A Bio-Inspired Feature Selection and Ensemble Classification for DDoS Detection in Cloud

Aditya Kumar Shukla * and Ashish Sharma

Department of Computer Engineering and Applications, GLA University, Post Ajhai, Mathura, India
Email: uraditya@gmail.com (A.K.S.); ashishs.sharma@gla.ac.in (A.S.)
*Corresponding author

***Abstract*—The investigation of cloud computing is becoming more popular in both the business world and the academic world. The use of cloud computing presents many opportunities for growth and improvement for cloud service providers as well as end users. Due to the dramatic increase in demand for cloud computing, data security has emerged as a primary area of concern. There have been a great deal of risks that make the use of cloud computing more difficult. Detecting distributed denial of service attacks is a key bottleneck in the cloud technology industry. The development of an efficient attack detection technique is a challenging endeavor because of the intricate interactions between nonlinear interruption activities, aberrant system traffic behavior, and other variables. As a result, establishing preventive solutions against these threats is critical for the broad adoption of cloud computing. This work presented a combination of the bio-inspired feature-choosing method Particle Swarm Optimization (PSO) with the classification methods Logistic Regression, Gaussian, and Random Forest as an ensemble technique for Distributed Denial of Service (DDoS) attack detection. The Bio-Inspired Feature-Selection and Ensemble-Classification DDoS-Detection (BIFSED) output is finalized by combining the results of each categorization technique. To determine the final DDoS classification, we employed a certain threshold and a vote of simple majority. The performance results with the NSL-Knowledge Discovery-Dataset (NSL-KDD) dataset showed that the BIFSED approach, with thirteen characteristics and ensemble techniques, outperforms a complete set of features and different classification methods in the literature using logistic regression, Gaussian, and random forest classification methods.**

***Keywords*—Distributed Denial of Service (DDoS) detection, ensemble classification, Particle Swarm Optimization (PSO), NSL-Knowledge Discovery-Dataset (NSL-KDD)**

I. Introduction

Nowadays, cloud computing (Fig. 1) is counted as the greatest ground-breaking innovation in the history of the information technology industry [1]. This was made possible by improvements in modern computing paradigms including parallel computing, grid computing, distributed computing, and others [2]. Users can simply scale up or down clusters based on their expectations with the least amount of engagement from third parties thanks to these technical solutions, which enable consumers to seamlessly incorporate communication lines into a system of computer resources [3].

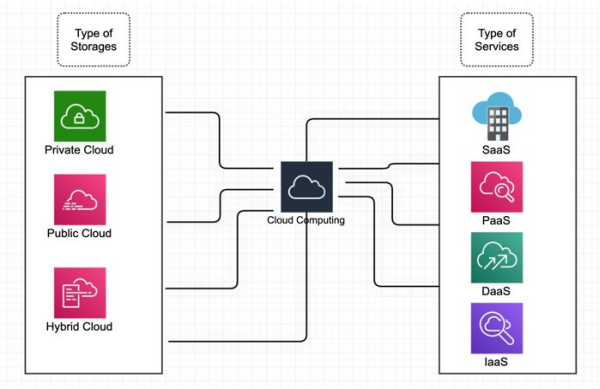

Fig. 1. High level view of cloud computing.

Even though cloud technology is still in its infancy, there are several flaws that bad individuals or hackers may exploit [4, 5]. Most clients worry about the frequent security breaches in cloud computing [6].

A denial-of-service attack seeks to overwhelm a target system such that it fails to perform its intended function as well as render it inaccessible to legitimate users [7–9]. Due to the potential effect of even a single cloud server on a large user base, these assaults are especially harmful to cloud computing systems [10–12]. Cloud systems by increasing their processing capacity increase the number of VMs and service instances when there is a lot of work to be completed [13]. The cloud architecture doesn't help when you're trying to thwart a cyber-assault. A slowdown in the cloud infrastructure has finally been seen, making it hard for genuine users to access their cloud services. If hackers target a large number of cloud-based services with more zombie machines, DDoS attacks might become much more dangerous.

Cloud computing necessitates a unique method of detecting and preventing assaults. DDoS attacks take many forms, and the client's network connectivity or capacity is the most common target. Bandwidth attacks negatively impact network performance since attackers consume all available network bandwidth and delay or prevent the fulfilment of user requests.

Manuscript received December 14, 2023; revised February 7, 2024; accepted February 26, 2024; published October 15, 2024.

Connection assaults, similar to DoS attacks, flood the victim's server with repeated application-layer requests, depleting all available resources. As a result, the server no longer handles legitimate user requests. In a flood attack, the intruder bombards the target with a large number of packets in a continuous flow, exhausting all of the victim's capacity and resources. A vulnerability attack occurs when a hostile party sends prepared messages to the victim's system in an attempt to overwhelm it. DDoS attacks often include flooding the targeted system or network with traffic from multiple directions.

