

Impact of feature selection on the performance of machine learning models for distributed denial of service detection

Jaimin Shroff^{1,2}, Sanjay Shah³, Jigna Jadav², Nakul Dave²

¹Department of Computer Engineering, Gujarat Technological University, Ahmedabad, India

²Department of Computer Engineering, Vishwakarma Government Engineering College, Ahmedabad, India

³Department of Computer Engineering, Government Engineering College, Rajkot, India

Article Info

Article history:

Received Feb 6, 2025

Revised Jul 31, 2026

Accepted Aug 12, 2026

Keywords:

CIC-DDoS2019

Distributed denial of service

Joint entropy

Mutual information score

Sequential feature selection

Software-defined networking

ABSTRACT

Distributed denial-of-service (DDoS) attacks significantly compromises network availability. Distributed reflection denial-of-service (DrDoS) is a variant of DDoS that exploits intermediary servers to reflect and amplify traffic toward the victim. In software-defined networking (SDN) contexts, machine learning (ML)-based detection has proven to be an efficient countermeasure; nevertheless, high-dimensional traffic features frequently diminish detection performance. This study examines the influence of sequential feature selection on the efficacy of ML models for DDoS detection utilizing the CIC-DDoS2019 dataset. A two-stage feature selection method integrating mutual information (MI) score and joint entropy analysis is suggested to diminish feature dimensionality while maintaining discriminative efficacy. The diminished feature sets are assessed utilizing random forest (RF), support vector machine (SVM), k-nearest neighbors (KNN), gradient boosting algorithm (GBA), and neural network classifiers. Experimental findings indicate that the suggested strategy markedly enhances computational efficiency and detection accuracy, with RF attaining over 97% accuracy and F1-score across several DDoS attack types. The results affirm that efficient feature selection is essential for scalable and precise DDoS detection in SDN systems.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Jaimin Shroff

Department of Computer Engineering, Gujarat Technological University

Nr. Visat Three Roads, Visat - Gandhinagar Highway, Chandkheda, Ahmedabad, Gujarat, India

Email: jaimin_shroff22@yahoo.co.in

1. INTRODUCTION

In modern digital landscapes, distributed denial-of-service (DDoS) assaults represent a critical issue, threatening the availability, integrity, and security of online services. These assaults aim to incapacitate target systems by inundating them with an excessive amount of harmful traffic, making them unreachable for legitimate users. With technological progress and heightened dependence on digital services, the prevalence, magnitude, and complexity of DDoS attacks are escalating, necessitating resilient and inventive mitigation measures [1]. A prominent instance demonstrating the effects of DDoS attacks is the 2016 Dyn incident. A substantial botnet consisting of hijacked internet of things (IoT) devices was utilized to execute a series of DDoS attacks against the infrastructure of Dyn, a prominent domain name system (DNS) provider. The assault caused extensive service interruptions for prominent websites and platforms, including Twitter (now X), Netflix, and Spotify. This incident underscored the potential weaknesses in the interconnected internet infrastructure and the necessity for adequate DDoS mitigation strategies [2].

Conventional network systems face challenges in managing DDoS attacks due to restricted scalability, insufficient real-time visibility, and dependence on human setups, which impede prompt replies. Their inflexible designs restrict adaptation to advancing attack methodologies, whereas centralized firewalls, as single points of failure, are readily susceptible to exploitation. These inefficiencies lead to protracted mitigation and extensive service disruptions. Sophisticated, adaptive strategies are essential for addressing contemporary DDoS threats [3]–[5].

Software-defined networking (SDN) mitigates the shortcomings of conventional networks in countering DDoS attacks by employing centralized control, programmability, and real-time visibility, which provide dynamic resource allocation and adaptive defense. It transforms network administration by separating control and data planes, hence improving scalability and resilience. Notwithstanding weaknesses in its centralized framework, SDN markedly enhances DDoS mitigation and network robustness [6]–[9].

The increasing complexity of DDoS attacks hinders detection and mitigation attempts, as perpetrators leverage IoT botnets for high-traffic or low-rate assaults that deplete SDN controller resources. Flaws in SDN protocols such as OpenFlow intensify these issues, allowing adversaries to inundate communication channels and induce systemic failures. These assaults aim at all layers of SDN: switch flooding in the data plane, resource exhaustion in the control plane, and application programming interface (API) exploitation for privilege escalation in the application plane [10]. Responding to emerging threats necessitates flexible detection systems. Machine learning (ML) and deep learning examine traffic patterns to identify harmful flows. Feature selection improves accuracy, decreases computational expenses by pinpointing essential traffic characteristics, facilitating the real-time detection of both high-volume and low-rate DDoS attacks in SDN systems [11], [12]. In this study, DDoS is used as the general term for DDoS attacks, whereas distributed reflection denial-of-service (DrDoS) refers specifically to attacks represented by the corresponding CIC-DDoS2019 attack classes

The organization of this research paper is as follows. Section 2 presents a comprehensive summary of the contemporary advancements in DDoS detection for SDN. Section 3 presents the methodology and research conducted in this study, including the implementation of feature selection techniques and ML models. Section 4 explores the findings and analysis of the results, encompassing the performance of diverse feature selection methodologies applied to the CIC-DDoS2019 dataset. Section 5 addresses the conclusions and future directions.

