A Comparative Study of DDoS Detection Techniques In Cloud Computing

Kritika Verma[1], Radhika Dhiman[2],Jawahar Thakur[3]
[1, 2, 3] Dept of Computer Science
[1, 2, 3] Himachal Pradesh University, Shimla, HP.

Abstract- *Cloud computing has become increasingly popular as it is cost-effective, scalable, flexible, and supports virtualization. Nonetheless, its susceptibility to a plethora of threats and attacks is evident. Among these, Distributed Denial of Service (DDoS) attacks are the most prevalent within the cloud computing realm. As DDoS attacks evolve to possess increased sophistication and complexity, current Machine Learning (ML) and Deep Learning (DL) techniques predominantly cater to isolated attack types. However, their effectiveness wanes due to diminished accuracy and prolonged detection times. This underscores the imperative for a fresh, hybrid approach to address the afore-mentioned challenges inherent in ML and DL. This study aims to compare the existing ML and DL techniques. Within this landscape, Support Vector Machines (SVM), Random Forest, and Naïve Bayes emerge as the most pervasive methodologies. Notably, the CICIDS 2017 and NSL KDD datasets have gained prominence as commonly employed resources. The study's findings underscore the potency of hybrid models that integrate Artificial Neural Networks (ANNs), yielding elevated detection rates and exceptional accuracy. Comparative analysis reveals that, in contrast to deep learning methods, hybrid approaches exhibit heightened accuracy levels.*

Keywords- Cloud computing, DDoS, Machine Learning, Deep Learning, Hybrid Approach.

I. INTRODUCTION

Cloud computing stands out as one of the most widely discussed technologies of the previous decade. The term refers to the provision of computing services over the internet. Cloud Computing offers on-demand services via the internet, eliminating the need for physical infrastructure or maintenance. Through Cloud Computing, users gain the capability to access applications, data, unlimited storage, resources, and more, irrespective of their location or the time[1]. This technology operates on a pay-as-you-go model, enabling users to rapidly adjust their computing resources to match their requirements, thereby facilitating quick scaling up or down as necessary[2][3]. Recent emerging technologies like IoT, IoV (Internet of Vehicles), 5G, big data, and WSN require cloud computing as it supports services like virtualization, flexibility, and scalability. But the only issue is its lack of security. It is therefore imperative that cloud computing address security concerns.Cloud computing security encompasses network and access control challenges, alongside those related to the cloud infrastructure[4]. Figure 1 illustrates a basic snapshot of DDoS attack. Enforcing comprehensive security measures is intricate due to varying user security demands[5][6]. Cloud services, often delivered via the HTTP protocol for accessibility and cost reduction, are susceptible to HTTP DDoS attacks. Malicious users intentionally orchestrate DDoS attacks to disrupt and degrade services and resources for legitimate users. These attacks involve compromised computers targeting network resources and servers, flooding with messages, malformed packets, and connection requests, resulting in service denial[7]. DDoS attacks in the cloud exhibit high sophistication, utilizing crafted request methods to exploit vulnerabilities and execute flooding attacks. Classification of DDoS attacks hinges on network protocol and application, with network or transport level attacks utilizing UDP, ICMP, and TCP protocols.HTTP DDoS attacks occur in both high and low-rate scenarios, each significantly impacting the victim. In high-rate attacks, a deluge of requests overwhelms the victim, while low-rate scenarios involve slow, compromised requests that drain resources. Within the cloud computing environment, DDoS attacks are primarily at the application layer, utilizing communication protocols that mimic legitimate requests. This makes them hard to discern at the network layer, rendering traditional defense systems ineffective. Various categories of DDoS flooding attacks on the cloud include session and request flooding, slow response, and asymmetric attacks.

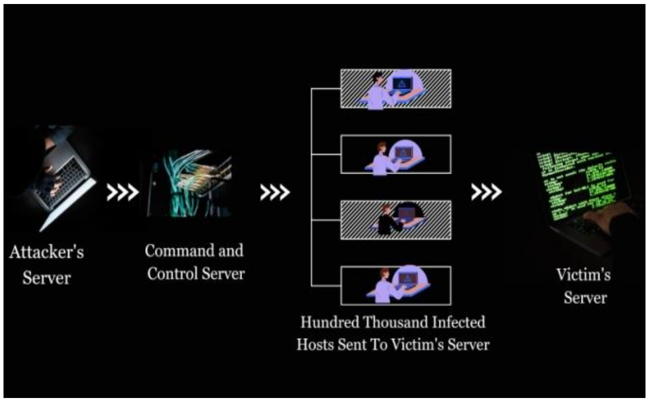

Attacker's Server
Command and Control Server
Hundred Thousand Infected Hosts Sent To Victim's Server
Victim's Server

Figure 1. Basic DDoS Attack

These attacks generate traffic resembling that of genuine users, making it challenging for the target to differentiate between attack and legitimate traffic, ultimately disrupting services for genuine users.