Distributed denial of service attacks originate from Internet-connected computer systems. A hacker may take remote control of a server in one of these networks and spread malware across it using special software. A botnet is a group of bots, while a single bot is a bot [14]. After a botnet is set up, an attack may be launched by delivering orders to every bot individually. When a botnet assaults (Fig. 2) a server or network, each bot in the network sends out a query to the interface, causing a denial of service by flooding the system or connection. Each bot is a real computer is connected to the Internet, which means it may be difficult to distinguish malicious from benign data [15]. Website or service delays or outages are the most subtle signs of a Distributed Denial of Service (DDoS) attack. However, because a number of factors, such as traffic volume, may produce similar productivity concerns, greater attention is clearly required. Some of these DDoS attack indicators may be detected by traffic analytics software [16]. Weird or irregular traffic patterns, including peaks at uncommon times or odd layouts [17].

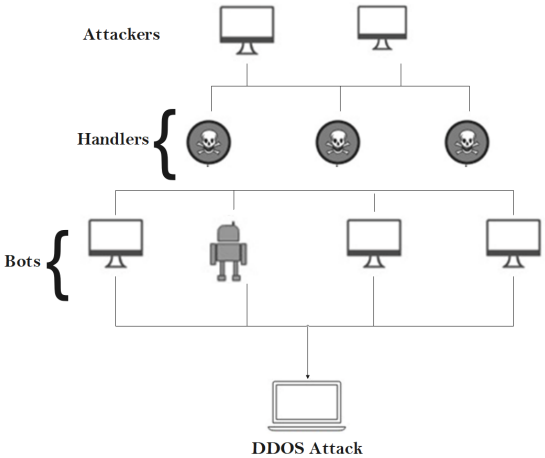

Fig. 2. DDoS attack.

The most severe difficulty in current DDoS attack tactics is identifying the correct collection of network and traffic data characteristics while maintaining appropriate detection accuracy. When the application is decentralized and deployed internationally, the network traffic data may have various aspects with redundant information, making the task more difficult. For this study, we examined standard data from a military network. A wide range of intrusions are repeated in the context of a military network, and there are numerous independently certified data features. So, the goal is to extract informative characteristics for DDoS detection in the cloud and then train those features into the proposed algorithm. Performance measures are compared to existing algorithms to show how the new technique compares. Network traffic data sets naturally include repetitious or nonessential characteristics, which result in unreasonable training and classification time. Important features mean identifying features from the dataset, aiming to improve prediction accuracy and reduce computational complexity. Features can be categorized into the following categories:

- Independent features;
- Correlated features;
- Redundant features;
- Feature with Information;
- Feature with no information;
- Weak features.

In recent research, many network datasets are being used with multiple characteristics because network data has multiple dimensions by nature. This "heightened dimensionality" makes the classifier learning procedure difficult because not all characteristics are applicable to the type labels and usually contain duplicated data, reducing the accuracy of attack detection. Such data usually requires feature selection to remove irrelevant and duplicated features. So, the analysis gap indicates that a combination of characteristic-selecting approaches can improve classifier performance by specifying characteristics that are insufficient as individuals but powerful as a group, extracting repetitive characteristics, and defining characteristics that have a high correlation with the result type.

Contribution of this research paper:

1. The goal of this work is to use an ensemble learning classifier to extract relevant features or minimize the characteristic group while improving or preserving classification accuracy. The NSL-KDD DDoS detection model dataset, which has 41 features, is utilized to assess the efficacy of our proposed BIFSED approach.
2. In this paper, we introduce BIFSED, a DDoS attack outpour classification technique for reliably and quickly determining attack flows in network data. First, BIFSED selects the best features using a bio-inspired feature selection technique to filter characteristics and select the most informative ones. Second, ensemble learning algorithms will be used to classify the DDoS attacks. Finally, a majority vote is used to weight the final classification.
3. To establish the viability of the presented strategy, this study compares the proposed method to other algorithms based on performance metrics. The PSO-based ensemble learning method is quite effective in witnessing DDoS attacks in cloud computing infrastructures.

II. Related Works

This section provides a full justification for the correlation with previous findings. We examined the methodology of contemporary study, as well as its

benefits and limitations. In this literature review, several studies employing diverse methodologies for attack detection in network security are explored.

The research conducted by Narayanasami *et al.* [18] leveraged the BAT method in tandem with SVM for classification. While the BAT method showcased excellence in the realm of feature selection, the resultant accuracy from SVM classification fell short of initial expectations. This highlights the delicate balance between feature selection methodologies and the downstream classification algorithms.

In the study presented by Shone *et al. [*19], an auto-encoder was employed for intricate feature identification, coupled with deep learning for precise attack categorization. The deliberate choice of a non-symmetric classification aimed to mitigate model complexity. However, this strategic decision had repercussions on the detection effectiveness, particularly for unauthorized access attacks.

Virupakshar *et al.* [20] introduced an innovative socket programming approach to monitor network traffic, effectively contributing to the blockage of attacks at the network layer. Despite this achievement, the study revealed limitations in its coverage of a broader range of attacks, leaving certain vulnerabilities unaddressed.

The utilization of flow control techniques and random forest in [21] demonstrated success in minimizing erroneous alerts. However, the absence of support for multilayer DDoS mitigation showcased the need for a more comprehensive defense strategy in the face of evolving cyber threats.