2. RELATED WORK

2.1. Distributed reflection denial-of-service detection using machine learning

The detection of DDoS attacks in SDN has been thoroughly investigated through ML, owing to its capacity to identify intricate traffic patterns and adjust to emerging threats. Chouhan *et al.* [13] developed an anomaly-based detection system connected with the Ryu controller, employing feature extraction and classifiers for real-time detection of DDoS attacks. The support vector machine (SVM) attained superior accuracy, adeptly differentiating between benign and malicious traffic with elevated precision and recall. Alsumaidaie *et al.* [14] introduced an ensemble voting methodology that integrates random forest (RF) and decision tree classifiers for DDoS detection utilizing the CIC-DDoS2019 dataset, attaining 100% accuracy in particular circumstances. Nevertheless, restricted investigation of classifier combinations and interpretability issues impede its wider applicability in dynamic SDN situations. Mohsin and Hamad [15] assessed RF and k-nearest neighbors (KNN) for DDoS detection in SDN systems through Mininet simulations across diverse topologies. Both models exhibited commendable accuracy however encountered constraints, such as considerable packet loss in singular topologies (28% for RF and 39% for KNN). The authors combined SVM and KNN algorithms with five extracted features to identify DDoS assaults in SDN systems, attaining over 99% detection accuracy with little resource consumption of 11%. Nevertheless, dependence on simulation environments constrains the model's relevance to actual network situations [16]. Ye *et al.* [17] employed a six-tuple feature extraction method alongside SVM to categorize DDoS attacks in SDNs, attaining a detection accuracy of 95.24% in a simulated floodlight controller setting. Nevertheless, dependence on a regulated simulation environment constrains the method's flexibility and resilience in practical SDN contexts. The authors utilized linear regression with gradient descent on a simulated simple network management protocol (SNMP) dataset to identify transmission control protocol-synchronized (TCP-SYN) attacks, attaining 99.7% accuracy and a 0.3% error rate. Nonetheless, the constraints of gradient descent in managing extensive datasets diminish its efficacy in practical, high-volume attack situations [18].

The authors suggested a framework that integrates feature selection with stacking ensemble learning utilizing light gradient boosting machine (LightGBM) and RF for intrusion detection. This method attains elevated detection accuracy by refining chosen features for the classification of network traffic. Yet its computational complexity constrains scalability for real-time detection in extensive networks [19]. This study

introduces a recurrent neural network (RNN) based model for identifying application-layer DDoS attacks through the analysis of communication patterns in application-layer protocols. The model attains good detection accuracy for explicit-duration attacks but encounters difficulties in generalizing across various protocols and variable network conditions [20]. Singh and Jayakumar [21] suggested a deep convolutional neural network (CNN) augmented with feature selection for the detection of DDoS attacks in SDN environments. The approach attained 96% detection accuracy; however, its computational inefficiency presents obstacles for real-time implementation in extensive and dynamic network environments. Dong and Sarem [22] proposed a DDoS detection algorithm based on data analysis (DDADA) and a DDoS detection algorithm based on machine learning (DDAML) for DDoS detection in SDN using traffic-behavior features such as flow length, duration, size, and ratio. Their methods achieved better detection performance than NB, KNN, SVM, and cognitive-inspired computing-support vector machine CIC-SVM, with DDAML showing strong true positive rate (TPR), false positive rate (FPR), and area under the curve (AUC) results. However, further improvement is required for practical deployment in real SDN environments. Xu *et al.* [23] proposed k-means++ fast k-nearest neighbors (K-FKNN), combining k-means++ preprocessing with FKNN for efficient DDoS detection in SDN. The method improved the efficiency, accuracy, and stability of conventional KNN and achieved strong F1-measure performance. The authors suggested extending the method to collaborative detection in distributed SDN as future work.

2.2. Feature selection techniques in network security

Feature selection is crucial for enhancing the effectiveness of ML models in DDoS detection in network security. This method increases classification accuracy, decreases computing load, and boosts model interpretability by pinpointing the most significant traffic features. Furthermore, proficient feature selection allows real-time detection systems to scale well while managing extensive and high-dimensional network traffic datasets.

Table 1 presents a comparative analysis of recent feature-selection and DDoS detection approaches. The reviewed studies employ entropy-based analysis, hybrid statistical feature selection, mutual information (MI), recursive feature elimination, correlation-based methods, information-theoretic selection, and deep learning-based traffic classification. Although many approaches achieve high detection accuracy, limitations remain regarding computational complexity, real-time deployment, scalability, and generalization to evolving attack patterns. These limitations motivate the development of an efficient two-stage feature-selection approach capable of retaining discriminative information while reducing feature dimensionality.

