International Journal of Science and Engineering Applications
Volume 13-Issue 05, 40 - 45, 2024, ISSN:- 2319 - 7560
DOI:10.7753/IJSEA1305.1007

Ensemble Learning Methods for DDoS Attack Detection in Cloud Environments: A Comprehensive Review

Jayshree Vishnu Ade
Department of Computer Science and Engineering
Government College of Engineering
Amravati, Maharashtra, India

Anil Vasantrao Deorankar
Associate Professor
Department of Computer Science and Engineering
Government College of Engineering, Amravati, India

Abstract: With the increasing prevalence of Distributed Denial of Service (DDoS) attacks in cloud computing environments, there is a growing need for robust and efficient detection mechanisms. This review paper aims to provide a comprehensive overview of the application of ensemble learning methods in enhancing DDoS attack detection within cloud environments. Ensemble learning, a paradigm that leverages the strengths of multiple models to achieve superior performance, has shown promising results in mitigating the challenges posed by DDoS attacks. The paper begins with an exploration of the significance of DDoS attacks in cloud environments, emphasizing the complexities associated with their detection. A thorough examination of the existing literature reveals the limitations of traditional machine learning approaches in addressing these challenges, paving the way for the introduction of ensemble learning as a viable solution. A detailed discussion on the principles of ensemble learning is presented, accompanied by an overview of prominent ensemble methods such as Random Forest, Gradient Boosting, and Bagging. The strengths and weaknesses of these methods in the context of DDoS detection are critically analyzed, providing insights into their effectiveness.To contextualize the discussion, the paper examines commonly used datasets and features in DDoS detection studies. The application of ensemble learning methods, particularly Random Forest, Gradient Boosting, and Bagging, is then explored in detail through a review of relevant literature. Each method's working principle and its efficacy in detecting DDoS attacks in the cloud are thoroughly assessed.Performance metrics, including accuracy, precision, recall, and F1-score, are discussed as essential criteria for evaluating the effectiveness of ensemble learning in DDoS detection. The challenges faced in implementing ensemble learning for DDoS detection and potential avenues for future research are also identified. In conclusion, this review consolidates the current state of knowledge on ensemble learning methods for DDoS attack detection in cloud environments. By synthesizing existing literature and critically evaluating the strengths and limitations of ensemble approaches, this paper contributes to a better understanding of the role of ensemble learning in fortifying cloud security against DDoS threats.

Keywords: DDoS Attacks, Ensemble Learning, Cloud Computin, Bagging, Gradient Boosting, Random Forest and Machine Learning

1. INTRODUCTION

In the ever-evolving landscape of information technology, cloud computing has emerged as a pivotal paradigm, offering scalable and flexible resources to meet the demands of modern applications. However, this advancement has not come without challenges, with security concerns taking center stage. Among these concerns, Distributed Denial of Service (DDoS) attacks represent a formidable threat to the availability and reliability of cloud-based services.DDoS attacks, characterized by orchestrated efforts to overwhelm a target system's resources, have become increasingly sophisticated, exploiting vulnerabilities in cloud infrastructures. The repercussions of successful DDoS attacks extend beyond mere service disruptions, encompassing financial losses, reputational damage, and potential breaches of sensitive data. As organizations migrate critical services to the cloud, the need for robust and adaptive DDoS detection mechanisms becomes paramount.

Traditional machine learning approaches have been instrumental in detecting and mitigating cyber threats. However, the dynamic nature of DDoS attacks, coupled with the complexities of cloud environments, poses unique challenges that conventional methods struggle to address effectively. Recognizing the limitations of standalone models, researchers and practitioners have turned to ensemble learning as a promising avenue for bolstering DDoS detection in the cloud. Ensemble learning, a methodology that combines the predictions of multiple models to enhance overall performance, presents an innovative approach to tackling the intricate nature of DDoS attacks. By leveraging the strengths of diverse models, ensemble methods such as Random Forest, Gradient Boosting, and Bagging exhibit the potential to adapt to evolving attack patterns and improve overall detection accuracy.

This review paper embarks on a comprehensive exploration of the role of ensemble learning methods in fortifying DDoS attack detection within cloud environments. Through an extensive analysis of existing literature, we aim to shed light on the efficacy of ensemble approaches and their ability to address the nuanced challenges posed by DDoS attacks in the dynamic cloud landscape. The subsequent sections delve into the principles of ensemble learning, the application of specific ensemble methods, and an evaluation of their performance metrics, ultimately providing a foundation for future research directions.

