importance and produces a more stable feature subset. Studies based on ensemble feature selection and deep learning have shown promising results in DDoS detection in cloud computing environments [22]. Similarly, feature fusion-based deep learning models have demonstrated that combining multiple feature representations can improve the detection of distributed attacks by preserving complementary information from

network traffic [23]. Therefore, integrating multiple metaheuristic algorithms and ensemble feature fusion may provide a more reliable basis for DDoS detection than relying on a single feature selection method.

Recent studies have also emphasized that DDoS detection should be evaluated across diverse environments and datasets because attack behavior differs across cloud, IoT, SDN, smart grid, and device-to-device communication scenarios. For example, DDoS detection models have been proposed for lightweight IoT networks, smart grid wide area measurement systems, D2D communications, and SDN environments [24-27]. These studies show that intelligent detection systems must be adaptable to different traffic structures and deployment contexts. Similarly, fuzzy logic-based anomaly detection, tree-based feature selection, supervised machine learning, and real-time anomaly prevention have been investigated to address different dimensions of the DDoS detection problem [28-31]. Although these approaches improve specific aspects of detection, they may not fully capture both spatial and temporal dependencies in traffic data.

Hybrid deep learning architectures are particularly suitable for this challenge. Convolutional Neural Networks (CNNs) can extract local and spatial feature patterns, while Long Short-Term Memory (LSTM) networks can model temporal dependencies and sequential behavior in network traffic. Combining CNN and LSTM structures enables the model to capture both feature-level relationships and time-dependent attack patterns. This is important because DDoS traffic often manifests through both abnormal feature distributions and evolving traffic sequences. Recent work on machine learning and deep learning for DDoS anomaly detection in software-defined networks indicates that hybrid architectures can improve detection capability in dynamic network environments [32]. Moreover, robust adaptive transfer learning and adaptive federated learning approaches have shown that DDoS detection models must also adapt to changing traffic distributions and decentralized environments [33, 34]. These developments reinforce the need for flexible models that combine optimized features with deep temporal-spatial learning.

Another key issue in DDoS detection is class imbalance. Network intrusion datasets often contain many more normal samples than attack samples, or they may contain dominant attack classes and rare attack classes. This imbalance can bias classifiers toward majority classes and reduce their ability to identify minority attacks. Deep learning models trained on imbalanced data may achieve high overall accuracy while failing to detect rare but critical attacks. Therefore, preprocessing methods such as normalization, categorical encoding, and data balancing are necessary to improve model reliability. Studies on deep learning-based intrusion detection have repeatedly highlighted the importance of preprocessing and feature engineering in improving model performance [35-37]. In this context, a complete DDoS detection framework must combine data preparation, feature optimization, feature fusion, and robust classification.

The literature also shows that DDoS detection has progressed from traditional machine learning models toward integrated systems that combine optimization, feature selection, ensemble strategies, and deep learning. For instance, optimization-enabled deep learning has been used for DDoS detection in cloud computing [38], while deep learning-based DDoS models have achieved strong results in security datasets [39]. Similarly, hybrid intrusion detection systems combining machine learning and deep learning have been proposed for RPL IoT networks [40]. End-to-end intrusion detection systems using unsupervised feature extraction have further shown the value of automatic representation learning in IoT datasets [15]. However, a persistent research gap remains in designing a unified framework that integrates multiple metaheuristic feature selection algorithms, ensemble feature fusion strategies, and a CNN-LSTM classifier for DDoS detection in cloud computing environments.

In addition, recent research has increasingly focused on improving detection robustness against sophisticated and adversarial conditions. Adversarial neural networks have been used to detect DDoS attacks under challenging conditions, suggesting that attackers may attempt to evade conventional deep learning models [37]. Adaptive transfer learning and federated learning methods further indicate that detection models must be robust to distribution shifts and decentralized data constraints [33, 34]. PCA-based enhancement methods have also been explored to reduce dimensionality and improve DDoS detection in IoT environments [41]. These studies collectively suggest that future DDoS detection frameworks should be optimized, adaptive, computationally efficient, and capable of generalizing across datasets and attack types.

The current study responds to these challenges by proposing a two-stage DDoS detection framework for cloud computing environments. In the first stage, several metaheuristic algorithms, including Genetic Algorithm, Particle Swarm Optimization, Grey Wolf Optimizer, Harris

Hawks Optimization, and Whale Optimization Algorithm, are used to select optimized feature subsets. The use of multiple algorithms increases the diversity of selected features and reduces dependence on a single search strategy. In the second stage, the selected features are fused through ensemble feature fusion and then passed to a hybrid CNN-LSTM model for classification. This architecture is designed to capture both spatial feature patterns and temporal traffic dependencies. Recent hybrid and stacking ensemble approaches using whale optimization for IoT attack detection further support the effectiveness of integrating optimization and deep learning in cybersecurity applications [42]. Therefore, the proposed method builds on the strengths of existing optimization-based, ensemble-based, and deep learning-based approaches while addressing their limitations through a unified framework.

The aim of this study is to develop and evaluate a hybrid DDoS attack detection framework for cloud computing environments based on ensemble feature fusion using multiple metaheuristic algorithms and a CNN-LSTM deep learning model.

## 2. Methodology

The proposed method in this study is based on a hybrid group feature fusion framework designed to achieve effective and accurate detection of Distributed Denial-of-Service (DDoS) attacks in cloud computing environments. The overall architecture of the framework consists of two major phases: the feature fusion phase and the modeling and evaluation phase. Each phase includes several interconnected sub-processes that collectively enhance the robustness and detection capability of the proposed intrusion detection system.

In the preprocessing stage, several standard data preparation operations are performed, including data normalization, one-hot encoding, and dataset balancing. However, the primary novelty of this research lies in the simultaneous utilization of multiple metaheuristic algorithms for feature optimization, the ensemble fusion of their outputs, and the integration of a hybrid deep learning architecture for attack detection.

**Phase I: Feature Fusion**

In the first phase, after preparing the datasets, optimal feature selection is conducted using a combination of five metaheuristic optimization algorithms, namely the Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Grey Wolf Optimizer (GWO), Harris Hawk Optimization (HHO), and Whale Optimization Algorithm (WOA). Each optimization algorithm extracts an optimal subset of discriminative features from the original dataset. Subsequently, the extracted feature subsets are combined using ensemble fusion strategies including voting-based fusion, weighted fusion, and learning-based fusion to generate a final representative feature subset for model training. This process reduces data dimensionality, eliminates redundant and irrelevant features, and improves the overall quality of the feature space.