The remainder of this paper is organized as: section II discusses the related work, section III defines the research problem and objectives of this study, and section IV illustrates the comparative analysis of the various DDoS Detection techniques. The paper is concluded in section V followed by section VI which provides the future scope of the study.

II. RELATED WORK

DDoS is one of the predominant security-related concerns in cloud computing, which demands its early detection.Cloud service providers can minimize downtime and ensure that their services remain accessible to users by detecting DDoS attacks early and implementing appropriate mitigation strategies. There are many detection techniques that can be used for DDoS prevention.

A. Detection of DDoS Attacks Using Machine Learning

A machine learning-based system for detecting cloud-based Denial of Service (DOS) attacks is proposed in [8]. The system involves a new approach focusing on source-side detection, overcoming limitations in previous victim-side threshold analysis. Nine methods of machine learning are compared by the authors in the paper. However, the study lacks an in-depth literature review on DOS attack detection. Another study[9] centers on a system to identify Distributed Denial of Service (DDoS) attacks in cloud computing. The C.4.5 algorithm is compared with Naive Bayes and Snort, an open-source IDS using signature-based techniques. The comparison is drawn from a literature review and involves different algorithms and platforms.

The surge in DDoS attacks and the need for novel cloud computing defense mechanisms is highlighted in [10] . In this work, the authors have compared three classification algorithms for detecting DDoS attacks. Support Vector Machine demonstrates the highest overall accuracy, followed closely by Random Forest. The paper concludes that SVM outperforms other methods for DDoS attack detection.

An overview of intrusion detection systems (IDS) in cloud environments is presented in [11], where the authors have addressed the challenges like real-time detection and scalability. Various machine learning techniques and feature selection methods applied in cloud-based intrusion detection are discussed. Also, the evaluation of IDS effectiveness across different datasets and attack scenarios is emphasized in the study.

A machine learning-based DDoS detection and prevention system for cloud computing is introduced in [12]. The study reveals that statistical feature extraction and three classification algorithms yield 99.76% detection accuracy. Further, future research directions are illustrated, including exploration of unsupervised and reinforcement learning, deep learning techniques, real-time detection systems, and ensemble approaches to enhance accuracy.

The study done in [13],advocates machine learning's utility in detecting DDoS attacks in Cloud settings due to intricacies in distinguishing normal and malicious traffic. The authors have applied regression analysis on the dataset (CICIDS 2017), achieving high accuracy in predicting DDoS and Bot attacks.

Another technique for DDoS attack detection in cloud computing is demonstrated in [14]. This technique uses feature selection and machine learning algorithms. The results show that RF, GB, WVE, and KNN attain 0.99 accuracy with 19 features. RF excels other algorithms, misclassifying only one attack as normal.

B. Detection of DDoS Attacks Using Deep Learning

The threat of insider DDoS attacks in cloud environments is highlighted in [15], suggesting conventional defenses like firewalls fall short. Their proposed solution employs an evolutionary neural network in the hypervisor layer for anomaly-based detection between virtual machines. Evaluated on a 60,000-connection dataset, it exhibits strong effectiveness with minimal false alarms. However, resource requirements might be a constraint in certain cloud setups.

A CS-ANN technique for cloud DDoS attack detection is introduced in [16]. Optimizing features via Cuckoo Search (CS) and applying an Artificial Neural

Network (ANN) yields superior “True Positive Rate (TPR)”, “False Positive Rate (FPR)”, and detection accuracy compared to state-of-the-art methods. The approach shows promise in effectively detecting cloud DDoS attacks and safeguarding service availability

C. Detection of DDoS Attacks Using Hybrid Approach

In [17], the authors have provided a background on the problem, introducing Deep Neural Networks, Genetic Algorithms, and optimization strategies like Parallel Processing and Fitness Value Hashing. Their "MLIDS" approach achieves accurate intrusion detection, outperforming benchmarks across datasets.

In [18], an enhanced Self-adaptive evolutionary extreme learning machine (SaE-ELM) model has been devised for DDoS attack detection in cloud computing. The proposed system attains high accuracy on diverse datasets, overcoming limitations of traditional signature-based methods and addressing challenges in machine learning-based systems.