As organizations continue to navigate the complexities of securing their cloud-based infrastructures, a deeper understanding of the potential offered by ensemble learning becomes crucial. By synthesizing current knowledge and identifying avenues for further exploration, this review seeks to contribute to the advancement of DDoS detection strategies, offering insights that are both timely and indispensable in the realm of cloud security.

2. LITERATURE REVIEW

The evolution of cloud computing has ushered in a new era of technological possibilities, accompanied by an escalating arms race against cyber threats. Among these threats, Distributed Denial of Service (DDoS) attacks stand out as a persistent and pervasive menace to the stability and resilience of cloud-based services. In this section, we embark on a journey through the existing body of literature, offering a synthesized overview of DDoS attack detection within cloud environments and the pivotal role that ensemble learning methods play in fortifying these defenses.

2.1 DDoS Attack Landscape:

The literature reveals a dynamic and evolving landscape of DDoS attacks, characterized by their increasing frequency, sophistication, and ability to exploit vulnerabilities inherent in cloud infrastructures. Early studies emphasized the disruptive nature of DDoS attacks, underscoring the need for proactive detection mechanisms to mitigate their impact. Researchers have delved into the taxonomy of DDoS attacks, categorizing them based on attack vectors, intensity, and duration. Understanding the multifaceted nature of DDoS attacks serves as a foundational step in developing effective detection strategies. Imam Sharafaidin et al. proposed a new taxonomy for DDoS attacks as illustrated in Figure 1.

1. Reflection-based DDoS (Distributed Denial of Service): These attacks are a type of cyberattack that exploits the functionality of certain network protocols to amplify the volume of traffic directed at a target. In a reflection-based DDoS attack, the attacker leverages servers or systems on the internet to reflect and amplify their attack traffic towards the victim, making it more challenging to trace the origin of the attack. The packets are forwarded to reflectors servers by setting source IP by IP of the victim. These attacks can be carried out through application layer protocols using transport layer protocols, i.e. Transmission control protocol (TCP), User datagram protocol (UDP) or through a combination of both. As Figure 1 shows, in this category, TCP based attacks include MSSQL, SSDP while as UDP based attacks include CharGen, NTP and TFTP. There are certain attacks that can be carried out using either TCP or UDP like DNS, LDAP, NETBIOS, and SNMP.

2. Exploitation-based attacks: These attacks refer to a category of cyberattacks where the primary goal is to identify and exploit vulnerabilities in computer systems, networks, applications, or other digital assets. In these attacks, the attacker seeks to take advantage of weaknesses or flaws in the target's defenses to gain unauthorized access, manipulate data, or disrupt normal operations. The exploitation of vulnerabilities is a key step in many types of cyberattacks. The packets are sent to reflector servers by attackers with the source IP address set to the target victim’s IP address to overwhelm the victim with response packets. These attacks can also be carried out through application layer protocols using transport layer protocols e.g. TCP and UDP. TCP based exploitation attacks include SYN flood and UDP based attacks include UDP flood and UDP-Lag.

UDP flood attack is initiated on the remote host by sending a large number of UDP packets. These UDP packets are sent to random ports on the target machine at a very high rate. As a result, the available bandwidth of the network gets exhausted, system crashes and performance degrades. On the other hand, SYN flood also consumes server resources by exploiting TCP-three-way handshake. This attack is initiated by sending repeated SYN packets to the target machine until server crashes/malfunctions. The UDP-Lag attack is that kind of attack that disrupts the connection between the client and the server. This attack is mostly used in online gaming where the players want to slow down/interrupt the movement of other players to outmaneuver them. This attack can be carried in two ways, i.e. using a hardware switch known as lag switch or by a software program that runs on the network and hogs the bandwidth of other users.

2.2 Challenges in DDoS Detection in Cloud Environments:

The following are the issues or challenges in the defense of DDoS attack in cloud Environment as discussed in [2].

Firewall Constraints:

Firewalls engage in state-level monitoring for each incoming connection. Amidst a DDoS onslaught, an inundation of network packets inundates the Firewall. Depletion of Firewall resources results in a deterioration of performance. Firewalls encounter difficulty in distinguishing between legitimate and DDoS traffic in application layer attacks.

Issues with IDS/IPS:

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) possess anomaly-detection capabilities. They can discern malicious network packets but frequently produce false positives and negatives. Manual configurations tailored to a specific network become necessary. Both IDS/IPS and Firewalls are positioned proximately to the safeguarded web server, rather than at the network's foremost defense line.