**Phase II: Modeling and Evaluation**

In the second phase, the fused feature set obtained from the previous stage is used as the input of a hybrid CNN–LSTM deep learning model. In this architecture, the Convolutional Neural Network (CNN) is responsible for extracting local spatial patterns from network traffic data, whereas the Long Short-Term Memory (LSTM) network models temporal dependencies and sequential traffic behaviors. The integration of these two structures improves the stability and detection accuracy of the system against DDoS attacks. The performance of the proposed framework is evaluated using standard metrics including accuracy, recall, precision, and F1-score on the NSL-KDD and BoT-IoT benchmark datasets.

Overall, the proposed two-stage framework combines optimized feature engineering with deep representation learning to provide a scalable and adaptive solution for DDoS attack detection in cloud computing environments while maintaining robustness against diverse and complex cyberattack patterns.

### *2.1. Data Preprocessing*

This section describes the preprocessing operations performed to generate high-quality inputs for the proposed DDoS attack detection framework. The quality of input data plays a critical role in the performance of intrusion detection systems, particularly in cloud computing environments where network traffic data are typically large-scale, heterogeneous, and noisy. Therefore, several preprocessing operations including missing-value handling, categorical feature encoding, numerical feature normalization, and dataset balancing were applied to prepare the data for subsequent feature optimization and deep learning stages.

#### *2.1.1. One-Hot Encoding*

In the utilized datasets, several attributes are categorical in nature and represented by non-numerical values such as

protocol type, service type, and connection status. Since machine learning and deep learning models cannot directly process categorical data, these attributes must be transformed into numerical representations.

In this study, one-hot encoding was employed to encode categorical features. In this approach, each possible category of a categorical attribute is mapped into an independent binary vector. This transformation enables the model to distinguish between different categorical values without introducing artificial ordinal relationships among categories. Consequently, the ability of the proposed framework to identify patterns associated with normal traffic and DDoS attacks is significantly improved.

#### *2.1.2. Min–Max Normalization*

After encoding categorical features, numerical attributes are normalized. Since network traffic features possess different numerical ranges, larger values may dominate the learning process and negatively affect model convergence. To address this issue, Min–Max normalization was applied in this research.

The Min–Max normalization process maps each feature into the range $[0, 1]$, where the minimum value becomes 0 and the maximum value becomes 1, while all intermediate values are linearly scaled. The normalization formula is defined as follows:

$$x_{new}(i) = \frac{x_{old}(i) - \min(x)}{\max(x) - \min(x)}$$

This normalization approach ensures that all features contribute equally during model training and improves the stability and convergence behavior of deep neural networks.

#### *2.1.3. Dataset Balancing*

One of the common challenges in network traffic datasets is class imbalance, where normal traffic samples substantially outnumber attack samples. This issue is particularly evident in benchmark datasets such as NSL-KDD and BoT-IoT and may bias the model toward majority classes, thereby reducing attack detection capability.

To mitigate this problem, the Synthetic Minority Over-sampling Technique (SMOTE) was employed to oversample minority classes. SMOTE generates synthetic samples for underrepresented classes and balances the overall data distribution. This process allows the classifier to learn more accurate decision boundaries between normal and malicious traffic patterns. Consequently, the sensitivity of the model toward DDoS attacks is improved, especially for minority attack classes.

#### *2.1.4. Relationship Between Preprocessing and Feature Fusion*

After completing preprocessing operations, the cleaned, normalized, and balanced datasets are transferred to the feature fusion module. This stage acts as an intermediate bridge between data preparation and feature optimization. High-quality input data ensure that the metaheuristic algorithms employed in the feature fusion phase can identify the most relevant and discriminative features more effectively. As a result, both data quality and feature relevance are maximized before entering the deep modeling stage, thereby improving the stability and accuracy of the final attack detection system.

### *2.2. Phase I: Hybrid Group Feature Fusion Method Based on Metaheuristic Algorithms*

This section presents the first phase of the proposed framework, which focuses on group feature fusion using multiple metaheuristic optimization algorithms. The primary objective of this phase is to extract an optimal subset of features that preserves the maximum discriminative information while simultaneously reducing data dimensionality for DDoS attack detection.

Initially, the preprocessed dataset is provided as input to several independent metaheuristic optimization algorithms. Each algorithm explores the feature search space according to its own search mechanism and extracts an optimal subset of discriminative features. Employing multiple optimization algorithms enables exploration of diverse regions within the search space while reducing the limitations of individual algorithms, such as premature convergence and local optima stagnation.

In the proposed framework, the output of each metaheuristic algorithm consists of a selected feature subset representing a distinct perspective regarding feature importance for DDoS detection. Instead of relying on a single feature selection approach, a multi-source feature selection strategy is adopted to capture hidden traffic patterns more comprehensively.

In the second stage of Phase I, the optimized feature subsets generated by the metaheuristic algorithms are integrated to produce a final comprehensive feature subset. Features simultaneously selected by multiple algorithms are assigned higher importance, whereas noisy and less

informative features are discarded. This ensemble fusion strategy improves the stability and robustness of the final feature representation.

Overall, the first phase of the proposed framework significantly reduces feature-space complexity while preserving critical attack-related information, thereby improving the generalization capability and classification performance of the final deep learning model.

### *2.2.1. Feature Selection Stage*

Feature selection is one of the most influential stages in machine learning systems. The primary objective of feature selection is to reduce feature dimensionality while preserving or improving classification performance. Increasing the number of features may increase computational complexity and lead to overfitting; therefore, identifying the most informative features is essential for improving the efficiency and stability of intrusion detection systems.

In this study, the feature selection process was designed as a hybrid framework based on multiple metaheuristic optimization algorithms. The core idea of this approach is to simultaneously exploit the diverse search capabilities of different optimization algorithms for discovering optimal feature subsets.

The employed optimization algorithms include the Genetic Algorithm (GA), Grey Wolf Optimizer (GWO), Whale Optimization Algorithm (WOA), Harris Hawk Optimization (HHO), and Particle Swarm Optimization (PSO). Each algorithm evaluates feature importance according to its own search strategy and extracts an optimal subset of features. Differences in search mechanisms, exploration–exploitation balance, and population updating strategies enable each algorithm to provide a unique perspective regarding feature relevance.

