World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Enhancing DDoS Detection in Cloud Computing Environment Through Effective Feature Selection With SMOTE

Ogah Stephen Ugbowu [1,*], Benson Yusuf Baha [2] and Asabe Sandra Ahmadu [2]

[1] *Department of Computer Science, School of Science and Technology, Federal Polytechnic Mubi, Adamawa State, Nigeria.*
[2] *Department of Computer Science, Faculty of Computing, Modibbo Adama University Yola, Nigeria.*

World Journal of Advanced Research and Reviews, 2026, 30(01), 1671-1679

Publication history: Received on 05 March 2026; revised on 13 April 2026; accepted on 16 April 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.30.1.0962

Abstract

The growing reliance on internet-based services and the increasing sophistication of cyber threats have made network security a crucial concern in modern day computing. These attacks can disrupt operations, result in financial losses, damage reputations, and undermine trust in digital services. Distributed denial of service (DDoS) attacks has emerged as a critical challenge for cloud computing, impacting service availability and raising concerns among providers. Despite cloud computing's scalable and flexible architecture, its vulnerabilities make it an attractive target for attackers. This paper presents a comprehensive survey of DDoS attacks in cloud environments, focusing on detection mechanisms leveraging Synthetic Minority Oversampling Technique (SMOTE). The paper focuses on the analysis of cloud computing characteristics exploited by attackers, and a discussion of effective anomaly detection approaches. Solutions based on SMOTE, encompassing detection parameters, metrics and features were reviewed for their ability to enhance security with high accuracy and low computational costs. The results present 39 different feature selection as depicted in table 2. It recommends that different feature selection and resampling techniques be studied toward developing a faster system for identifying imbalance data for DDoS attack detection.

Keywords: Feature; Detection; Imbalance; Computing; Security

1. Introduction

Distributed Denial of Service (DDoS) attacks pose a significant threat to network security, causing substantial financial losses and reputational damage (Chawla, 2025). Machine learning-based detection methods have shown promise in identifying DDoS attacks, but their effectiveness is often hindered by the class imbalance problem, where normal traffic instances far outnumber DDoS attack instances (Zargar et al., 2023). This class imbalance can lead to biased models that prioritize accuracy on the majority class (normal traffic) over the minority class (DDoS attacks), resulting in poor detection rates and high false negative rates (Jonker et al., 2024).

In the field of network intrusion detection, particularly in the classification of Distributed Denial of Service (DDoS) attacks, many existing methods often neglect the challenge of class imbalance in the datasets (Chawla, 2025). In these datasets, certain attack types dominate, causing machine learning models to develop a bias toward the more prevalent classes. As a result, these models tend to favor frequent attack types, while overlooking or misclassifying less common but crucial attack types. This leads to a decline in the overall reliability and effectiveness of the detection system, especially when it is critical to identify rare but important attack types for maintaining robust network defense (Zargar et al., 2023).

* Corresponding author: Ogah Stephen Ugbowu

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

Although numerous studies have focused on classifying and detecting network attacks without addressing the class imbalance issue, these approaches frequently yield skewed performance metrics. Typically, these models achieve high overall accuracy but perform poorly in detecting the minority classes (Pael et al., 2022). This becomes particularly concerning when rare attack types such as advanced or novel DDoS methods are missed. In such cases, high accuracy can be deceptive, as it reflects the model's good performance in detecting majority classes but fails to identify the more dangerous and often harder to detect minority attacks (Cheng et al., 2021).

The growing reliance on internet-based services and the increasing sophistication of cyberattacks have made network security a crucial concern in modern-day computing (Sharma et al., 2023). These attacks can disrupt operations, result in financial losses, damage reputations, and undermine trust in digital services (Amin et al., 2023). Hence, network security is crucial for maintaining integrity and availability of services in all organizations.

Industries such as the financial sector, IT and insurance organizations continue to be severely hit by cyberattacks due to the nature of the sensitive data held by them (Islamia et al., 2018). These organizations possess an extensive database of high-value, customer records to include credit card information and email addresses. Information hackers can use when planning future attacks (Groot et al., 2019). This is characterized by a series of extraordinary attacks, including threats against malware, credit crunches and debit card, phishing efforts, data breaches and information violation (Islamia et al., 2018).

In the realm of network security, Distributed Denial of Service (DDoS) attacks have emerged as a formidable threat, aiming to disrupt the availability of services by overwhelming network resources (Jin et al., 2024). The detection and mitigation of such attacks are paramount to maintaining the integrity and reliability of network infrastructures (Jin et al., 2024).

Distributed Denial of Service (DDoS) attacks, which flood a target network or server with an overwhelming amount of traffic, have emerged as one of the most significant threats to the availability and reliability of online services (Zhang et al., 2024). As such, effectively detecting and mitigating DDoS attacks is a critical component of contemporary network security practices (Zhang et al., 2024).