Table 1. Comparative analysis of DDoS detection approaches in SDN environments

Ref.	Feature selection method	Performance	Limitations	Dataset
[24]	Statistical feature extraction and manual selection	High accuracy in simulation setups	Limited scalability and lacks real-world validation	Custom dataset
[25]	None	100% accuracy in specific setups	Scalability issues in real-time setups	Time-series dataset
[26]	None	RF achieved 98% accuracy, KNN lower	Lacked dynamic adaptability for evolving attacks	CICIDS2017 dataset
[27]	Manual feature extraction with dimensional reduction	99% accuracy in SDN attack detection	Struggles with scalability and dynamic attack patterns	UNSW-NB15
[28]	Gradient descent optimization	94% accuracy with low prediction error rates	Ineffective for imbalanced datasets	NSL-KDD dataset
[29]	LGBM and RF embedded feature ranking	99% detection accuracy	Limited validation in live SDN environments	CICIDS2019
[30]	Embedded in deep learning models	99.75% detection accuracy in SDN	High computational time around 216.39 seconds	SDN-DDoS dataset

3. PROPOSED WORK

3.1. Dataset description

The CIC-DDoS2019 dataset, developed by the Canadian Institute for Cybersecurity, is one of the most comprehensive datasets for evaluating DDoS detection systems. It replicates authentic network traffic situations, encompassing both benign and malicious activities, spanning many attack vectors. The dataset encompasses many types of DDoS attacks, including high-rate and low-rate attacks, application-layer attacks, and volumetric attacks, rendering it especially pertinent for SDN [31].

Figure 1 depicts the workflow of an ML system designed to assess and contrast several methodologies for DDoS detection, emphasizing feature selection and classification procedures. This study process commences with a dataset of unprocessed network traffic or system information, which underpins the analysis of DDoS attack detection. The data is preprocessed to cleanse and normalize it, rectifying missing values, normalizing the dataset, and converting features into an appropriate format for subsequent analysis.

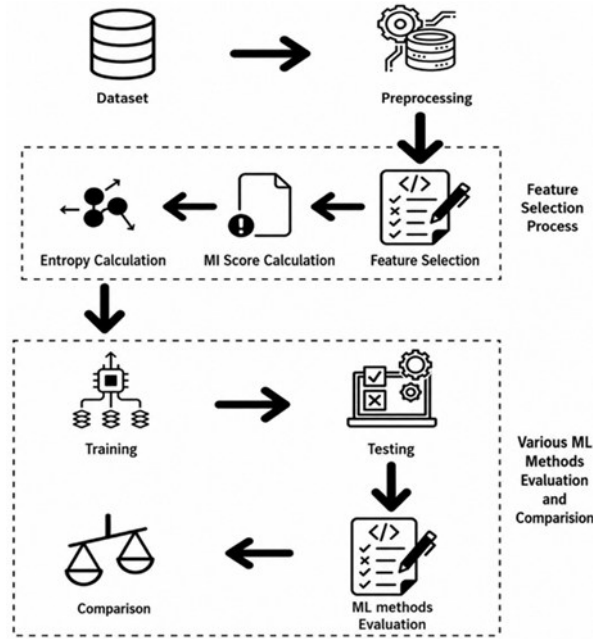


Figure 1. Proposed model pipeline

3.2. Feature selection method

Feature selection is an essential process for enhancing the efficacy and accuracy of ML models, especially in the realm of DDoS attack detection. In high-dimensional network traffic data, numerous variables may be redundant, irrelevant, or weakly linked with the attack class, potentially impairing classification performance and elevating processing demands. Consequently, the MI score is utilized to measure the extent of dependency between each feature and the target variable, facilitating the identification of the most informative and discriminative features for precise DrDoS detection. It is possible to express the MI score as in (1).

$$I(X; Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} \quad (1)$$

Where $I(X; Y)$ denotes the MI between the random variables X and Y . $p(x, y)$ represents the joint probability distribution of X and Y . $p(x)$ and $p(y)$ denote the marginal probability distributions of X and Y , respectively. The logarithm is typically computed using base 2 (yielding the result in bits) or the natural logarithm (yielding the result in nats), depending on the application.

Represent the marginal probability distribution functions of X and Y , respectively. The logarithm is conventionally base 2, indicating that the information is quantified in bits. Alongside MI, the joint entropy of feature pairs is calculated to elucidate their interactions and the extent to which their combined unpredictability aids in identifying DDoS assault patterns. Joint entropy is defined as in (2).

$$H(X, Y) = - \sum_{x \in X} \sum_{y \in Y} p(x, y) \log p(x, y) \quad (2)$$

Let $p(x, y)$ be the joint probability distribution function of the random variables X and Y . A modified joint entropy $H'(X, Y)$ is developed to enhance feature selection by incorporating MI to identify the most pertinent features. The revised joint entropy formula for $H'(X, Y)$ as in (3).

$$H'(X, Y) = - \sum_{x \in X} \sum_{y \in Y} (p(x, y) + \alpha I(X; Y)) \log p(x, y) + \alpha I(X; Y) \quad (3)$$

Where $p(x, y)$ is original joint probabilities of X and Y . $I(X; Y)$ represents MI, and α is a scaling factor that regulates the impact of MI on joint entropy.

Feature importance ratings are computed to assess their contribution to the identification of DDoS assault patterns. Features with elevated importance scores are deemed crucial for the precise identification of DDoS assaults. This method utilizes MI and joint entropy metrics to systematically identify the most pertinent characteristics, thereby reducing dimensionality and enhancing the effectiveness of the ML model for DDoS attack detection. The chosen features are subsequently employed for the training and testing of

several ML models, enabling the models to discern patterns that distinguish between regular and malicious communication. These models are subsequently assessed on novel data to gauge their proficiency in accurately identifying DDoS attacks.