The importance of appropriate feature selection is highlighted in [19], leading to the creation of a new dataset, KDD DDoS, by isolating DDoS packets. The hybrid approach demonstrates superior DDoS detection rates compared to existing methods, with an average detection rate of 99.01% and the highest rate at 99.86%. However, the scalability, computational complexity, false positive/negative rates, and robustness against adversarial attacks remain unexplored. Future work includes real cloud environment implementation and prevention strategies against actual DDoS attacks.

A self-learning method for detecting DDoS attacks in cloud computing is introduced in [20]. The effectiveness is shown, but concerns arise regarding data quality, scalability, and evolving attack techniques. An adaptive approach estimates traffic changes and employs a relearning algorithm for improved accuracy. The method addresses limitations of pre-learned models and rule-based systems in dynamic cloud networks. It emphasizes data mining's significance for detection and proposes adapting models through new data.

III. RESEARCH PROBLEM AND OBJECTIVE

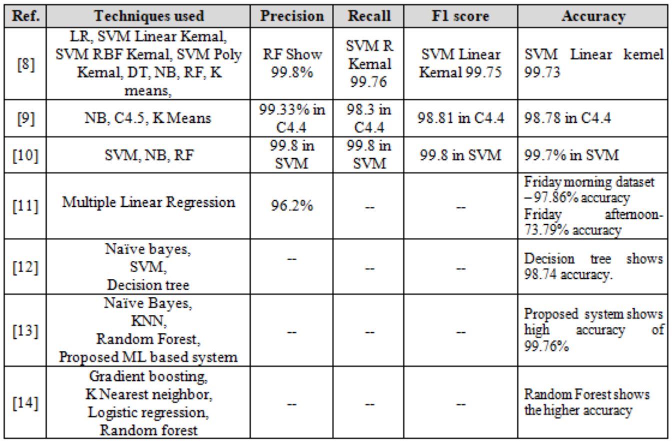
The existing methods for DDoS attack detection are time-consuming, narrowly focused on specific attack types, and rely on outdated datasets. Furthermore, there is no optimization, no real-time detection, and little emphasis on mitigation rather than detection. A comprehensive approach is needed to address these limitations and enhance DDoS attack prevention and response strategies[21].

This study provides valuable insight in selecting and implementing appropriate DDoS detection technique to safeguard the system against DDoS attacks. The main objective of this study is to review and perform comparative analysis of current DDoS detection techniques in cloud computing.

IV. COMPARITIVE ANALYSIS OF DDoS DETECTION TECHNIQUES

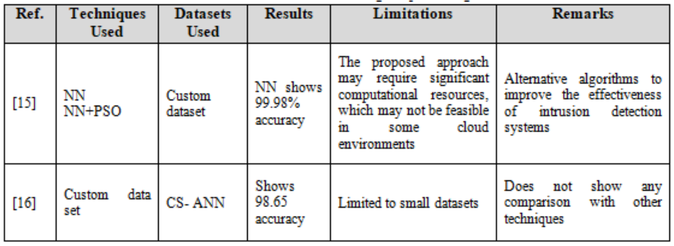
Different machine learning, deep learning and hybrid methods for DDoS attack detection are studied for comparatively analyzing the different results achieved by the authors. This section presents the in-depth theoretical analysis of the various techniques explored by the authors. Table 1 illustrates the different machine learning techniques used for DDoS attack. For each paper, the table describes the techniques used for detection, algorithms achieving highest precision, recall, F1 score and Accuracy. Table 2 demonstrates the different deep learning techniques for DDoS attack detection. Not much literature has been found on this technique. The table describes the techniques and datasets used by the authors,best results attained with respect to accuracy, limitations and remarks. Table 3 provides the information regarding hybrid techniques used to detect DDoS attack. This table also describes the various hybrid techniques and datasets used by the authors, results in terms of achieved accuracy, limitations and remarks.