The combination of an autoencoder and DNN in [22] for attack identification tackled the challenges of unbalanced, noisy data. Yet, the considerable computational complexity underscored the ongoing trade-off between model sophistication and resource demands.

Velliangiri *et al.* [23] explored the implementation of the DBN technique for DDoS detection, offering a viable solution for handling crucial information in cloud platforms. However, the observed accuracy in classification did not align with the anticipated outcomes, prompting further inquiry into refining the model.

The imperative role of regression analysis in ML model development was underscored by Sambangi *et al.* [24], emphasizing the model's significance in predictive purposes. However, the study's limited examination using one-day log files brought attention to the constraints inherent in the dataset.

The application of the CNN–LSTM method in [25] for attack detection in cloud data exhibited effectiveness with a standard dataset. Yet, the computational workload associated with this methodology raised questions about scalability and resource consumption.

Ahmed *et al.* [26] introduced a comprehensive approach with proactive traffic anomaly detection and sophisticated malware prevention techniques. While the multilayer technique demonstrated efficacy in risk limitation, the study highlighted potential performance variations at different layers, influencing the overall effectiveness.

Cil *et al.* [27] showcased the implementation of a deep neural network as a threat learning model, operating efficiently even with a small packet sample. However, the reliance on an outdated dataset emphasized the need for contemporary data sources to ensure the model's relevance.

The CNN-based technique employed in [28] for threat identification outperformed other deep learning methods. Nevertheless, the study's limitation in considering multiple categories of attack types hinted at the complexity of comprehensively covering diverse cyber threats.

Hezavehi *et al.* [29] proposed a holistic approach with third-party auditors, a zone-divider, and a protocol for anomaly recognition, safeguarding cloud service providers from security risks. However, the investigation's restriction to a specific dataset pointed to the need for broader and more diverse datasets for comprehensive evaluations.

In Ref. [30], the combination of CNN and an auto-encoder proved effective for identifying assaults, particularly in the context of low-rate-DDoS detection. Nonetheless, the computational complexity posed a significant challenge, necessitating further optimization strategies to balance accuracy and resource efficiency.

Our study of earlier research revealed that hybrid algorithms perform better, with the main problem being the adoption of an appropriate feature learning method in conjunction with a classification. The majority of research papers that employed feature extraction alone for classification did not yield accurate results and instead suggested extremely complicated solutions. In order to obtain a highly accurate outcome with a novel approach, we employed a natural method for feature extraction with ensemble learning in our proposal.

III. METHODOLOGIES

One of the biggest obstacles to cloud computing is spotting DDoS attacks. It is important to note that the features of the interruption activities, such as their nonlinearity and the unusual behavior of the system's traffic, make an attack detection mechanism very difficult to implement. As a result, building safeguards against these threats is critical for the general adoption of cloud-based computing.

Network traffic data sets generally contain repetitious or nonessential characteristics, which result in overblown training and classification duration. Important features mean here to identify features from the dataset, with the goal of enhancing the ability and accuracy of prediction and decreasing computational intricacy.

"High dimensionality" of network data makes the classifier training procedure complicated because not all segments are suitable for the type labels and usually include repetitive information. Such data naturally requires characteristic preference to filter out unessential and duplicative characteristics.

This study introduced an ensemble strategy for DDoS attack detection that integrates a bio-inspired feature selection method with the classification techniques of

Gaussian, Random Forest, and logistic regression. In order to create an ensemble strategy for DDoS assault detection, this work combined the bio-inspired feature-choosing method with the classification techniques of Gaussian, Random Forest, and Logistic Regression. The final result of the BIFSED is obtained by combining the outputs of every classification method. We used a simple majority vote to determine the final DDoS classification using a chosen threshold. The NSL-KDD dataset performance results show that the BIFSED strategy, with thirteen characteristics and ensemble techniques, outperforms a full set of features and several classification methods, such as Random Forest, Gaussian, and logistic regression classification.

A. Resource Requirements

The proposed model was constructed using pyCharm, which was operating on a computer running 64-bit Mac OS 13.4, x64, and equipped with an Intel(R) CORE(TM) i9 CPU @ 2.4GHz, 8 cores, and 32 GB of RAM.

B. Benchmark Datasets

NSL-KDD Data set was used here to execute, test and verify the proposed method. NSL-KDD (Table I) is labelled benchmark database for research purposes.

TABLE I. DATASET

Data Type	Total Records	Attacks Data
Training Set	3,925,650 Dataset	262,178 Attacks
Testing Set	250,436 Dataset	29,378 Attacks

This database contains a comprehensive set of 41 independently validated data features that represent a wide range of invasions reproduced in the context of a military network.

C. Data Pre-processing

Before training the data to the BIFSED Model, certain preparation processes must be accomplished.

The Synthetic Minority Oversampling Technique (SMOTE) method was used here for feature balancing in the BIFSED Model with the NSL-KDD data set. If two minority instances already exist, SMOTE can combine them to make a new one (Fig. 3). Using linear interpolation, it generates hypothetical data for the underrepresented group. These synthetic training are selected at random from among the k-nearest neighbors of each minority class example. The data is reconstructed after oversampling and can then be analyzed using different types of classification methods.