Scalability Hurdles:

Traditional defenses do not represent the primary defense line for initial DDoS attack filtration. DDoS mitigation techniques could be implemented on edge routers for premature detection.

Limitations of Signature-based Detection:

IDS/IPS techniques can identify known DDoS attack types using signature-based detection. They grapple with zero-day attacks, lacking a mitigation function.

Router Access Control Lists (ACLs): Router ACLs unaccompanied cannot sift through DDoS attack traffic, particularly if it employs valid network protocols. Routers are typically ineffective against sophisticated spoofed and application-level DDoS attacks.

Additional Challenges:

Automated, user-friendly attack tools and budget-friendly Botnets-for-hire services empower attackers with limited technical acumen. Attackers imitate legitimate traffic traits, complicating the differentiation between legitimate and malevolent traffic. IP spoofing conceals the identity of participants, complicating trace back. DDoS attacks entail an extensive volume of traffic, overwhelming defense solutions and resulting in denial of service to legitimate users. Extensive recruitment of unwitting and geographically dispersed participants characterizes DDoS attacks. Persistent security vulnerabilities in the Internet, such as congested or crashed autonomous systems, can impact global connectivity. Limited collaboration within administrative domains and the absence of centralized control in Internet infrastructure impede effective DDoS defense.

[10] presents a comprehensive taxonomy of all the possible variants of cloud DDoS attacks solutions with detailed insight into the characterization, prevention, detection, and mitigation mechanisms. Also discussed about performance measurement metrics as shown below:

Accuracy:

Accuracy, a pivotal metric, is measured through TPR (True Positive Rate) and TNR (True Negative Rate). TPR signifies correctly identified attack traffic, while TNR indicates accurately identified legitimate traffic. Accuracy is calculated by summing correctly identified attack and legitimate instances, divided by the total.

Service Response Time:

Crucial for performance evaluation, service response time measures the duration from request to response. The defense system deployment should not adversely affect response time for legitimate users.

Attack Detection Time:

A critical metric, attack detection time emphasizes the speed of classifying network traffic as legitimate or malicious. Swift detection, with a low detection time, characterizes an effective defense system. Detection time is influenced by the communication and computational complexities of the defense algorithm.

Victim Service Downtime:

Significant for performance assessment, service downtime represents the period of unavailability for the victim cloud server. Effective defense systems aim to minimize downtime, ensuring prompt service to legitimate requests.

Total Estimated Cost:

The cost of attack detection and mitigation, covering resource utilization, is a crucial metric.Ideally, defense costs should be lower than losses incurred due to DDoS attacks.

Experimental Testbed:

To be effective, defense systems should actively capture and monitor real-time aggregate traffic. Real-time analysis of traffic from both legitimate and compromised nodes is crucial for effective attack detection. Evaluating defense approaches in simulated environments may not guarantee suitability for real-time analysis in large-scale cloud computing.

[13] proposed a classification based machine learning approach for detection of DDoS attack in cloud computing. With the help of three classification machine learning algorithms K Nearest Neighbor, Random Forest and Naive Bayes, the mechanism can detect a DDoS attack with the accuracy of 99.76%.[14] proposed a DDoS detection system based on the C.4.5 algorithm to mitigate the DDoS threat. This algorithm, coupled with signature detection techniques, generates a decision tree to perform automatic, effective detection of signatures attacks for DDoS flooding attacks.[15] propose atechnique for detecting DDoS attacks in a cloud computing environment using big data and deep learning algorithms. The proposed technique utilises big data spark technology to analyse a large number of incoming packets and a deep learning machine learning algorithm to filter malicious packets. The KDDCUP99 dataset was used for training and testing, and an accuracy of 99.73% was achieved.

[24] found that Stochastic Gradient Boosting algorithm is better than Naive Bayes and Random Forest algorithms in classifying DDoS attacks.

[25] the proposed system uses machine learning-based classifiers on network flow data. Four tree-based classifiers, i.e., decision tree, random forest, XGBoost, and AdaBoost are applied to the identified parameters. The CIDDS-001 dataset were used for training and evaluation. Results obtained show that the proposed classifier can achieve 99.99% accuracy using the random forest classifier.

[26] propose a novel optimized weighted voting ensemble model to detect DDoS attack in an SDN environment. The proposed ensemble employs six base classifiers (two SVMs, two Random forests, and two Gradient Boosted Machines) that are differentiated by hyperparameter values. The optimal set of weights are identified by a novel hybrid metaheuristic optimization algorithm (BHO).