Our pipeline ensures the selection of the most relevant features, thereby improving the accuracy and efficiency of the detection system while reducing computational overhead. In the evaluation and comparison step, we evaluate the performance of each ML model using metrics including accuracy, precision, recall, and F1-score. The outcomes are evaluated to determine the most efficient algorithm for DDoS detection.

3.3. Machine learning models

The chosen feature subsets derived from the proposed method are assessed using five standard ML algorithms: RF, SVM, KNN, neural networks, and gradient boosting algorithm (GBA). The models initially attained nearly 100% accuracy on the unprocessed dataset because of the intrinsic class imbalance and bias in the original data distribution, resulting in model overfitting. To address this issue, suitable preprocessing, normalization, and data balancing approaches were implemented, which substantially diminished overfitting and enhanced the models' generalization capacity on novel data.

4. EXPERIMENTAL RESULTS AND DISCUSSION

The CIC-DDoS2019 dataset was employed following feature selection and preprocessing to provide an optimal experimental framework. ML models, including RF, SVM, KNN, GBA, and neural networks, were implemented and evaluated using the processed dataset. The dataset was adjusted using a standard scaler to guarantee homogeneity. The performance of the models was evaluated using standard classification metrics, including accuracy, precision, recall, and F1-score. Results were visualized using Python programs like Matplotlib, Seaborn, and Scikit-learn, thereby corroborating the conclusions.

4.1. Feature selection results

The suggested study employs a sequential feature selection strategy that combines two complementing techniques: the MI score and the joint entropy-based method, to systematically enhance the feature space. These strategies are utilized to discover, rank, and delete redundant, irrelevant, and minimally useful variables that do not substantially enhance the accuracy of DDoS attack detection. The suggested technique improves computational efficiency and classification accuracy by minimizing feature dimensionality while retaining discriminative information, facilitating quicker and more dependable detection in SDN contexts. Figure 2 depicts the outcomes of the sequential feature selection technique. The x-axis denotes several categories of DDoS attacks, and the y-axis indicates the quantity of features. The first raw dataset has between 80 and 90 features. Following the implementation of the initial technique, the MI score indicates a reduction in the number of features to between 70 and 80. Consequently, utilizing the second way, the joint entropy-based strategy, the feature count is further reduced to between 50 and 60. This reduction markedly improves processing time, hence enhancing the efficiency of the detection system.

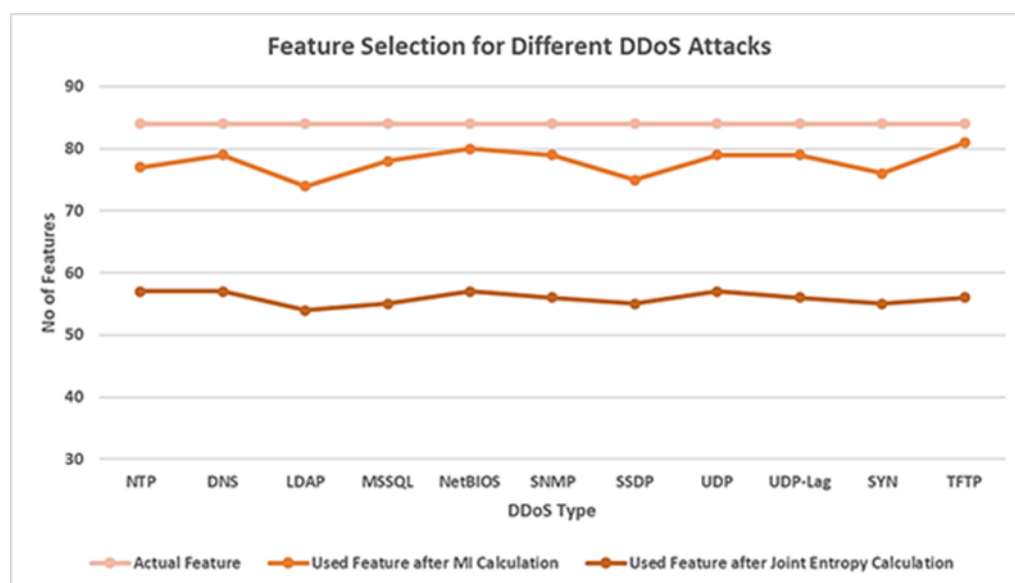


Figure 2. Feature selection for different DDoS attacks

4.2. Performance evaluation on various machine learning models

The assessment of the proposed methodology and ML models on the distributed reflective denial-of-service (DrDoS)_DNS dataset underscores its resilience and efficacy in identifying DrDoS DNS attacks. The outcomes are displayed via a confusion matrix for the RF model and a comparative analysis of various entropy approaches implemented across many ML models. A thorough performance benchmark Figure 2 was executed to assess the efficacy of diverse entropy approaches utilized across five ML models: RF, SVM, KNN, GBA, and neural networks. The benchmark evaluated four performance metrics: accuracy, precision, recall, and F1-score.