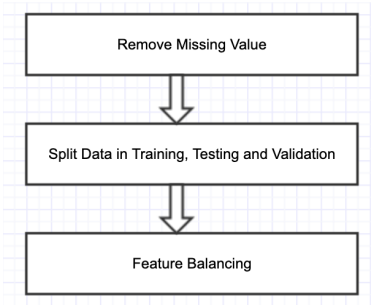

Fig. 3. Data processing steps in BIFSED.

D. BIFSED Model

The suggested BIFSED Model (Fig. 4) is an attack using a DDoS flow categorization system that identifies attack flows in network data accurately and fast. First, BIFSED selects the most informative features using the bio-inspired feature selection method (PSO) to filter features. Second, to apply ensemble learning methods to classify the DDoS attacks. Finally, an finally a majority voting is applied to weight the final classification (Fig. 5).

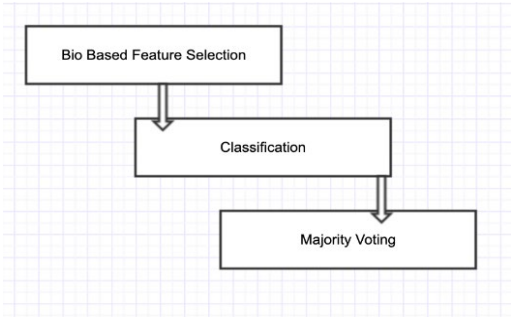

Fig. 4. High level BIFSED model.

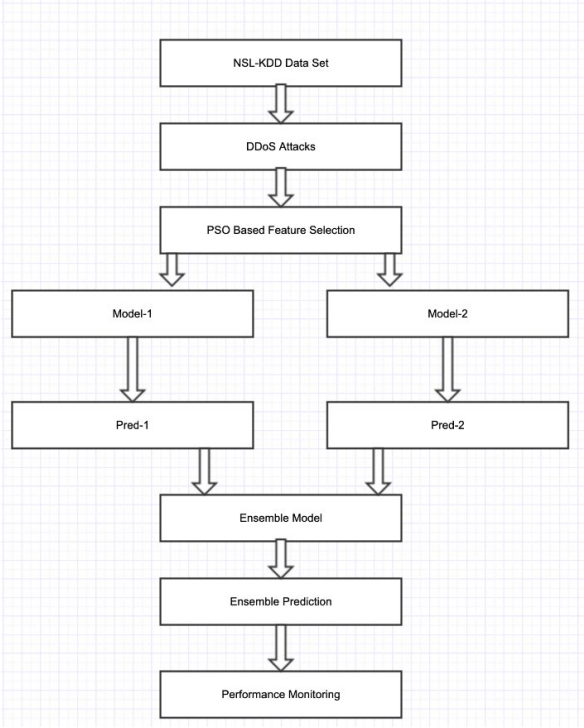

Fig. 5. Flow chart of the proposed BIFSED model.

E. Bio-Inspired Feature Selection Method (PSO)

Features are selected based on a bio-inspired algorithm-PSO (Fig. 6). Classification of high-dimensional (i.e, thousands of extents) data generally needs Characteristic Selection (CS) as a pre-processing stage to decrease the dimensionality. PSO is a method for global search that works well and efficiently. Due to superior representation, the capacity to explore huge areas, being less computationally costly, being simpler to construct, and needing fewer parameters, it is a suitable technique to handle feature selection difficulties. The following is the formula for PSO-based feature selection:

$$x_{id}^{t+1} = x_{id}^{t} + v_{id}^{t+1}$$

$$v_{id}^{t+1} = w \times v_{id}^{t} + c_1 \times r_{1i}(p_{id} - x_{id}^{t}) + c_2 \times r_{2i} \times (p_{gd} - x_{id}^{t})$$

where $d \in D$ is the d^{th} dimension of our search space. In PSO, t is the current iteration, x_{id}^{t} is the particle's current location, as well as v_{id}^{t} is the particle's current velocity in d in the t^{th} iteration. w is the inertia weight, which allows velocities from the previous iteration to have a controlling influence on the current one, while c_1 as well as c_2 are the learning rates. r_{1i} as well as r_{2i} are simply random numbers that are uniformly distributed in the range [0, 1], and p_{id} as well as p_{gd} are the p_{best} and g_{best} in the d.

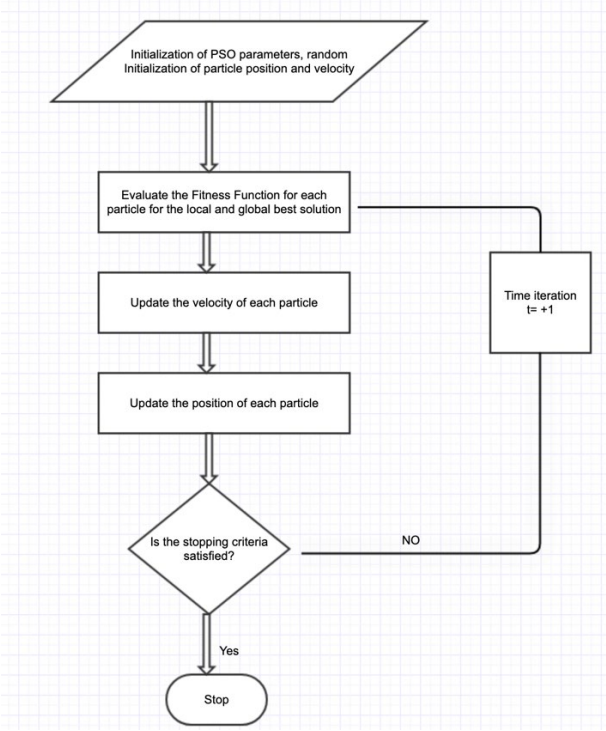

Fig. 6. PSO algorithm flowchart.