[27] used the hybrid classifier which is the integration of Random Forest classifier, Decision Tree classifier, Support Vector Machine and XGBoost classifier, all trained on the pre-processed Knowledge Discovery in Databases (KDD) Cup 99 and UNSW-NB15 datasets.

Traditional machine learning approaches have formed the bedrock of cybersecurity strategies, yet the unique challenges posed by DDoS attacks in cloud environments necessitate a reevaluation of existing methodologies. The literature points to the limitations of standalone models in adapting to the dynamic and scalable nature of cloud architectures. Challenges such as the variability of attack patterns, the sheer volume of network traffic, and the need for real-time detection have spurred researchers to explore innovative solutions, leading to the emergence of ensemble learning as a focal point of investigation.

3. ENSEMBLE LEARNING

3.1 Concept of Ensemble Learning:

Ensemble learning is a machine learning paradigm that involves the combination of multiple individual models to create a stronger, more robust predictive model. The basic premise is that aggregating the predictions of diverse models can lead to improved overall performance compared to any single model. Ensemble learning aims to mitigate the weaknesses of individual models by leveraging their collective intelligence, resulting in enhanced accuracy, generalization, and resistance to overfitting.

3.2 Overview of Popular Ensemble Learning Methods:

Ensemble learning encompasses various methods, each with its unique characteristics. Notable ensemble learning methods include Random Forest, Gradient Boosting, and Bagging. Random Forest constructs a multitude of decision trees and combines their outputs through a voting mechanism. Gradient Boosting, on the other hand, builds trees sequentially, with each tree correcting the errors of its predecessor. Bagging involves training multiple models on different subsets of the training data and aggregating their predictions. Each method brings its own strengths and nuances to the realm of DDoS detection in cloud environments.

3.3 Strengths and Weaknesses of Ensemble Learning:

Ensemble learning exhibits several strengths that make it particularly suited for DDoS detection. Its ability to handle high-dimensional data, reduce overfitting, and provide robust predictions in the presence of noise renders it advantageous. However, challenges exist, such as increased computational complexity and the potential for model interpretability issues. Balancing the trade-offs and understanding the contextual applicability of ensemble learning is crucial for its successful integration into DDoS detection frameworks.

4. DATASETS AND FEATURES

4.1 Commonly Used Datasets:

The evaluation of DDoS detection systems relies on the availability of benchmark datasets. Commonly used datasets in this domain include the CICDDoS2019 dataset, NSL-KDD, and UNSW-NB15. These datasets encompass a diverse range of attack scenarios and network conditions, providing a comprehensive basis for assessing the efficacy of detection models.

4.2 Relevant Features in DDoS Detection Studies:

The selection of features plays a pivotal role in the accuracy of DDoS detection models. Relevant features include network traffic attributes such as packet size, flow duration, protocol type, and source/destination IP addresses. Additionally, features derived from the frequency and intensity of network communication contribute to the discriminative power of models. The literature emphasizes the significance of feature engineering in capturing the nuanced patterns indicative of DDoS attacks Captions should be Times New Roman 9-point bold. They should be numbered (e.g., “Table 1” or “Figure 2”), please note that the word for Table and Figure are spelled out. Figure’s captions should be centered beneath the image or picture, and Table captions should be centered above the table body.

5. ENSEMBLE LEARNING IN DDOS DETECTION

1 Random Forest:

Random Forest constructs an ensemble of decision trees through a process of bootstrapped sampling and random feature selection. Each tree in the forest is trained on a subset of the training data, and during prediction, the outputs of individual trees are aggregated through voting (classification) or averaging (regression). Studies Applying Random Forest to DDoS Detection: The literature showcases studies that leverage Random Forest for DDoS detection in cloud environments. These studies highlight the effectiveness of Random Forest in handling the complexity and variability of DDoS attack patterns, contributing to improved detection rates.

5.2 Gradient Boosting:

Gradient Boosting builds a strong predictive model by sequentially adding weak models, with each new model focusing on correcting errors made by its predecessors. The process involves minimizing a loss function, and the final prediction is a weighted sum of the predictions from individual weak models.Studies Applying Gradient Boosting to DDoS Detection:Researchers have explored the application of Gradient Boosting techniques to enhance DDoS detection capabilities. Sequential learning and error correction mechanisms make Gradient Boosting suitable for capturing intricate relationships in network traffic data.