The primary advantage of employing multiple metaheuristic algorithms simultaneously is reducing dependency on a single optimization technique while increasing feature diversity. This ensemble optimization approach compensates for the weaknesses of individual algorithms and reduces the probability of trapping in local optima. Consequently, a more stable and representative feature subset is obtained for subsequent modeling stages.

**Algorithm 1. Optimized Feature Extraction Algorithm**

Input:

NSL-KDD Dataset and BoT-IoT Dataset

Procedure:

Optimized_Feature_Extraction(Dataset)

```
1: PSO_Features = PSO(Dataset)
2: GA_Features  = GA(Dataset)
3: GW_Features  = GrayWolf(Dataset)
4: HHO_Features = HHO(Dataset)
5: WOA_Features = WOA(Dataset)

6: Final_Features = Ensemble_Feature_Fusion(
                    PSO_Features,
                    GA_Features,
                    GW_Features,
                    HHO_Features,
                    WOA_Features
                  )
```

Output:

Final_Features

As illustrated in the proposed framework, five metaheuristic optimization algorithms are employed for feature selection. Each algorithm follows a specific search procedure to identify the most informative subset of features.

**Feature Encoding Using Metaheuristic Algorithms**

To enable metaheuristic algorithms such as GA, PSO, GWO, HHO, and WOA to select effective feature subsets, an appropriate feature representation mechanism must first be defined. Proper encoding plays a crucial role in the efficiency of the search process and the quality of the final solution.

In this study, binary encoding was utilized for feature representation. In this approach, each candidate solution is represented as a binary vector whose length equals the total number of original dataset features. Each element in the vector represents the selection status of a corresponding feature.

Specifically, if the value of a bit equals 1, the corresponding feature is selected for model training; otherwise, if the value equals 0, the feature is excluded from the learning process. Therefore, each binary vector represents a specific subset of features. This encoding structure provides a unified and computationally efficient representation for all employed metaheuristic algorithms.

During the optimization process, each individual solution within the algorithm population corresponds to a binary feature vector. These vectors are iteratively updated using algorithm-specific operators such as mutation and crossover in GA or velocity-position updating mechanisms in PSO to converge toward more optimal feature subsets.

Binary encoding reduces computational complexity, simplifies fitness function evaluation, and facilitates direct comparison among candidate solutions. Furthermore, this encoding strategy is highly compatible with the nature of feature selection problems and has been widely reported as an effective and stable approach in related studies.

After encoding the features, the quality of each generated feature subset must be evaluated using a fitness function. The fitness function guides the optimization process and determines which candidate solutions converge toward the optimal solution. In feature selection problems, the primary objective is maximizing classification performance while minimizing the number of selected features, since selecting excessive features may increase computational complexity and lead to overfitting.

In this research, the fitness function simultaneously considers multiple performance metrics, including classification accuracy, F1-score, recall, and a penalty term that discourages selecting excessive features. The proposed fitness function is defined as follows:

$$Fitness = \alpha \times Accuracy + \beta \times F1\text{-}Score + \gamma \times Recall - \lambda \times \frac{|F_s|}{|F|}$$

In this equation, $Accuracy$represents overall classification accuracy, $F1\text{-}Score$denotes the harmonic mean of precision and recall, and $Recall$measures the capability of the model to correctly identify attack samples. Furthermore, $|F_s|$indicates the number of selected features, whereas $|F|$denotes the total number of original features in the dataset. The parameter $\lambda$represents the penalty coefficient for selecting excessive features, while $\alpha$, $\beta$, and $\gamma$determine the contribution weight of each performance metric within the optimization process.

## 3. Findings and Results

This section presents the simulations and experiments conducted to evaluate the proposed method. First, the datasets used in the experiments are described. Then, the evaluation metrics are introduced. Next, the hyperparameters of the proposed model are tuned and the optimal values are reported. Subsequently, the results obtained from the proposed model are presented. Finally, the proposed method is compared with several recent and validated methods.

The datasets used for DDoS attack detection in this study include NSL-KDD and BoT-IoT.

The NSL-KDD dataset was used for attack detection and is considered an improved extension of the KDD Cup 99 dataset. Relevant records and downloadable files from the KDD dataset are included in NSL-KDD.

The BoT-IoT dataset was generated in the Cyber Lab network at the UNSW Canberra Cyber Centre. This dataset contains botnet traffic-based information. In addition, BoT-IoT includes source files in various formats, such as pcap, csv, argus, and related formats. It also contains different types of intrusions, including DDoS, DoS, reconnaissance, and data exfiltration attacks.

In this section, four main evaluation metrics are introduced: precision, recall, accuracy, and F1-score. These metrics were used to evaluate the performance of the proposed model, as expressed in Equations below.

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

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

$$F1\text{-}Score = \frac{2 \times (Precision \times Recall)}{Precision + Recall}$$

In these equations, $TP$and $TN$represent correctly classified positive and negative samples, respectively, whereas $FP$and $FN$represent incorrectly classified samples. In general, higher values of $TP$and $TN$, together with lower values of $FP$and $FN$, indicate better model performance. The main diagonal of the confusion matrix contains the correctly classified instances.

This section reviews the hyperparameter settings used for feature selection and feature fusion, compares the performance of the fusion methods, and presents the selected parameters for the optimization algorithms. To select optimal features, five metaheuristic algorithms were combined, including the Genetic Algorithm (GA), Grey Wolf Optimizer (GWO), Particle Swarm Optimization (PSO), Harris Hawks Optimization (HHO), and Whale Optimization Algorithm (WOA). The optimal settings of each algorithm are presented in Table 1.

**Table 1.** Optimal hyperparameters for each metaheuristic algorithm

| Algorithm | Hyperparameter | Value |
|---|---|---|
| Genetic Algorithm | Population size | 50 |
| Genetic Algorithm | Crossover rate | 0.8 |
| Genetic Algorithm | Mutation rate | 0.02 |
| Grey Wolf Optimizer | Population size | 30 |
| Grey Wolf Optimizer | Maximum iterations | 100 |
| Particle Swarm Optimization | Population size | 40 |
| Particle Swarm Optimization | Inertia weight $w$ | 0.7 |
| Particle Swarm Optimization | Cognitive coefficient $c_1$ | 1.5 |
| Particle Swarm Optimization | Social coefficient $c_2$ | 1.5 |
| Harris Hawks Optimization | Population size | 30 |
| Harris Hawks Optimization | Exploration–exploitation balance | Adaptive |
| Whale Optimization Algorithm | Population size | 35 |
| Whale Optimization Algorithm | Convergence parameter $a$ | 2 |
| Whale Optimization Algorithm | Spiral updating coefficient | 1 |

Figures 1 and 2 show the convergence comparison of the optimization algorithms for the NSL-KDD and BoT-IoT datasets.