One of the primary challenges is the issue of class imbalance in the datasets used to train intrusion detection models (Wang et al., 2023). Network traffic datasets, such as those used for DDoS detection, typically exhibit an imbalanced distribution of instances, where benign traffic significantly outnumbers malicious traffic (Gupta & Kumar, 2024). This imbalance is further compounded by the fact that certain attack types are overrepresented in the dataset, while others, such as advanced or novel DDoS attacks, are underrepresented (Zhou et al., 2023). As a result, machine learning models tend to develop a bias toward the majority class (benign traffic) or the more frequent attack types, resulting in suboptimal performance, particularly in detecting minority attack classes (Zhou et al., 2023).

An intrusion detection system is hardware or software that monitors the network traffic for suspicious or abnormal behavior. An anomaly-based detection approach is more prevalent than signature-based detection in detecting network threats. Traditional IDS still is not capable of detecting unknown attacks. In contrast, a distributed denial of service attack (DDoS) is a cyber-attack that attacks the network's resources. Usually, it overloads the bandwidth and prevents the intended users from accessing the network. DDoS is a distributed denial-of-service attack that uses TCP and UDP packets to flood a server with traffic. A DDoS attack is different from DoS because it uses multiple unique IP addresses to perform its operation. The attacks affect over a hundred Internet companies.

Due to the increasing number of attacks on computer systems, the demand for computer security has also grown. This is why various firms are focusing on developing effective Intrusion Detection Systems (IDSs). A distributed denial of service attack is carried out by an attacker to disrupt the operation of a computer system. It can be initiated by exploiting a vulnerability in the network. In this field, various techniques have been surveyed to minimize the malicious actions within end systems and networks. Some of the studies prove that the use of network-based systems and host-based systems can improve the detection of attacks (Chawla, 2025).

2. Literature review

2.1. The Cloud Computing Environment

The cloud computing environment comprises many servers, storage devices, and networks. Figure 1 represents a cloud computing environment with many servers; each server runs multiple numbers of virtual machines (VMs). Using an application programming interface, these servers are connected using a network to share the resources between cloud

participants. This interface manages interactions between cloud participants., i.e., cloud service providers, service providers, and service users.

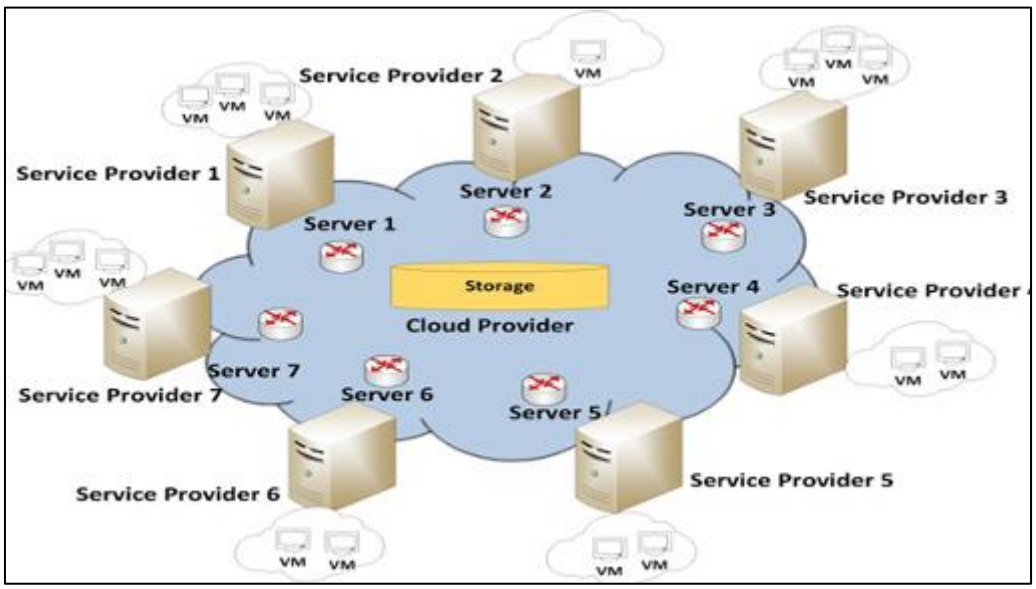

Figure 1 Cloud Computing Environment

The cloud service provider offers IaaS to service providers. IaaS equips and provides service providers with primary computing components such as servers, storage systems, network equipment, software applications, and other essential computing resources. Simultaneously, the service provider places web services in the cloud infrastructure as a set of VMs (Somani et al., 2017). Also, service providers can use on-demand services that allow them to obtain extra resources, when necessary, such as using additional central processing units (CPUs) or memory from VMs available in cloud computing (Kaaniche & Laurent, 2017). Nevertheless, the service provider must first pay the cloud provider using the pay-as-you-go model, which is a service that allows service providers to pay the cloud service provider when they require the use of VM resources (Sookhak et al., 2014), while service users with computers, mobile phones, and laptops can easily connect to cloud services over the internet (Kaaniche & Laurent, 2017).