Figure 3 demonstrates that traditional entropy-based feature selection methods, such as Shannon, Ubrico, Tsallis, and Rényi, display similar efficacy across all assessed ML models. The suggested technique regularly surpasses traditional entropy measures by attaining superior values across all performance parameters, especially when combined with the RF classifier. These findings highlight the importance of integrating advanced entropy-based feature selection with robust ML classifiers to achieve consistent and scalable performance in DDoS detection systems.

Building on these findings, among all models, RF demonstrates the most superior overall performance, achieving near-optimal outcomes, with accuracy, precision, recall, and F1-score all surpassing 0.97. Despite neural networks demonstrating competitive performance, they are marginally less effective than RF, particularly for recall and F1-score. Conversely, SVM, KNN, and GBA demonstrate modest efficacy, with SVM and GBA typically surpassing KNN across the majority of entropy-based feature selection methodologies.

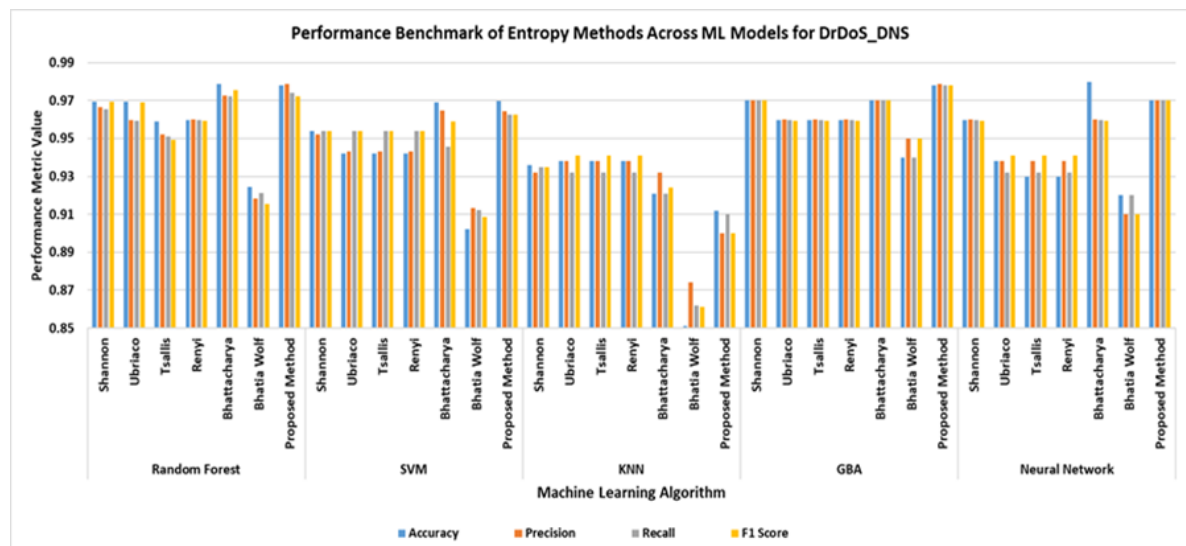


Figure 3. Performance of various ML models on DrDoS DNS attack

The proposed method consistently surpassed established entropy measures such as Shannon, Ubrico, Tsallis, and Rényi in the performance benchmark for DrDoS_lightweight directory access protocol (LDAP) across all ML models, as shown in Figure 4. The RF model demonstrated outstanding results with the proposed method, surpassing 0.97 in all criteria. Neural networks exhibited competitive performance but fell short of RF, especially in recall and F1-score. SVM and GBA exhibited moderate outcomes, exceeding KNN in the majority of instances. The assessment validates the strength and efficacy of the proposed method in enhancing detection performance.

The confusion matrices presented in Figures 5 and 6 validate the excellent accuracy of our RF model, exhibiting a preponderance of true positives and true negatives for all DrDoS attack types. Misclassifications (false positives and false negatives) were negligible, corroborating the model's robust precision, recall, and F1-scores as detailed in our analysis. The discrepancies in mistake rates among different attack methods underscore the significance of our dataset-specific tuning methodology. Our findings indicate that RF is exceptionally proficient at properly identifying DrDoS attacks.