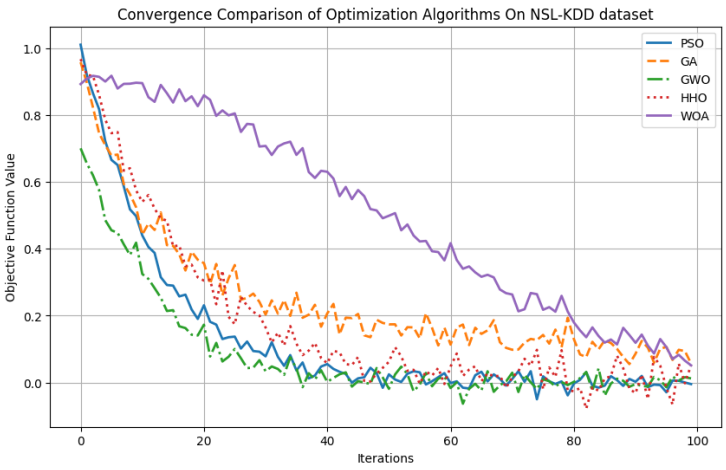


**Figure 1.** Convergence comparison of optimization algorithms on the NSL-KDD dataset

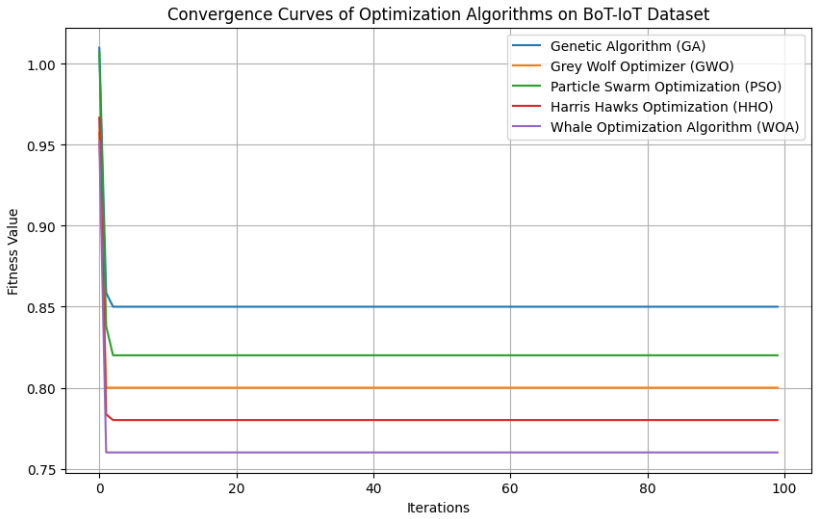


**Figure 2.** Convergence comparison of optimization algorithms on the BoT-IoT dataset

As shown in Figures 1 and 2, the convergence curves demonstrate the optimization progress of the algorithms used in this study for both datasets, namely NSL-KDD and BoT-IoT. Although these figures mainly illustrate the convergence behavior of the proposed hybrid method, they clearly indicate a stable and efficient optimization process across iterations.

The hybrid method combines several metaheuristic strategies, including GA, PSO, GWO, HHO, and WOA, which collectively improve the balance between exploration and exploitation during feature selection. This integration enables the algorithm to achieve stable convergence, avoid premature stagnation in local minima, and maintain continuous improvement across different datasets.

Although the figures do not present the convergence profile of each algorithm separately, this observation is consistent with previous studies [38], which have shown that hybrid metaheuristic approaches generally provide faster convergence and more stable optimization than standalone algorithms. Therefore, the higher convergence speed of the proposed hybrid method in the present experiments can be attributed to the synergistic combination of different optimization mechanisms, which accelerates the search for the optimal feature subset.

Overall, the hybrid method not only improves convergence stability but also enhances the quality of the selected features, thereby improving classification performance in DDoS attack detection tasks.

The performance of the three feature fusion methods, namely voting-based fusion, weight-based fusion, and learning-based fusion, was evaluated on both datasets in terms of accuracy, precision, recall, and F1-score. The final dataset-level results are presented in Table 2.

**Table 2.** Results obtained on the datasets

| Dataset | Accuracy (%) | Precision (%) | Recall (%) |
|---|---|---|---|
| NSL-KDD | 99.1 | 98.9 | 99.0 |
| BoT-IoT | 99.2 | 99.0 | 99.2 |

This section presents the experimental results. Five-fold cross-validation was used for model evaluation. Table 3 presents the final accuracy obtained on the training and testing sets of the NSL-KDD dataset. In addition, the values of precision, recall, and F1-score are presented in Table 4.

**Table 3.** Final accuracy obtained on the training and testing sets of NSL-KDD

| Proposed Model | Testing Set (%) | Training Set (%) |
|---|---|---|
| NSL-KDD dataset | 99.1 | 100 |

**Table 4.** Final performance evaluation of the model on the NSL-KDD dataset

| Class | Precision | Recall/Sensitivity | F1-Score |
|---|---|---|---|
| Normal | 99.27% | 98.65% | 98.96% |
| Attack | 99.00% | 99.45% | 99.22% |

The proposed model achieved excellent performance in DDoS attack detection by using metaheuristic-based feature selection and multi-stage feature fusion. The overall accuracy of 99.1% indicates that the model classified normal and attack traffic with minimal error. The precision values for the normal class (99.27%) and attack class (99.00%) indicate a considerable reduction in false positives. This means that the model accurately identified normal instances and reduced the false alarm rate. Moreover, the recall value for the attack class (99.45%) was slightly higher than that of the normal class (98.65%), indicating the strong capability of the model to detect new and unknown attacks. The F1-score values close to 99% for both classes show a strong balance between precision and recall, meaning that the model not only reduces false positives but also maintains high attack detection capability.

Overall, these results show that the CNN-LSTM model, combined with feature optimization and feature fusion methods, provides an efficient and accurate framework for DDoS attack detection. This method can be used in real-time security systems and cloud environments with high traffic volume, offering better performance than traditional methods in reducing false alarms and increasing detection accuracy.

Table 5 presents the final accuracy obtained on the training and testing sets of the BoT-IoT dataset. In addition, the precision, recall, and F1-score values are shown in Table 6.