F. Classification Algorithms in BIFSED Model

The focus of this research is to introduce a novel solution for classifying the identification of Denial of service attacks and to mitigate these attacks effectively by using a hybrid model of machine learning technologies. Using a combination of ML models and applying ensemble learning to get the best accuracy for attack detection, and this classification can be further used in the mitigation of attacks. Ensemble techniques are so termed because they utilize a collection of results to arrive at a final result.

The process of random forest classification is as follows: the two-child policy nodes (binary tree):

$$ni_j = w_j C_j - w_{left(j)} C_{left(j)} - w_{right(j)} C_{right(j)}$$

where the impurities level of node j is equal to the expression C_j left(j) = Splitting a child node from the left on node j, ni_j equals the weight placed on node j. right(j) is the child node formed by the right split on node j. w_j denotes the weighted number of samples that made it to node j. After that, an evaluation of the significance of the each characteristic on a tree structure is carried out using the following standards.

$$fi_i = \frac{\sum_{j:node\ j\ splits\ on\ feature\ i} ni_j}{\sum_{k \in all\ nodes} ni_k}$$

ni sub(j) equals the weight placed on node j. the weight that should be given to feature I denoted by fi sub(i). The variables can then be standardized to be between 0 and 1 by dividing the entire sum of all characteristic position values by the entire sum of all correlation-based feature values.

$$normfi_i = \frac{fi_i}{\sum_{j \in all\ features} fi_j}$$

Values assigned to each category in continuous data are often assumed to follow a standard (or Gaussian) distribution. It is expected that the characteristics' probability is Sometimes assume variance is independent of Y (i.e., σi), or independent of Xi (i.e., σk) or both (i.e., σ).

$$P(x, y) = \frac{1}{\sqrt{2\pi\sigma_y^2}} \exp\left(-\frac{(x_i - \mu_y)^2}{2\sigma_y^2}\right)$$

The goal of logistic regression is to represent the issue as a modified linear regression model.

$$\hat{y} = \beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n$$

By mixing several models, ensemble learning may boost machine learning performance. When compared to using only one model, this strategy yields far more accurate predictions. The central concept is to educate a panel of experts (classifiers), who will then cast a final vote.

Hard voting/ majority voting (combined ensemble method)

In its simplest form, majority voting, or "hard voting", is the method most often used. The category with the most votes, *Nc(yt)*, will be chosen. Through averaging the results of all classifiers, we make a prediction for the y-class label.

$$\hat{y} = argmax(N_c(y_t^1), N_c(y_t^2), \ldots, N_c(y_t^n))$$

IV. Results and Discussions

The goal of this research is to present a novel strategy for classifying and mitigating Denial of Service attacks utilizing a hybrid model of machine learning technologies. Using a common and distinctive assault database that includes a wide range of data attributes and covers a wide range of invasions duplicated within the network's structure. Implement a novel approach to feature selection to determine all available correlations between data sets and compare the results with and without applying the feature selection process. It is also part of the overall architecture. Using a combination of ML models and applying ensemble learning to get the best accuracy for attack detection, this classification can be further used in the mitigation of attacks. Compare the proposed method

to other algorithms based on performance metrics. In this section, as evidence of the superiority of the suggested algorithms, we provide graphical representations of key performance indicators for both the proposed and state-of-the-art techniques. Additionally, the algorithms are contrasted with and without feature selection. Also, a comparison of the PCA components is evaluated for the proposed algorithm.

The confusion matrix for DDoS identification utilizing ensemble learning and feature selection is shown in the diagram above. The confusion matrix (Fig. 7) depicts two classifications, class 0 representing normal, and class 1 representing a DDoS attack. Our suggested model properly identified 2,316 times as a DDoS assault and accurately predicted 4,714 times as normal. There are some misclassifications that also occurred, in which the model predicted 141 at normal as a DDoS attack and 269 at a DDoS attack as normal.

Above Graph shows the ROC curve (Fig. 8) for our proposed model, it's a visual depiction of how well Ensemble learning works. In this, the AUC value is 0.944 it is greater than 0.5, so the model is highly recommendable for detecting DDoS attack.