5.3 Bagging:

Bagging, short for Bootstrap Aggregating, involves training multiple models independently on random subsets of the training data. The predictions of these models are then combined, typically through voting for classification tasks or averaging for regression tasks. Studies Applying Bagging to DDoS Detection: Bagging has found application in DDoS detection studies, demonstrating its effectiveness in improving model robustness and generalization. By reducing the impact of outliers and noise, Bagging contributes to more resilient detection systems.

5.4 Other Ensemble Methods:

While Random Forest, Gradient Boosting, and Bagging are prominently featured in the literature, other ensemble methods such as AdaBoost, Stacking, and XGBoost have also been explored. These methods bring their unique approaches to ensemble learning, addressing specific challenges in DDoS detection scenarios.

6. PERFORMANCE METRICS

Evaluation of DDoS detection systems necessitates the use of well-defined performance metrics. Commonly employed metrics include accuracy, precision, recall, F1-score, and area under the ROC curve (AUC). These metrics provide a comprehensive assessment of a model's ability to correctly classify normal and attack instances, while accounting for potential trade-offs between false positives and false negatives.

7. CHALLENGES AND FUTURE DIRECTIONS

7.1 Challenges in Implementing Ensemble Learning:

Implementing ensemble learning for DDoS detection is not without challenges. The dynamic nature of cloud environments, evolving attack strategies, and the need for real-time detection present hurdles. Ensuring scalability, interpretability, and seamless integration into existing cybersecurity infrastructures are ongoing challenges that researchers and practitioners grapple with.

7.2 Potential Solutions and Future Research Directions:

Addressing the identified challenges requires innovative solutions and prompts future research directions. Hybrid models, combining ensemble learning with deep learning or anomaly detection methods, hold promise. Incorporating threat intelligence, leveraging explainable AI techniques, and developing adaptive models capable of continuous learning are avenues for future exploration.

8. CONCLUSION

In conclusion, the synthesis of literature pertaining to DDoS detection in cloud environments reveals the critical role played by ensemble learning methods. Random Forest, Gradient Boosting, Bagging, and other ensemble techniques have demonstrated their efficacy in enhancing detection accuracy and robustness. Leveraging benchmark datasets and relevant features, researchers have contributed to the evolution of DDoS detection models. Performance metrics provide a quantitative basis for evaluating model effectiveness.

9. REFERENCES

[1] Imam Sharafaidin, Arash Habibi Lashkari, Ali A Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy" 2019 International Carnahan Conference on Security Technology (ICCST).

[2] 2. Sajal Bhatia, Sunny Behal, and Irfan Ahmed, " Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions", Springer Nature Switzerland AG 2018 M. Conti et al. (eds.), Versatile Cybersecurity, Advances in Information Security 72, https://doi.org/10.1007/978-3-319-97643-3_3

[3] 3. M. Sachdeva, K. Kumar, and G. Singh, "A comprehensive approach to discriminate ddos attacks from flash events," Journal of Information Security and Applications, vol. 26, pp. 8– 22, 2016

[4] 4.. Ni, X. Gu, H. Wang, and Y. Li, "Real-time detection of application-layer ddos attack using time series analysis," Journal of Control Science and Engineering, vol. 2013, p. 4, 2013.

[5] 5. K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "Ddos attack detection method using cluster analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659–1665, 2008.

[6] 6. A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking ddos attacks," IEEE Communications Letters, vol. 13, no. 9, 2009.

[7] 7. Z. Xia, S. Lu, J. Li, and J. Tang, "Enhancing ddos flood attack detection via intelligent fuzzy logic," Informatica, vol. 34, no. 4, 2010.

[8] 8. R. Karimazad and A. Faraahi, "An anomaly-based method for ddos attacks detection using rbf neural networks," in Proceedings of the International Conference on Network and Electronics Engineering, 2011, pp. 16–18.

[9] 9.D. Das, U. Sharma, and D. Bhattacharyya, "Detection of http flooding attacks in multiple sce-narios," in Proceedings of the 2011 international conference on communication, computing & security. ACM, 2011, pp. 517–522.

[10] 10. Neha Agrawal and Shashikala Tapaswi, "Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges", I 0.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

[11] 11. O. Osanaiye, K.K.R. Choo, and M. Dlodlo, "Distributed Denial of Service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," Journal of Network and Computer Applications, vol. 67, pp. 147-165, May 2016.