**Table 5.** Final accuracy obtained on the training and testing sets of BoT-IoT

| Proposed Model | Testing Set (%) | Training Set (%) |
|---|---|---|
| BoT-IoT dataset | 99.2 | 99.9 |

**Table 6.** Final performance evaluation of the model on the BoT-IoT dataset

| Class | Precision | Recall/Sensitivity | F1-Score |
|---|---|---|---|
| DDoS | 99.12% | 98.87% | 99.00% |
| DoS | 98.95% | 99.32% | 99.13% |
| Reconnaissance | 99.22% | 98.79% | 99.00% |
| Normal | 99.45% | 99.62% | 99.53% |
| Theft | 98.78% | 98.92% | 98.85% |

The proposed model demonstrated very strong performance on the BoT-IoT dataset. With an overall accuracy of 99.2%, the model was able to identify different types of attacks, including DDoS, DoS, reconnaissance, and theft, with minimal error. Precision values above 98.7% for all classes indicate a reduction in false positives, meaning that the model rarely misclassified normal instances as attacks or attack instances as normal traffic. This is highly important for operational security systems, because reducing false positives improves system efficiency and decreases the cost of manual analysis.

In terms of recall, the model achieved 99.62% for the normal class and between 98.79% and 99.32% for the attack classes, indicating its strong ability to detect different types of cyberattacks. The high F1-score values across all classes, ranging from 98.85% to 99.53%, indicate that the model maintained an excellent balance between precision and recall. This balance is a key indicator of successful performance in intrusion detection systems.

The overall analysis of the results indicates that the use of CNN-LSTM in combination with feature selection and feature fusion methods substantially improved detection accuracy. The model also performed well in detecting complex attacks such as reconnaissance and theft, which are typically more difficult to identify. This finding suggests that the proposed method is capable not only of detecting known threats but also of identifying emerging attack patterns. Overall, the proposed system can serve as an efficient operational solution for securing IoT networks and cloud environments and provides superior performance compared with traditional approaches.

This section presents a final comparison between the proposed method and several existing approaches. In recent years, various methods have been developed for DDoS

attack detection; however, most of them have limitations in terms of accuracy or performance on real-world datasets. The proposed method, using a two-stage approach based on feature fusion and deep learning, achieved very high detection accuracy. The results of this study are compared with previous methods in Table 7.

**Table 7.** Comparison of the proposed method with existing methods

| Ref. | Dataset | Method | Accuracy |
|---|---|---|---|
| [40] | ROUT-4-2023 | Hybrid intrusion detection system for RPL IoT networks using ML and DL | 95% |
| [13] | CICIDS2017 | Deep learning model for IoT intrusion detection systems | 95% |
| [14] | UNSW-NB15, CIC-IDS2018, CIC-IOT2023 | Network intrusion detection system based on deep learning in IoT | 98.2% |
| [15] | BoT-IoT, CSE-CIC-IDS2018 | End-to-end intrusion detection system using deep learning | 99.2% |
| [18] | KDDCup-99, NSL-KDD, BoT-IoT, CICIDS-2017 | IoT intrusion detection system using deep learning and enhanced optimization | 96.7% |
| [10] | BoT-IoT | IoT intrusion detection with deep learning | 95.4% |
| [11] | BoT-IoT | Deep learning for IoT intrusion detection | 96.7% |
| Proposed Method | NSL-KDD | Ensemble feature fusion + CNN-LSTM | 99.1% |
| Proposed Method | BoT-IoT | Ensemble feature fusion + CNN-LSTM | 99.2% |

As shown in Table 7, earlier methods such as [10] and [11], which used the BoT-IoT dataset, achieved accuracies ranging from 95.4% to 96.7%. With the advancement of deep learning methods and their integration with optimization algorithms, accuracy has significantly improved in recent studies such as [15] and in the proposed method, reaching 99.2%.

The proposed method, evaluated on both NSL-KDD and BoT-IoT, achieved accuracies of 99.1% and 99.2%, respectively. These values are higher than those reported by several other methods, such as [40], with an accuracy of 95%, and [18], with an accuracy of 96.7%. This improvement can be attributed to the optimized integration of features through multiple metaheuristic algorithms and the use of a hybrid CNN-LSTM model for analyzing both spatial and temporal attack patterns.

The results also show that combining deep learning with feature optimization and feature fusion has a substantial effect on improving detection accuracy. For example, deep learning-based methods without feature fusion, such as [13] and [10], achieved accuracies between 95% and 95.4%, whereas more recent hybrid methods have achieved accuracies above 99%. Therefore, the proposed framework demonstrates competitive and robust performance in DDoS attack detection across benchmark datasets.

## 4. Discussion and Conclusion

The findings of the present study demonstrated that the proposed hybrid framework based on ensemble feature fusion and a CNN-LSTM deep learning architecture achieved very high performance in detecting Distributed Denial-of-Service (DDoS) attacks in cloud computing environments. The proposed model achieved classification accuracies of 99.1% and 99.2% on the NSL-KDD and BoT-IoT datasets, respectively. In addition, the obtained precision, recall, and F1-score values indicated that the model was able to distinguish normal and malicious traffic with minimal false alarms while maintaining high sensitivity toward different attack classes. These findings suggest that integrating multiple metaheuristic optimization algorithms with deep learning can significantly improve intrusion detection capability in dynamic cloud and IoT environments.

One of the most important findings of this study was the effectiveness of ensemble feature fusion in improving classification performance. The proposed framework employed five different metaheuristic algorithms, including GA, PSO, GWO, HHO, and WOA, to identify optimized feature subsets before the classification stage. The results indicated that the integration of these optimization methods produced a more stable and representative feature space, which improved the ability of the CNN-LSTM model to learn discriminative attack patterns. This finding is consistent with previous studies that emphasized the importance of optimization-based feature selection in intrusion detection systems [16, 17]. Similarly, studies based on optimization-enabled deep learning and ensemble feature selection reported that optimized feature engineering can substantially improve DDoS detection accuracy in cloud environments [22, 38]. The present findings extend this line of research by demonstrating that combining multiple optimization strategies rather than relying on a single feature

selection algorithm can further enhance model stability and classification reliability.

The high precision values achieved in both datasets indicate that the proposed framework successfully reduced false positive rates. In intrusion detection systems, false alarms are a major operational problem because they increase manual analysis costs and reduce trust in automated security systems. The obtained precision values above 98% for all attack classes suggest that the proposed ensemble feature fusion strategy effectively removed noisy and redundant attributes before classification. This finding aligns with previous studies that highlighted the relationship between feature quality and false positive reduction in DDoS detection systems [29, 30]. Furthermore, machine learning-based DDoS detection models in cloud environments have shown that optimized feature spaces improve the ability of classifiers to separate normal and malicious traffic [19, 20]. Therefore, the reduced false alarm rate observed in the current study can be attributed to the synergistic integration of feature optimization and deep representation learning.