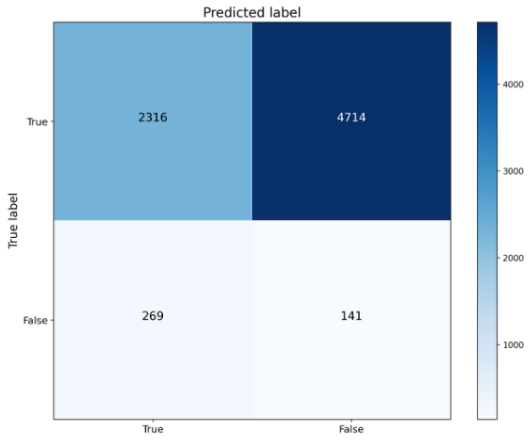

Fig. 7. Confusion matrix of DDoS detection result.

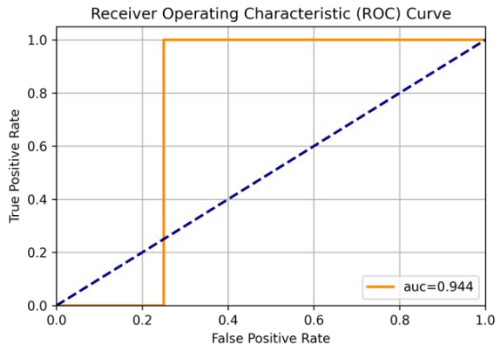

Fig. 8. ROC curve comparison of Ensemble classifier result.

The earlier figure displays the accuracy analysis of the four ways, with the suggested and present strategies plotted on the x-axis and the accuracy score plotted on the y-axis. The accuracy results illustrate the impact of feature selection on different classifiers (Fig. 9).

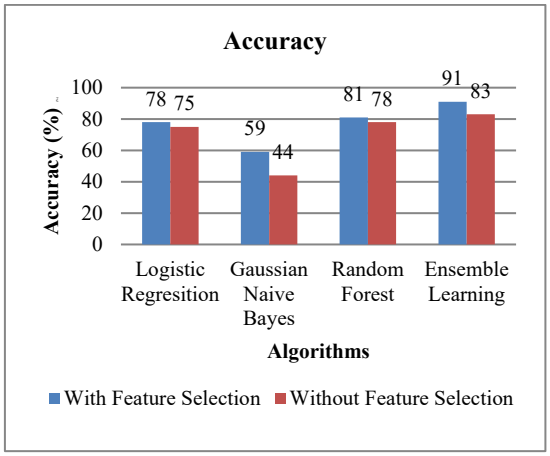

Fig. 9. Accuracy-score of ML algorithms and Ensemble method.

The new and current algorithms are on the x-axis, and the recall score is on the y-axis in the prior picture, which shows the recall analysis (Table IV) of four approaches. The results illustrate that feature selection generally enhances recall across various classifiers. (Fig. 10). When compared to other techniques, ensemble learning and picking features produce good outcomes.

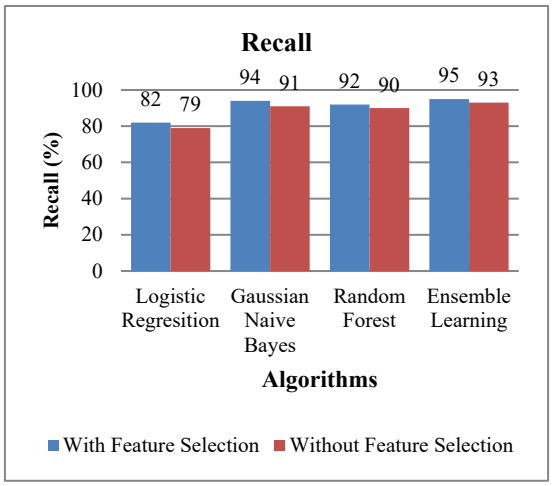

Fig. 10. Recall result of ML algorithms and Ensemble method.

The before mentioned graphic shows a precision study using four techniques, with the recommended and present techniques on the x-axis and the precision score on the y-axis. The results indicate that feature selection generally improves precision across different classifiers (Fig. 11). It may be stated that, when compared to other methods, ensemble learning with selected features produces effective outcomes.

The suggested and current algorithms are on the x-axis of the previous figure, which shows the F1-Score analysis of four methods, and the F1-Score result is on the y-axis. The F1-Scores demonstrate the impact of feature selection on model performance across different classifiers. Logistic regression shows a moderate improvement in F1-Score (Fig. 12). The voting classifier also showing good result with feature selection. Comparing ensemble learning using a selection of features to other methods, it can be determined that it yields efficient outcomes.

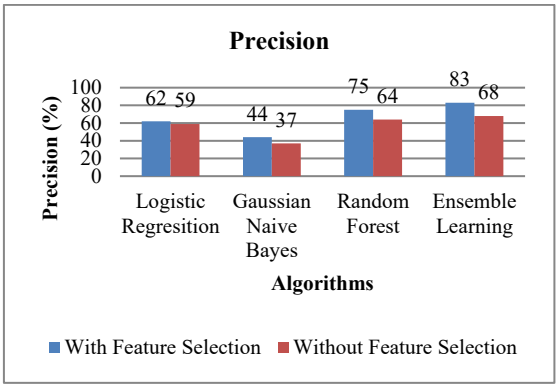

Fig. 11. Precision comparison of ML algorithms and Ensemble method.