Table 1. DDoSDetection using Machine Learning



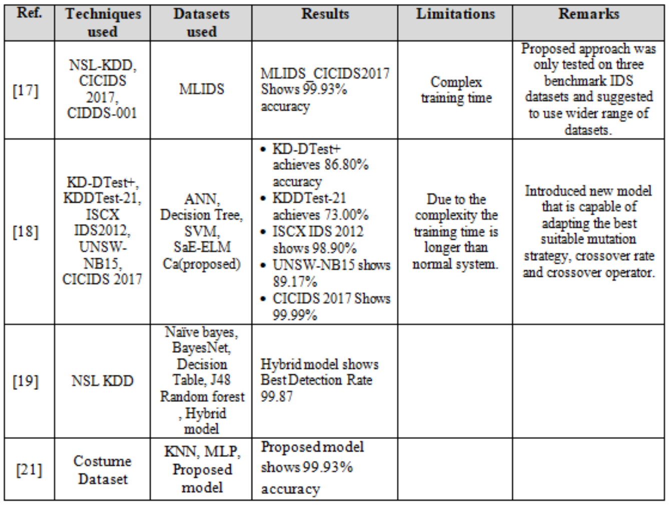
Ref.	Techniques used	Precision	Recall	F1 score	Accuracy
[8]	LR, SVM Linear Kernal, SVM RBF Kernal, SVM Poly Kernal, DT, NB, RF, K means,	RF Show 99.8%	SVM R Kernal 99.76	SVM Linear Kernal 99.75	SVM Linear kernel 99.73
[9]	NB, C4.5, K Means	99.33% in C4.4	98.3 in C4.4	98.81 in C4.4	98.78 in C4.4
[10]	SVM, NB, RF	99.8 in SVM	99.8 in SVM	99.8 in SVM	99.7% in SVM
[11]	Multiple Linear Regression	96.2%	--	--	Friday morning dataset –97.86% accuracy Friday afternoon-73.79% accuracy
[12]	Naïve bayes, SVM, Decision tree	--	--	--	Decision tree shows 98.74 accuracy.
[13]	Naïve Bayes, KNN, Random Forest, Proposed ML based system	--	--	--	Proposed system shows high accuracy of 99.76%
[14]	Gradient boosting, K Nearest neighbor, Logistic regression, Random forest	--	--	--	Random Forest shows the higher accuracy

Table 2. DDoSDetection using Deep Learning



Ref.	Techniques Used	Datasets Used	Results	Limitations	Remarks
[15]	NN NN+PSO	Custom dataset	NN shows 99.98% accuracy	The proposed approach may require significant computational resources, which may not be feasible in some cloud environments	Alternative algorithms to improve the effectiveness of intrusion detection systems
[16]	Custom data set	CS- ANN	Shows 98.65 accuracy	Limited to small datasets	Does not show any comparison with other techniques

Table 3. DDoS Detection using Hybrid Approach



Ref.	Techniques used	Datasets used	Results	Limitations	Remarks
[17]	NSL-KDD, CICIDS 2017, CIDDS-001	MLIDS	MLIDS_CICIDS2017 Shows 99.93% accuracy	Complex training time	Proposed approach was only tested on three benchmark IDS datasets and suggested to use wider range of datasets.
[18]	KD-DTest+, KDDTest-21, ISCX IDS2012, UNSW-NB15, CICIDS 2017	ANN, Decision Tree, SVM, SaE-ELM Ca(proposed)	• KD-DTest+ achieves 86.80% accuracy • KDDTest-21 achieves 73.00% • ISCX IDS 2012 shows 98.90% • UNSW-NB15 shows 89.17% • CICIDS 2017 Shows 99.99%	Due to the complexity the training time is longer than normal system.	Introduced new model that is capable of adapting the best suitable mutation strategy, crossover rate and crossover operator.
[19]	NSL KDD	Naïve bayes, BayesNet, Decision Table, J48 Random forest , Hybrid model	Hybrid model shows Best Detection Rate 99.87		
[21]	Costume Dataset	KNN, MLP, Proposed model	Proposed model shows 99.93% accuracy		

V. CONCLUSION

In this study several DDoS detection techniques for Cloud Computing have been discussed and compared based on their performance and other metrics. The most commonly used techniques are SVM, Random Forest, and Nave Bayes. The most frequently used datasets are CICIDS 2017 and NSL KDD. According to the study, ANN, NN, and hybrid models are more efficient, faster, and more accurate when used for detecting DDoS attacks. According to the study, the Hybrid Approach is more accurate than simple machine learning techniques.

VI. FUTURE SCOPE

Cloud computing is rapidly expanding, offering numerous research avenues. Potential research directions encompass the exploration of deep learning methods, like convolutional neural networks and recurrent neural networks, for feature extraction and classification in detecting distributed denial-of-service (DDoS) attacks. Moreover, a demand exists for real-time detection systems capable of swiftly identifying and countering DDoS attacks in cloud computing settings. Techniques like anomaly detection and flow-based analysis patterns hold promise. Examining the impact of diverse network configurations and topologies on DDoS attack detection, as well as developing adaptable methods in response to changing network dynamics, offers another promising avenue. The effectiveness of combining traditional intrusion detection techniques with emerging approaches presents an intriguing area of investigation. Blockchain technology can be used to mitigate DDoS attacks using cloud computing.