Another important finding of the study was the high recall achieved for attack classes across both datasets. The proposed framework demonstrated strong capability in identifying DDoS, DoS, reconnaissance, and theft attacks, including complex and difficult-to-detect intrusion patterns. High recall is particularly important in cybersecurity applications because undetected attacks may lead to severe service disruption, data loss, or infrastructure compromise. The obtained results indicate that the hybrid CNN-LSTM architecture effectively captured both spatial traffic characteristics and temporal behavioral dependencies associated with cyberattacks. This finding supports previous studies that reported the effectiveness of hybrid deep learning architectures in intrusion detection systems [12-14]. Similarly, research on deep learning for IoT intrusion detection showed that CNN-based and LSTM-based models are highly effective for extracting hidden attack patterns from sequential traffic data [11, 15]. The present study contributes to this literature by integrating optimized feature fusion with hybrid CNN-LSTM learning, which improved the detection of both known and unknown attack behaviors.

The strong performance of the proposed method on the BoT-IoT dataset is particularly significant because this dataset contains diverse and realistic attack scenarios associated with IoT and cloud infrastructures. The model achieved high F1-score values across all attack categories, indicating a balanced relationship between precision and recall. This finding suggests that the proposed framework maintained high detection capability while simultaneously minimizing classification errors. Previous studies have emphasized that intrusion detection in IoT-based cloud systems is especially challenging because of traffic heterogeneity, large-scale data generation, and the presence of stealthy attacks [2, 5]. Other studies have also demonstrated that DDoS attacks in smart grids, SDN environments, and lightweight IoT networks require adaptive and robust learning architectures capable of generalizing across multiple attack patterns [24, 25, 27]. The results of the present study support these observations and indicate that ensemble feature fusion combined with CNN-LSTM learning provides a scalable and adaptive solution for such environments.

The convergence behavior observed during optimization further supports the effectiveness of the proposed framework. The hybrid optimization approach demonstrated stable convergence behavior and avoided premature stagnation during feature selection. This finding is consistent with previous research showing that hybrid metaheuristic methods generally outperform standalone optimization algorithms because they improve the balance between exploration and exploitation within the search space [16, 42]. Studies using enhanced optimization strategies in intrusion detection systems similarly reported improved convergence stability and classification performance when multiple optimization mechanisms were combined [17, 18]. Therefore, the convergence stability observed in the current study likely contributed to the quality of the final selected features and the overall robustness of the proposed model.

The comparison analysis with previous methods also demonstrated the superiority of the proposed framework. Traditional deep learning models and machine learning approaches generally achieved accuracies between 95% and 97%, whereas the proposed method achieved accuracies above 99% on both benchmark datasets. These findings are consistent with recent studies suggesting that hybrid and ensemble learning methods outperform conventional standalone models in DDoS detection tasks [40, 42]. Similarly, optimization-based deep learning frameworks have been reported to improve attack classification capability in cloud and IoT systems [23, 38]. The present study strengthens this evidence by demonstrating that combining multiple metaheuristic algorithms with ensemble feature fusion and CNN-LSTM classification can produce highly accurate and generalized intrusion detection systems.

Another interpretation of the results relates to the complementary role of spatial and temporal learning within

the proposed architecture. CNN layers extracted local traffic patterns and structural feature relationships, whereas LSTM layers modeled sequential and time-dependent attack behaviors. DDoS attacks are inherently temporal because attack traffic often evolves dynamically over time. Therefore, using a purely static classifier may fail to capture sequential dependencies. Previous studies have emphasized the importance of temporal learning in modern intrusion detection systems [10, 32]. The findings of the current study further confirm that integrating CNN and LSTM structures improves the capability of the model to capture multidimensional attack behaviors and enhances overall classification performance.

The results also demonstrate the importance of preprocessing strategies such as normalization, one-hot encoding, and data balancing. The use of SMOTE balancing contributed to improved minority class recognition and prevented the classifier from becoming biased toward dominant classes. This finding is consistent with previous literature indicating that data imbalance is one of the primary challenges in intrusion detection datasets [6, 36]. Studies on machine learning-based DDoS detection have similarly shown that preprocessing and feature engineering strongly influence model reliability and detection accuracy [8, 43]. Therefore, the high classification performance observed in the present study can also be partially attributed to the effective preprocessing pipeline used before optimization and classification.

In addition, the findings support the growing shift from traditional centralized intrusion detection toward adaptive and intelligent cybersecurity frameworks. Recent studies on adaptive transfer learning, federated learning, and adversarial neural networks have argued that modern DDoS detection systems must be flexible, scalable, and capable of adapting to evolving attack patterns [33, 34, 37]. The proposed framework contributes to this emerging direction by integrating adaptive feature selection and deep representation learning into a unified architecture. The ability of the model to maintain high accuracy across multiple datasets suggests that the framework possesses strong generalization capability and can potentially be adapted to real-world cloud and IoT infrastructures.

Furthermore, the current findings reinforce previous surveys and comprehensive reviews that identified hybridization as a key future direction in DDoS detection research [1, 39]. Survey studies on machine learning and deep learning techniques for DDoS detection have repeatedly emphasized that no single model is sufficient to handle the diversity and complexity of modern attacks [7, 28]. Instead, integrated approaches that combine feature engineering, optimization, and deep learning are more likely to provide reliable and scalable solutions. The present study supports this perspective by empirically demonstrating that the combination of ensemble feature fusion and CNN-LSTM learning substantially improves intrusion detection performance.

Overall, the results indicate that the proposed ensemble feature fusion framework based on multiple metaheuristic optimization algorithms and hybrid CNN-LSTM learning provides a highly effective solution for DDoS attack detection in cloud computing environments. The framework achieved high classification accuracy, reduced false alarm rates, improved attack recognition capability, and demonstrated strong generalization across benchmark datasets. These findings highlight the importance of integrating optimized feature selection, feature fusion, and deep temporal-spatial learning for improving cybersecurity systems in cloud and IoT infrastructures.