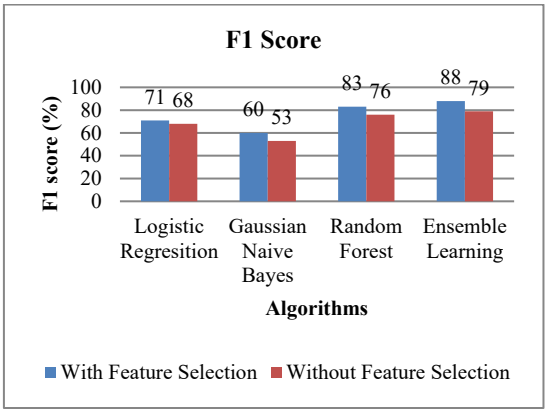

Fig. 12. F1-Score of ML algorithms and Ensemble method.

The outcomes for accuracy, precision, recall, and the F1-Score assessment for ensemble learning in three different scenarios are displayed above, along with parameter values (x-axis). The outcome of the analysis indicates that as the number of PCA components increases from 10 to 30, there is a slight fluctuation in the performance metrics (Fig. 13).

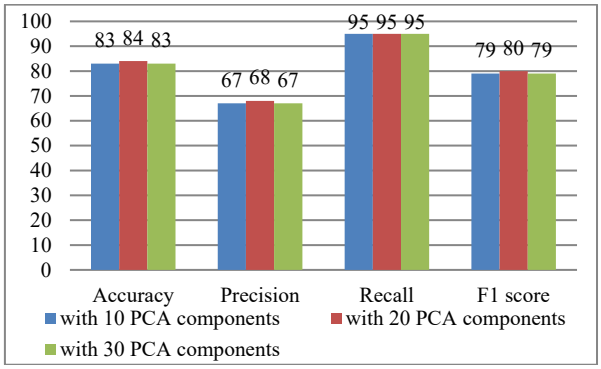

Fig. 13. Performance metrics with PCA result.

V. Conclusion

In this study, a novel technique is used to discover and choose specific elements of the dataset to detect denial-of-service attacks in cloud computing systems. Ensemble learning classification with feature selection is proposed to extract actionable features from the data as well as distinguish the attack. It is decided to use the NSL-KDD dataset, which includes features connected to the attack. We can separate the valuable features from the wider set of features using a PSO-based natural optimization technique. Within the extracted features, to identify DoS assaults, we choose a subset of characteristics and train the suggested model on them. To prove the viability of the proposed strategy, it is compared to other algorithms using the same performance parameters. PSO-based feature selection clearly favors high-priority features. As a result, DoS attacks need more targeted service characteristics. By comparing two situations with and without feature selection, several performance measures, including accuracy, sensitivity, and specificity, are compared against various current algorithms. The recommended solution outperforms the existing feature selection methods with a 91% accuracy rate compared to an 83% accuracy rate without feature selection. Without feature selection, the suggested method has a recall of 93%, whereas with it, it reaches 95%. Without feature selection, the suggested method only achieves 68% accuracy, but with it, it achieves 83%. The suggested approach achieves an F1-Score of 88% when feature selection is used and 79% when it is not. These figures show that the suggested approach is more effective than previous algorithms. The proposed algorithm is also compared with different (10, 20, 30) extracted PCA components. The results depict that the performance parameters are higher with 20 extracted features, which indicates that feature selection impacts the accuracy of the algorithm. Thus, it is concluded that the PSO-based ensemble learning method is quite effective in detecting DDoS assaults in cloud computing infrastructures.

Multiclass classifications may be used in the future for attacks that fall under different KDD and CSE-CIC-IDS 2022 attack categories. To enhance performance, the model can also be applied to other intrusion datasets. Future research could improve the method presented for spotting assaults in real-time traffic flows, with shorter detection times and less computer complexity when analyzing large real-time data sets. Future efforts will be directed towards suggesting a strategy for mitigating the consequences of identified DDoS assaults on the system in order to meet the crucial network security criterion of being able to accurately identify attack traffic and recover the system from attack. The paper's results may be applied to a variety of industries, including healthcare, industry, and national defense, which need sophisticated intrusion detection methods.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Aditya Kumar Shukla conducted the research and wrote the Paper. Ashish Sharma analyzed the data sets and reviewed the Papers. All authors had approved the final version.

References

[1] M. Jangjou and M. K. Sohrabi. "A comprehensive survey on security challenges in different network layers in cloud computing,"

Archives of Computational Methods in Engineering, vol. 29, no. 6, pp. 3587–3608, 2022.

[2] S. Yu, J. Zhang, J. Liu, X. Zhang, Y. Li, and T. Xu, "A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN," *Eurasip J. Wirel. Commun. Netw.*, vol. 2021, no. 1, 2021. doi: 10.1186/s13638-021-01957-9

[3] D. Alsmadi and V. Prybutok, "Sharing and storage behavior via cloud computing: Security and privacy in research and practice," *Comput. Human Behav.*, vol. 85, pp. 218–226, 2018. doi: 10.1016/j.chb.2018.04.003

[4] K. Patel and A. Alabisi, "Cloud computing security risks: Identification and assessment," *The Journal of New Business Ideas & Trends*, vol. 17, no. 2, pp. 11–19, 2019.