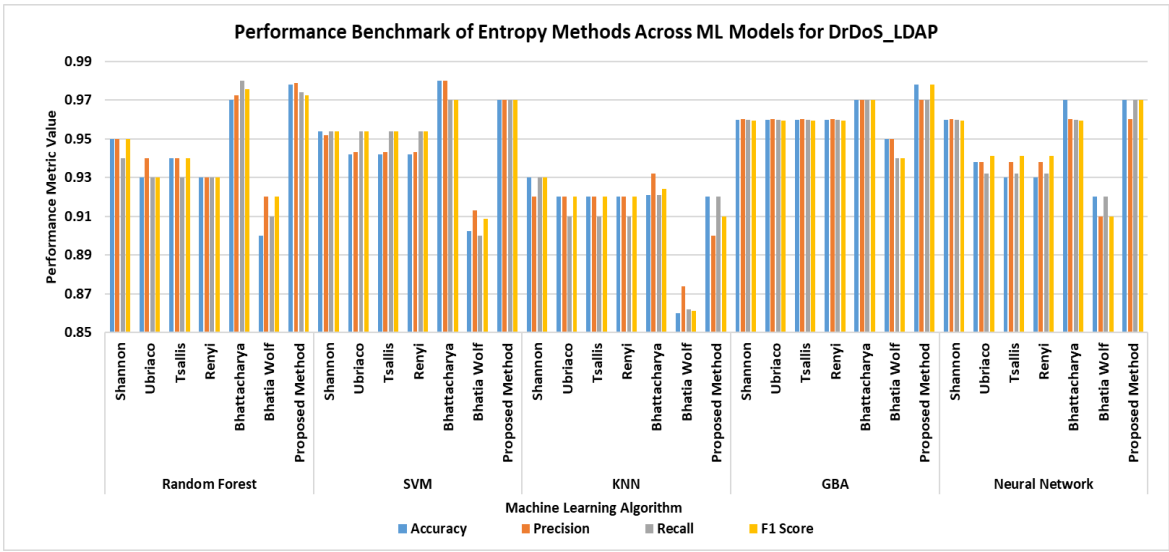


Figure 4. Performance of various ML models on DrDoS LDAP attack

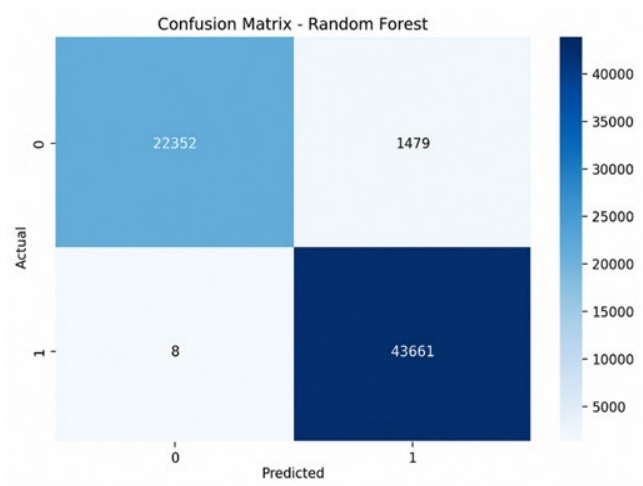


Figure 5. Confusion matrix of DrDoS DNS

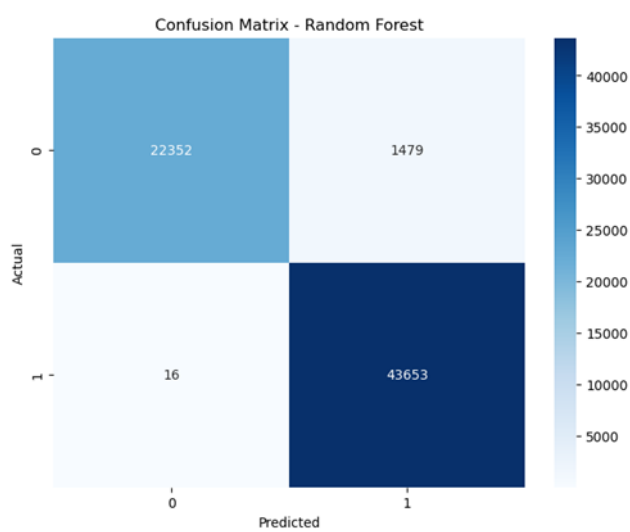


Figure 6. Confusion matrix of DrDoS LDAP

5. CONCLUSION AND FUTURE WORK

The proposed approach, when combined with the RF classifier, significantly enhances the performance of ML models on the CIC-DDoS2019 dataset. The sequential feature selection method effectively detects the most pertinent traffic attributes, enhancing detection accuracy, scalability, and practical utility in SDN-based settings. Furthermore, the methodology significantly diminishes false positives while preserving an exceptionally low false negative rate, which is essential for dependable and immediate network security implementation. These findings underscore the essential importance of feature selection and ensemble learning in managing extensive, high-dimensional cybersecurity datasets. The findings demonstrate that meticulously crafted feature selection methods can markedly enhance computing efficiency and classification resilience. This study establishes a robust basis for subsequent research on sophisticated feature extraction and hybrid learning frameworks. Future endeavors will concentrate on modifying the suggested methodology to accommodate emerging attack patterns, broadening its applicability to encompass more attack categories, and incorporating it with deep learning frameworks to further augment detection efficacy and system robustness.

ACKNOWLEDGMENTS

The authors would like to thank their respective institutions for providing the research facilities and academic environment necessary for this work.

FUNDING INFORMATION

The authors assert that their study did not obtain any specific financing from public, commercial, or non-profit entities. All experiments, data analysis, and manuscript writing were conducted utilizing institutional resources and the authors' personal efforts.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Jaimin Shroff	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	
Sanjay Shah		✓				✓		✓		✓	✓	✓	✓	
Jigna Jadav	✓		✓	✓	✓					✓			✓	
Nakul Dave			✓	✓	✓					✓	✓		✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

The authors assert that they possess no recognized competing financial interests, personal connections, or professional ties that may have seemingly influenced the work presented in this study. The authors affirm that there are no political, ideological, academic, or intellectual conflicts that could compromise the objectivity or integrity of this research.