One limitation of the present study is that the experiments were conducted primarily on benchmark datasets, including NSL-KDD and BoT-IoT, which may not fully capture the complexity and continuously evolving nature of real-world network traffic. In addition, although the proposed hybrid framework achieved high accuracy, the integration of multiple metaheuristic algorithms and deep learning structures increased computational complexity and training time. Another limitation is that the model was evaluated mainly in offline conditions rather than in fully operational real-time cloud environments. Therefore, the practical deployment performance of the framework under extremely large-scale and continuously changing traffic conditions requires further investigation.

Future research should evaluate the proposed framework on additional large-scale and real-world cybersecurity datasets collected from operational cloud and IoT infrastructures. Further studies may also investigate lightweight optimization techniques and model compression strategies to reduce computational overhead and improve real-time deployment capability. In addition, integrating transfer learning, federated learning, explainable artificial intelligence, and adversarial defense mechanisms could improve model adaptability, interpretability, and robustness against emerging cyber threats. Future work may also explore transformer-based architectures and self-supervised learning approaches for improving sequential traffic analysis and attack generalization.

From a practical perspective, the proposed framework can be integrated into cloud security monitoring systems, IoT gateways, software-defined networking infrastructures, and real-time intrusion detection platforms to improve cyberattack detection capability. Organizations operating large-scale cloud services may benefit from the high detection accuracy and reduced false alarm rate of the model, which can improve operational efficiency and reduce manual security analysis costs. The proposed ensemble feature fusion approach may also assist cybersecurity administrators in selecting more informative traffic attributes for monitoring and anomaly detection. Overall, the framework provides a scalable and practical foundation for improving the resilience of cloud and IoT infrastructures against evolving DDoS attacks.

## Authors' Contributions

Authors equally contributed to this article.

## Acknowledgments

Authors thank all participants who participate in this study.

## Declaration of Interest

The authors report no conflict of interest.

## Funding

According to the authors, this article has no financial support.

## Ethical Considerations

All procedures performed in this study were under the ethical standards.

## References

[1] M. A. Alarqan, Z. F. Zaaba, and A. Almomani, "Detection mechanisms of DDoS attack in cloud computing environment: A survey," in *Advances in Cyber Security: First International Conference, ACeS 2019, Penang, Malaysia, July 30-August 1, 2019, Revised Selected Papers 1*, 2020: Springer Singapore, pp. 138-152, doi: 10.1007/978-981-15-2693-0_10.

[2] Z. R. Alashhab, M. Anbar, M. M. Singh, I. H. Hasbullah, P. Jain, and T. A. Al-Amiedy, "Distributed denial of service attacks against cloud computing environment: Survey, issues, challenges and coherent taxonomy," *Applied Sciences,* vol. 12, no. 23, p. 12441, 2022, doi: 10.3390/app122312441.

[3] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Computer Science Review,* vol. 39, p. 100332, 2021, doi: 10.1016/j.cosrev.2020.100332.

[4] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," *IEEE Access,* vol. 9, pp. 42236-42264, 2021, doi: 10.1109/ACCESS.2021.3062909.

[5] M. K. Hasan, A. K. M. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah, and B. Pandey, "DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," *Energy Reports,* vol. 9, pp. 1318-1326, 2023, doi: 10.1016/j.egyr.2023.05.184.

[6] L. Pattnaik, S. Satpathy, B. K. Paikaray, and P. K. Swain, "DDoS analysis using machine learning: Survey, issues, and future directions," *International Journal of Business Continuity and Risk Management,* vol. 14, no. 1, pp. 57-76, 2024, doi: 10.1504/IJBCRM.2024.137242.

[7] U. A. Butt *et al.*, "A review of machine learning algorithms for cloud computing security," *Electronics,* vol. 9, no. 9, p. 1379, 2020, doi: 10.3390/electronics9091379.

[8] D. Soni and N. Kumar, "Machine learning techniques in emerging cloud computing integrated paradigms: A survey and taxonomy," *Journal of Network and Computer Applications,* vol. 205, p. 103419, 2022, doi: 10.1016/j.jnca.2022.103419.

[9] P. Singh Samom and A. Taggu, "Distributed denial of service (DDoS) attacks detection: A machine learning approach," in *Applied Soft Computing and Communication Networks: Proceedings of ACN 2020*, 2021: Springer Singapore, pp. 75-87, doi: 10.1007/978-981-33-6173-7_6.

[10] A. Dawoud, O. A. Sianaki, S. Shahristani, and C. Raun, "Internet of Things Intrusion Detection: A Deep Learning Approach," in *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2020: IEEE, pp. 1516-1522, doi: 10.1109/SSCI47803.2020.9308293.

[11] T. Stefanos, L. Thomas, and R. Konstantinos, "Deep Learning in IoT Intrusion Detection," *Journal of Network and Systems Management,* vol. 30, 2022, doi: 10.1007/s10922-021-09621-9.

[12] S. Aktar and A. Y. Nur, "Towards DDoS attack detection using deep learning approach," *Computers & Security,* vol. 129, p. 103251, 2023, doi: 10.1016/j.cose.2023.103251.

[13] E. Omar, S. Eman, M. Mohamed, and E. Karim, "EIDM: Deep learning model for IoT intrusion detection systems," *Journal of Supercomputing,* vol. 79, pp. 13241-13261, 2023, doi: 10.1007/s11227-023-05197-0.

[14] W. Xiao, D. Lie, and Y. Guang, "A network intrusion detection system based on deep learning in the IoT," vol. 80, pp. 24520-24558, 2024, doi: 10.1007/s11227-024-06345-w.

[15] K. Yesi Novaria, N. Siti, S. Deris, and Y. S. Bhakti, "An end-to-end intrusion detection system with IoT dataset using deep learning with unsupervised feature extraction," *International Journal of Information Security,* pp. 1619-1648, 2024, doi: 10.1007/s10207-023-00807-7.

[16] P. Agrawal, H. F. Abutarboush, T. Ganesh, and A. W. Mohamed, "Metaheuristic algorithms on feature selection: A survey of one decade of research (2009-2019)," *IEEE Access,* vol. 9, pp. 26766-26791, 2021, doi: 10.1109/ACCESS.2021.3056407.

[17] S. Velliangiri, P. Karthikeyan, and V. Vinoth Kumar, "Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks," *Journal of Experimental & Theoretical Artificial Intelligence,* vol. 33, no. 3, pp. 405-424, 2021, doi: 10.1080/0952813X.2020.1744196.

[18] A. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness, and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," *IEEE Access,* vol. 9, pp. 123448-123464, 2021, doi: 10.1109/ACCESS.2021.3109081.