REFERENCES

[1] M. S. M. Sivam, “What is Cloud Computing? | Basics of Cloud Computing,” OSTechNix. Accessed: Sep. 30, 2023. [Online]. Available: https://ostechnix.com/cloud-computing-basics/

[2] “Characteristics of Cloud Computing - GeeksforGeeks.” Accessed: Oct. 01, 2023. [Online]. Available: https://www.geeksforgeeks.org/characteristics-of-cloud-computing/

[3] “(PDF) Cloud Computing Architecture: A Critical Analysis.” Accessed: Oct. 01, 2023. [Online]. Available: https://www.researchgate.net/publication/327125094_Cloud_Computing_Architecture_A_Critical_Analysis

[4] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, “DDoS attacks in cloud computing: Issues, taxonomy, and future directions,” *Comput. Commun.*, vol. 107, pp. 30–48, Jul. 2017, doi: 10.1016/j.comcom.2017.03.010.

[5] A. Mondal, S. Paul, R. T. Goswami, and S. Nath, “Cloud computing security issues & challenges: A Review,” in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, Jan. 2020, pp. 1–5. doi: 10.1109/ICCCI48352.2020.9104155.

[6] S. Aldossary and W. Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 4, 2016, doi: 10.14569/IJACSA.2016.070464.

[7] F. Sabahi, “Cloud computing security threats and responses,” in *2011 IEEE 3rd International Conference on Communication Software and Networks*, May 2011, pp. 245–249. doi: 10.1109/ICCSN.2011.6014715.

[8] Z. He, T. Zhang, and R. B. Lee, “Machine Learning Based DDoS Attack Detection from Source Side in Cloud,” in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, Jun. 2017, pp. 114–120. doi: 10.1109/CSCloud.2017.58.

[9] M. Zekri, S. E. Kafhali, N. Aboutabit, and Y. Saadi, “DDoS attack detection using machine learning techniques in cloud computing environments,” in *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, Oct. 2017, pp. 1–7. doi: 10.1109/CloudTech.2017.8284731.

[10] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, “Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques,” in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Feb. 2019, pp. 870–875. doi: 10.1109/AICAI.2019.8701238.

[11] Bagyalakshmi and E. Samundeeswari, “DDoS Attack Classification on Cloud Environment Using Machine Learning Techniques with Different Feature Selection

Methods," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, pp. 7301–7308, Nov. 2020, doi: 10.30534/ijatcse/2020/60952020.

[12] A. Mishra, B. B. Gupta, D. Peraković, F. J. G. Peñalvo, and C.-H. Hsu, "Classification Based Machine Learning for Detection of DDoS attack in Cloud Computing," in *2021 IEEE International Conference on Consumer Electronics (ICCE)*, Jan. 2021, pp. 1–4. doi: 10.1109/ICCE50685.2021.9427665.

[13] S. Sambangi and L. Gondi, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression," in *The 14th International Conference on Interdisciplinarity in Engineering—INTER-ENG 2020*, MDPI, Dec. 2020, p. 51. doi: 10.3390/proceedings2020063051.

[14] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method," *Symmetry*, vol. 14, no. 6, Art. no. 6, Jun. 2022, doi: 10.3390/sym14061095.

[15] A. Rawashdeh, M. Alkasassbeh, and M. Al-Hawawreh, "An anomaly-based approach for DDoS attack detection in cloud environment," *Int. J. Comput. Appl. Technol.*, vol. 57, no. 4, pp. 312–324, Jan. 2018, doi: 10.1504/IJCAT.2018.093533.

[16] A. Gupta and M. Kalra, "Intrusion Detection and Prevention system using Cuckoo search algorithm with ANN in Cloud Computing," in *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Nov. 2020, pp. 66–72. doi: 10.1109/PDGC50313.2020.9315771.

[17] Z. Chiba, N. Abghour, K. Moussaid, A. El omri, and M. Rida, "Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms," *Comput. Secur.*, vol. 86, pp. 291–317, Sep. 2019, doi: 10.1016/j.cose.2019.06.013.

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

[19] S. Nandi, S. Phadikar, and K. Majumder, "Detection of DDoS Attack and Classification Using a Hybrid Approach," in *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, Feb. 2020, pp. 41–47. doi: 10.1109/ISEA-ISAP49340.2020.234999.

[20] A. Rukavitsyn, K. Borisenko, and A. Shorov, "Self-learning method for DDoS detection model in cloud computing," in *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Feb. 2017, pp. 544–547. doi: 10.1109/EIConRus.2017.7910612.

[21] "Shodhganga@INFLIBNET: A Hybrid Approach Using Digital Forensics for Attack Detection and Classification in Cloud Network Environment." Accessed: Oct. 01, 2023. [Online]. Available: https://shodhganga.inflibnet.ac.in/handle/10603/444715