DATA AVAILABILITY

The dataset utilized in this work (CIC-DDoS2019) is accessible to the public through the Canadian Institute for Cybersecurity repository. Data supporting the conclusions of this study can be obtained from the corresponding author, [JS], upon reasonable request.

REFERENCES

- [1] A. Singh and B. B. Gupta, "Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–43, 2022, doi: 10.4018/IJSWIS.297143.

- [2] M. Antonakakis *et al.*, "Understanding the Mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, Canada: USENIX Association, 2017, pp. 1093–1110.
- [3] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004, doi: 10.1016/j.comnet.2003.10.003
- [4] N. Agrawal and S. Tapaswi, "Defense mechanisms against DDoS attacks in a cloud computing environment: state-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3769–3795, 2019, doi: 10.1109/COMST.2019.2934468.
- [5] B. L. Dalmazo, J. A. Marques, L. R. Costa, M. S. Bonfim, R. N. Carvalho, L. P. Gaspar, and W. Cordeiro, "A systematic review on distributed denial of service attack defense mechanisms in programmable networks," *International Journal of Network Management*, vol. 31, no. 6, 2021, doi: 10.1002/nem.2163.
- [6] Y. Al-Hadhrami and F. K. Hussain, "DDoS attacks in IoT networks: a comprehensive systematic literature review," *World Wide Web*, vol. 24, no. 3, pp. 971–1001, 2021, doi: 10.1007/s11280-020-00855-2.
- [7] U. Rahamathullah and E. Karthikeyan, "Distributed denial of service attacks prevention, detection and mitigation—a review," in *Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021)*, 2021, doi: 10.2139/ssrn.3852902.
- [8] J. Wang and L. Wang, "SDN-defend: a lightweight online attack detection and mitigation system for DDoS attacks in SDN," *Sensors*, vol. 22, no. 21, Oct. 2022, doi: 10.3390/s22218287.
- [9] D. B. Rawat and S. R. Reddy, "Software-defined networking architecture, security and energy efficiency: a survey," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 325–346, 2017, doi: 10.1109/COMST.2016.2618874.
- [10] B. Alhijawi, S. Almajali, H. Elgala, H. B. Salameh, M. Ayyash, "A survey on DoS/DDoS mitigation techniques in SDNs: classification, comparison, solutions, testing tools and datasets," *Computers and Electrical Engineering*, vol. 99, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107706.
- [11] V. D. M. Rios, P. R. M. Inacio, D. Magoni, and M. M. Freire, "Detection and mitigation of low-rate denial-of-service attacks: a survey," *IEEE Access*, vol. 10, pp. 76648–76668, 2022, doi: 10.1109/ACCESS.2022.3191430.
- [12] D. Tang, R. Dai, C. Zuo, J. Chen, K. Li, and Z. Qin, "A low-rate DoS attack mitigation scheme based on port and traffic state in SDN," *IEEE Transactions on Computers*, vol. 74, no. 5, pp. 1758–1770, 2025, doi: 10.1109/TC.2025.3541143.
- [13] R. K. Chouhan, M. Atulkar, and N. K. Nagwani, "A framework to detect DDoS attack in Ryu controller based software defined networks using feature extraction and classification," *Applied Intelligence*, vol. 53, no. 4, pp. 4268–4288, Feb. 2023, doi: 10.1007/s10489-022-03565-6.
- [14] M. Alsumaidaie, K. Alheeti, and A. Alaloosy, "An assessment of ensemble voting approaches, random forest, and decision tree techniques in detecting DrDoS attacks," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 20, no. 1, pp. 16–24, Jun. 2024, doi: 10.37917/ijeee.20.1.2.
- [15] M. A. Mohsin and A. H. Hamad, "Performance evaluation of SDN DDoS attack detection and mitigation based random forest and k-nearest neighbors machine learning algorithms," *Revue d'Intelligence Artificielle*, vol. 36, no. 2, pp. 233–240, Apr. 2022, doi: 10.18280/ria.360207.
- [16] Z. Ma and B. Li, "A DDoS attack detection method based on SVM and k-nearest neighbour in SDN environment," *International Journal of Computational Science and Engineering*, vol. 23, no. 3, pp. 224–234, 2020, doi: 10.1504/IJCSE.2020.111431.
- [17] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software-defined network," *Security and Communication Networks*, 2018, doi: 10.1155/2018/9804061.
- [18] G. Rajakumaran, N. Venkataraman, and R. R. Mulkamala, "Denial of service attack prediction using gradient descent algorithm," *SN Computer Science*, vol. 1, no. 1, Jan. 2020, doi: 10.1007/s42979-019-0043-7.
- [19] A. K. Mishra and S. Paliwal, "Mitigating cyber threats through integration of feature selection and stacking ensemble learning: the LGBM and random forest intrusion detection perspective," *Cluster Computing*, vol. 26, no. 4, pp. 2339–2350, 2023, doi: 10.1007/s10586-022-03735-8.
- [20] B. Xie, Y. Wang, G. Wen, and X. Xu, "Application-layer DDoS attack detection using explicit duration recurrent network-based application-layer protocol communication models," *International Journal of Intelligent Systems*, no. 1, Jan. 2023, doi: 10.1155/2023/2632678.
- [21] S. Singh and S. K. V. Jayakumar, "DDoS attack detection in SDN: optimized deep convolutional neural network with optimal feature set," *Wireless Personal Communications*, vol. 125, no. 3, pp. 2781–2797, Aug. 2022, doi: 10.1007/s11277-022-09685-z.
- [22] S. Dong and M. Sarem, "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.
- [23] Y. Xu, H. Sun, F. Xiang, and Z. Sun, "Efficient DDoS detection based on K-FKNN in software-defined networks," *IEEE Access*, vol. 7, pp. 160536–160545, 2019, doi: 10.1109/ACCESS.2019.2950945.
- [24] H. Lotfalizadeh and D. S. Kim, "Investigating real-time entropy features of DrDoS attack based on categorized partial-flows," in *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, Jan. 2020, pp. 1–6, doi: 10.1109/IMCOM48794.2020.9001690.
- [25] M. A. Hossain and M. S. Islam, "Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: a promising solution for robust cybersecurity," *Measurement: Sensors*, vol. 32, Apr. 2024, doi: 10.1016/j.measen.2024.101037.
- [26] M. Aldualij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Aldualij, and F. Malik, "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, no. 6, May 2022, doi: 10.3390/sym14061095.
- [27] P. Kumari, A. K. Jain, Y. Pal, K. Singh, and A. Singh, "Towards detection of DDoS attacks in IoT with optimal features selection," *Wireless Personal Communications*, vol. 137, no. 2, pp. 951–976, Jul. 2024, doi: 10.1007/s11277-024-11419-2.
- [28] U. S. Chanu, K. J. Singh, and Y. J. Chanu, "A dynamic feature selection technique to detect DDoS attack," *Journal of Information Security and Applications*, vol. 74, May 2023, doi: 10.1016/j.jisa.2023.103445.
- [29] C. Westphal, S. Hailes, and M. Musolesi, "Feature selection for network intrusion detection," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, vol. 1, pp. 1599–1610, 2025, doi: 10.1145/3690624.3709339.
- [30] N. Ahuja, D. Mukhopadhyay, and G. Singal, "DDoS attack traffic classification in SDN using deep learning," *Personal and Ubiquitous Computing*, vol. 28, no. 2, pp. 417–429, Apr. 2024, doi: 10.1007/s00779-023-01785-2.
- [31] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, Oct. 2019, pp. 1–8, doi: 10.1109/CCST.2019.8888419.