[19] 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,* vol. 53, p. 102532, 2020, doi: 10.1016/j.jisa.2020.102532.

[20] G. S. Kushwah and V. Ranga, "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," *Computers & Security,* vol. 105, p. 102260, 2021, doi: 10.1016/j.cose.2021.102260.

[21] G. S. Kushwah and V. Ranga, "Distributed denial of service attack detection in cloud computing using hybrid extreme learning machine," *Turkish Journal of Electrical Engineering and Computer Sciences,* vol. 29, no. 4, pp. 1852-1870, 2021, doi: 10.3906/elk-1908-87.

[22] Y. Sanjalawe and T. Althobaiti, "DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning," *Computers, Materials & Continua,* vol. 75, no. 2, 2023, doi: 10.32604/cmc.2023.037386.

[23] E. S. Gsr, R. Ganeshan, I. D. J. Jingle, and J. P. Ananth, "FACVO-DNFN: Deep learning-based feature fusion and Distributed Denial of Service attack detection in cloud computing," *Knowledge-Based Systems,* vol. 261, p. 110132, 2023, doi: 10.1016/j.knosys.2022.110132.

[24] S. A. Khanday, H. Fatima, and N. Rakesh, "Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks," *Expert Systems with Applications,* vol. 215, p. 119330, 2023, doi: 10.1016/j.eswa.2022.119330.

[25] A. K. M. A. Habib, M. K. Hasan, R. Hassan, S. Islam, R. Thakkar, and N. Vo, "Distributed denial-of-service attack detection for smart grid wide area measurement system: A hybrid machine learning technique," *Energy Reports,* vol. 9, pp. 638-646, 2023, doi: 10.1016/j.egyr.2023.05.087.

[26] S. V. J. Rani *et al.*, "Detection of DDoS attacks in D2D communications using machine learning approach," *Computer Communications,* vol. 198, pp. 32-51, 2023, doi: 10.1016/j.comcom.2022.11.013.

[27] V. Hnamte, A. A. Najar, N.-N. Hong, J. Hussain, and M. N. Sugali, "DDoS attack detection and mitigation using deep neural network in SDN environment," *Computers & Security,* vol. 138, p. 103661, 2024, doi: 10.1016/j.cose.2023.103661.

[28] D. Javaheri, S. Gorgin, J.-A. Lee, and M. Masdari, "Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives," *Information Sciences,* vol. 626, pp. 315-338, 2023, doi: 10.1016/j.ins.2023.01.067.

[29] M. A. Bouke, A. Abdullah, S. H. Alshatebi, M. T. Abdullah, and H. El Atigh, "An intelligent DDoS attack detection tree-based model using Gini index feature selection method," *Microprocessors and Microsystems,* vol. 98, p. 104823, 2023, doi: 10.1016/j.micpro.2023.104823.

[30] A. Fathima, G. Shree Devi, and M. Faizaanuddin, "Improving distributed denial of service attack detection using supervised machine learning," *Measurement: Sensors,* vol. 30, p. 100911, 2023, doi: 10.1016/j.measen.2023.100911.

[31] P. K. Kishore, S. Ramamoorthy, and V. N. Rajavarman, "ARTP: Anomaly based real time prevention of Distributed Denial of Service attacks on the web using machine learning approach," *International Journal of Intelligent Networks,* vol. 4, pp. 38-45, 2023, doi: 10.1016/j.ijin.2022.12.001.

[32] N. S. Musa, N. M. Mirza, S. H. Rafique, A. Abdallah, and T. Murugan, "Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks-Current Research Solutions," *IEEE Access,* 2024, doi: 10.1109/ACCESS.2024.3360868.

[33] M. B. Anley, A. Genovese, D. Agostinello, and V. Piuri, "Robust DDoS attack detection with adaptive transfer learning," *Computers & Security,* vol. 144, p. 103962, 2024, doi: 10.1016/j.cose.2024.103962.

[34] R. Doriguzzi-Corin and D. Siracusa, "FLAD: Adaptive federated learning for DDoS attack detection," *Computers & Security,* vol. 137, p. 103597, 2024, doi: 10.1016/j.cose.2023.103597.

[35] A. V. Kachavimath and D. G. Narayan, "A deep learning-based framework for distributed denial-of-service attacks detection in cloud environment," in *Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1*, 2021: Springer Singapore, pp. 605-618, doi: 10.1007/978-981-33-6977-1_44.

[36] Z. Liu, B. Xu, B. Cheng, X. Hu, and M. Darbandi, "Intrusion detection systems in the cloud computing: A comprehensive and deep literature review," *Concurrency and Computation: Practice and Experience,* vol. 34, no. 4, p. e6646, 2022, doi: 10.1002/cpe.6646.

[37] A. Mustapha *et al.*, "Detecting DDoS attacks using adversarial neural network," *Computers & Security,* vol. 127, p. 103117, 2023, doi: 10.1016/j.cose.2023.103117.

[38] S. Balasubramaniam *et al.*, "Optimization enabled deep learning-based DDoS attack detection in cloud computing," *International Journal of Intelligent Systems,* vol. 2023, 2023, doi: 10.1155/2023/2039217.

[39] Y. B. Sanap and P. Aher, "A Comprehensive Survey On Detection and Mitigation of DDoS Attacks Enabled with Deep Learning Techniques in Cloud Computing," in *2023 6th International Conference on Advances in Science and Technology (ICAST)*, 2023: IEEE, pp. 149-154, doi: 10.1109/ICAST59062.2023.10454990.

[40] U. Shahid, M. Z. Hussain, M. Z. Hasan, A. Haider, J. Ali, and J. Altaf, "Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning," *IEEE Access,* 2024, doi: 10.1109/ACCESS.2024.3442529.

[41] S. K. Dash *et al.*, "Enhancing DDoS attack detection in IoT using PCA," *Egyptian Informatics Journal,* vol. 25, p. 100450, 2024, doi: 10.1016/j.eij.2024.100450.

[42] R. Tavoli, E. Rezvani, and M. Hosseini Shirvani, "An Efficient Hybrid Approach Based on Deep Learning and Stacking Ensemble Using the Whale Optimization Algorithm for Detecting Attacks in IoT Devices," *Engineering Reports,* vol. 7, no. 9, p. e70338, 2025, doi: 10.1002/eng2.70338.

[43] T. H. H. Aldhyani and H. Alkahtani, "Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments," *Sensors,* vol. 22, no. 13, p. 4685, 2022, doi: 10.3390/s22134685.