[5] N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. Van Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," *Electron.*, vol. 9, no. 3, pp. 1–19, 2020. doi: 10.3390/electronics9030413

[6] P. S. Suryateja, "Threats and vulnerabilities of cloud computing a review," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 3, pp. 297–302, 2018. doi: 10.26438/ijcse/v6i3.297302

[7] A. K. Shukla and A. Sharma, "Reduce false intrusion alerts by using PSO feature selection in NSL-KDD dataset," in *Proc, 8th International Conference on Computing in Engineering and Technology (ICCET 2023)*, Hybrid Conference, Patna, India, 2023, pp. 226–231. doi: 10.1049/icp.2023.1495

[8] A. K. Shukla and A. Sharma, "Distributed attacks classification based on radical basis function and particle swarm optimization in hypervisor layer," in *Proc. 2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2023, pp. 1–4. doi: 10.1109/ISCON57294.2023.10112162

[9] Jia and Y. Liang, "Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain," *China Commun.*, vol. 17, no. 9, pp. 11–24, 2020. doi: 10.23919/JCC.2020.09.002

[10] A. K. Shukla and A. Sharma, "Cloud data security by hybrid machine learning and cryptosystem approach", *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 2s, pp. 01–14, Oct. 2023.

[11] J. Liu, X. Wang, S. Shen, G. Yue, S. Yu, and M. Li, "A bayesian Q-Learning game for dependable task offloading against DDoS attacks in sensor edge cloud," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7546–7561, 2020. doi: 10.1109/JIOT.2020.3038554

[12] F. S. de Lima-Filho, F. A. F. Silveira, A. de Medeiros-Brito-Junior, G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," *Secur. Commun. Networks*, vol. 2019, 2019. doi: 10.1155/2019/1574749

[13] A. K. Shukla and A. Sharma, "Cloud base intrusion detection system using convolutional and supervised machine learning," in *Proc. 2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2023, pp. 1–5. doi: 10.1109/ISCON57294.2023.10112007

[14] T. V. Phan and M. Park, "Efficient distributed denial-of-service attack defense in SDN-based cloud," *IEEE Access*, vol. 7, pp. 18701–18714, 2019. doi: 10.1109/ACCESS.2019.2896783

[15] P. T. Dinh and M. Park, "BDF-SDN: A big data framework for DDoS attack detection in large-scale SDN-based cloud," in *Proc. 2021 IEEE Conf. Dependable Secur. Comput.*, 2021. doi: 10.1109/DSC49826.2021.9346269

[16] A. K. Shukla and A. Sharma, "Classification and mitigation of DDoS attacks based on self-organizing map and support vector machine," in *Proc. 2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2023, pp. 1–5. doi: 10.1109/ISCON57294.2023.10111988

[17] I. Mukhtar and M. A. Azer, "Evaluating the modsecurity Web application firewall against SQL injection attacks," in *Proc. ICCES 2020-2020 15th Int. Conf. Comput. Eng. Syst.*, 2020. doi: 10.1109/ICCES51560.2020.9334626

[18] S. Narayanasami, S. Sengan, S. Khurram *et al.*, "Biological feature selection and classification techniques for intrusion detection on BAT," *Wireless Personal Communications,* pp. 1–23, 2021.

[19] N. Shone, T. N. Ngoc, V. D. Phai *et al.*, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence,* vol. 2, no. 1, pp. 41–50, 2018.

[20] K. B. Virupakshar, M. Asundi, K. Channal *et al.*, "Distributed Denial of Service (DDoS) attacks detection system for OpenStack-based private cloud," *Procedia Computer Science*, vol. 167, pp. 2297–2307, 2020.

[21] J. Cheng, M. Li, X. Tang *et al.*, "Flow correlation degree optimization driven random forest for detecting DDoS attacks in cloud computing," *Security and Communication Networks 2018,* 2018, pp. 1–14.

[22] A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud," *IEEE Access*, vol. 8, pp. 181916–181929, 2020.

[23] 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.

[24] S. Sambangi, and L. Gondi, "A machine learning approach for DDoS (distributed denial of service) attack detection using multiple linear regression," in *Proc. the 14th International Conference on Interdisciplinarity in Engineering*, 2020.

[25] T. H. H. Aldhyani and H. Alkahtan, "Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model," *Mathematics,* vol. 11, no. 1, 2023.

[26] M. M. Ahmed and A. El-Hajjar, "A proactive approach to protect cloud computing environment against a Distributed Denial of Service (DDoS) attack," *AI, Blockchain and Self-Sovereign Identity in Higher Education*, pp. 243–278, 2023.

[27] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Systems with Applications,* vol. 169, 114520, 2021.

[28] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics*, vol. 9, no. 6, 2020.

[29] S. M. Hezavehi and R. Rahmani, "Interactive anomaly-based DDoS attack detection method in cloud computing environments using a third party auditor," *Journal of Parallel and Distributed Computing*, vol. 178, pp. 82–99, 2023.

[30] M. J. Pasha, K. P. Rao, A. MallaReddy, and V. Bande, "LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments," *Measurement: Sensors*, 100828, 2023.