BIOGRAPHIES OF AUTHORS



Jaimin Shroff     has been serving as an assistant professor in the Technical Education Department of the Government of Gujarat since 2012. With a strong academic and research background, he is currently pursuing his Ph.D. at Gujarat Technological University, specializing in network and information security. His research is primarily focused on developing advanced methodologies for DDoS attack detection and mitigation, leveraging machine learning algorithms and feature selection techniques to enhance network security frameworks. His broader research interests encompass various aspects of computer networks and information security, including intrusion detection systems, network anomaly detection, cryptographic security mechanisms, and secure communication protocols. Over the years, he has made significant contributions to the field through his research, having published more than five papers in reputed international journals and conferences. He can be contacted at email: jaimin_shroff22@yahoo.co.in.



Dr. Sanjay Shah     is a distinguished academician and professor in the field of Computer Engineering (GES Class -1) with extensive experience spanning over 30 years. He is currently associated with the Department of Computer Engineering, Government Engineering College and holds an impressive academic background with a Ph.D., M.E., and B.E. in the discipline. Throughout his academic career, he has been actively involved in teaching various subjects, including data structures, database management systems, software engineering, computer networks, advanced data structures, and system software. His research interests lie in the areas of soft computing and data mining, contributing significantly to advancements in these domains. Over the years, he has published more than twenty research papers in esteemed national and international journals and conferences, showcasing his commitment to academic excellence. He can be contacted at email: sanjay_shah_r@yahoo.com.



Dr. Jigna Jadav     is an assistant professor in the Department of Computer Engineering at Vishwakarma Government Engineering College (VGEC), India. She has over 15 years of teaching experience and holds a Ph.D., M.E., and B.E. in Computer Engineering. She has taught both undergraduate and postgraduate courses, including data mining, machine learning, artificial intelligence, and database management systems. Her research interests include artificial intelligence, machine learning, data mining, and healthcare analytics. She has published several research papers in reputed national and international journals and conference proceedings. She can be contacted at email: jigna.j.jadav@gmail.com.



Dr. Nakul Dave     has been serving as an assistant professor in the Department of Computer Engineering at Vishwakarma Government Engineering College, Ahmedabad, under the Technical Education Department, Government of Gujarat. He received his Ph.D. in Computer Engineering from Gujarat Technological University (GTU). His research interests include natural language processing, theory of computation, information security, machine learning, and information retrieval. He has published several research papers in reputed national and international journals and conferences indexed in Scopus and Web of Science. He actively contributes to teaching, research, academic administration, accreditation, and outcome-based education initiatives. He can be contacted at email: davenakulr@gmail.com.