[12] 12. Sherwin Kati, Abhishek Ove, Bhavana Gotipamul, Mayur Kodche,Prof. Swati Jaiswal, "Comprehensive Overview of DDOS Attack in Cloud Computing Environment using different Machine Learning Techniques", Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022

[13] 13. Anupama Mishra, B. B. Gupta, Dragan Perakovi´c, Francisco Jos´e Garc´ıa Pe˜nalvo, Ching-Hsien Hsu, " Classification Based Machine Learning for Detection of DDoS attack in Cloud Computing",2 021 IEEE International Conference on Consumer Electronics (ICCE) | 978-1-7281-9766-1/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICCE50685.2021.942766

[14] 14. Marwane Zekri, Said El Kafhali, Noureddine Aboutabit, Youssef Saadi " DDoS attack detection using machine learning techniques in cloud computing environments",Conference Paper · October 2017 DOI: 10.1109/CloudTech.2017.8284731

[15] 15. B. B. Gupta, Akshat Gaurav, Dragan Perakovi´c, "A Big Data and Deep Learning based Approach for DDoS Detection in Cloud Computing Environment", 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE) | 978-1-6654-3676-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/GCCE53005.2021.9622091

[16] 16. S. Balasubramaniam , C. Vijesh Joe, T. A. Sivakumar , A. Prasanth, K. Satheesh Kumar, V. Kavitha, and Rajesh Kumar Dhanaraj, "Optimization Enabled Deep Learning-Based DDoS AttackDetection in Cloud Computing", International Journal of Intelligent Systems Volume 2023, Article ID 2039217, 16 pages,https://doi.org/10.1155/2023/2039217

[17] 17. Sandeep Kautish , Reyana A , Member, IEEE, and Ankit Vidyarthi, "SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 18, NO. 9, SEPTEMBER 2022

[18] 18. C.Bagyalakshmi1 , Dr.E.S.Samundeeswari, "DDoS Attack Classification on Cloud Environment Using Machine Learning Techniques with Different Feature Selection Methods", kshmi et al., International Journal of Advanced Trends in Computer Science and Engineering, 9(5), September - October 2020, 7301 – https://doi.org/10.30534/ijatcse/2020/60952020

[19] 19. Gopal Singh Kushwah1, Virender Ranga, "Detecting DDoS Attacks in Cloud Computing Using Extreme Learning Machine and Adaptive Differential Evolution", Vol.:(0123456789)Wireless Personal Communications (2022) 124:2613–2636 https://doi.org/10.1007/s11277-022-09481-9

[20] 20. Mona Alduailij, Qazi Waqas Khan , Muhammad Tahir , Muhammad Sardaraz , Mai Alduailij and Fazila Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method", Symmetry 2022 , 14 , 1095 https://doi.org/10.3390/sym14061095

[21] 21. Yun Tian, Andres F. Romero Nogales, "Survey on Data Integrity Attacks and DDoS Attacks inCloud Computing" , 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) | 979-8-3503-3286-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/CCWC57344.2023.10099240

[22] 22. Iehab Alrassan, Asma Alqahtani, "Detection of DDoS Attacks on Clouds Computing Environments Using Machine Learning Techniques", 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS) | 979-8-3503-3929-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCNS58795.2023.10193141

[23] 23. Om Prakash Suman, Mohit Kumar, "Machine Learning Based Theoretical and Experimental Analysis of DDoS Attacks in Cloud Computing", 2023

International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT) | 978-1-6654-7491-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/DICCT56244.2023.10110201

[24] 24. Ricki Firmansyah, Ema Utami, Eko Pramono, "Evaluation of Naive Bayes, Random Forest and Stochastic Gradient Boosting Algorithm on DDoSAttack Detection", 1st International Conference on Science and Technology Innovation (ICOSTEC) February, 26 2022. Yogyakarta, Indonesia ISBN: 978-623-331-338-4

[25] 25. N. Muraleedharan & B. Janet, "An HTTP DDoS Detection Model Using Machine Learning Techniques for the Cloud Environment", Advances in Computing and Network Communications Proceedings of CoCoNet 2020, Volume 1

[26] 26. Aastha Maheshwari, Burhan Mehraj, Mohd Shaad Khan, Mohd Shaheem Idrisi, "An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment", Microprocessors and Microsystems Volume 89, March 2022, 104412

[27] 27. Beenish Habib, and Farida Khursheed," REST-API based DDoS Detection Using Multi Feature Hybrid Classification in the Cloud Architecture", International Journal of Computing and Digital Systems ISSN (2210-142X) Int. J. Com. Dig. Sys. 14, No.1 (Sep-2023) http://dx.doi.org/10.12785/ijcds/140184