2.2. Characteristics of Cloud Computing Environment

Cloud computing has five characteristics: on-demand self-service, broad network access, shared resources, elasticity, and the pay-as-you-go model. The main reasons for cloud computing's success depend on these cloud computing characteristics. In contrast, attackers may exploit these characteristics to launch DDoS attacks in a cloud computing environment (Kaaniche & Laurent, 2017).

2.2.1. On-Demand Self-Service

This characteristic enables cloud consumers to obtain extra resources like storage capabilities with no involvement of human beings, relating to the self-management functionality of shared resources (Kaaniche & Laurent, 2017). However, an attacker planning a DDoS attack would exploit this characteristic by sending fake requests to the cloud victim server to consume its resources and deny legitimate users access to the cloud victim server. The fake requests sent by attackers would cause intensive resource utilization, leading to a DoS on the victim server (Behal et al., 2017; Yu et al., 2012).

2.2.2. Broad Network Access

Legitimate cloud users can use heterogeneous devices, such as computers, tablets, mobile phones, etc. Therefore, the broad network access feature enables cloud users to access cloud services from anywhere and at any time; accessibility anywhere is generally achieved via standard internet protocols (Kaaniche & Laurent, 2017). However, an attacker could select different heterogeneous devices to operate as agents and use them to launch a DDoS attack. These devices are usually selected according to the vulnerabilities associated with these devices. Typically, an attacker compromises many devices to achieve powerful attacks, leading to DDoS (Bhuyan et al., 2015b).

2.2.3. Shared Resources

Cloud resources are shared between multiple service providers. These resources are not allocated to a particular service provider; rather, multiple providers can use the same resources. These shared resources are allocated and reallocated according to service providers' needs and requests. Multiple providers use shared resources depending on virtualization methods, in which one physical machine can run different operating systems by sharing the physical machine location (Kaaniche & Laurent 2017). However, an attacker who plans to consume shared resources on a target server will send fake requests to that server to overwhelm its resources, leading to a DoS on the victim server.

2.2.4. Elasticity

This characteristic allows a VM to expand and shrink resources while it operates. It also allocates extra storage, network bandwidth, memory, and CPUs to a VM when needed (Somani et al., 2017). Therefore, the cloud has the greatest capacity for allocating and releasing resources through self-provisioning property (Toosi et al., 2014). However, the bandwidth's self-provisioning property enabled by this characteristic is the main vulnerability that must be considered. Consequently, an attacker may cause DDoS attacks by exploiting the bandwidth under-provisioning by targeting an application or a service in the victim server (Xiao & Xiao, 2013).

2.2.5. Pay-As-You-Go Model

A service provider can use cloud computing resources by using the pay-as-you-go model without purchasing these resources. Resources may be added or deleted as needed by a cloud service provider. Cloud fees are commonly calculated hourly for cloud instances, i.e., a VM instance used by the service provider. Therefore, one hour is the lowest accounting period (Toosi et al., 2014). However, in the DDoS attack scenario, which may happen in the cloud environment, all cloud VM resources are exhausted if the cloud provider does not consider the accounting period. Therefore, cloud providers can manage DDoS attack scenarios by selecting one alternative between the two: the VM owner needs to pay before allocating additional resources using the pay-as-you-go model, or cloud resources will not be allocated to the VM owner because resources of a victim server that is hosted in cloud computing have run out during a DDoS attack (Deepali & Bhushan, 2017).

2.3. DDoS Attack Scenario in Cloud Computing

An attacker who plans to target a victim server on a cloud with a DDoS attack will take two steps to launch a DDoS attack. The attacker will first prepare a botnet or obtain a botnet network from booters that provide bots to customers as a fee-paid service and then launch a DDoS attack using a botnet (Bhuyan et al., 2015b; Santanna et al., 2015). The botnet is a large network of compromised machines, called "bots," controlled and managed by the botnet master, who works remotely. On the other hand, the launched attacks have different scenarios and require certain procedures to be coordinated in advance by the attacker (Behal et al., 2021, 2017; Bhatia, 2016; Bhuyan et al., 2015b; Gupta & Badve, 2017; Saravanan et al., 2016; Tao & Yu, 2013).

2.4. Detection Of DDoS Attacks in Cloud Computing

Researchers have extensively studied DDoS defense methods in cloud computing. Several approaches have been proposed to defend against DDoS attacks. Generally, DDoS attack defense methods are classified into three types: prevention, detection, and mitigation (Alarqan et al., 2019; Bonguet & Bellaiche, 2017; Shameli-Sendi et al., 2015). Indeed, detection methods against DDoS attacks are better than other defense methods, such as prevention and mitigation (Tao & Yu, 2013).

Attack prevention methods have a usability issue since they are applied to all users of services, whether legitimate or malicious, causing additional server computational costs and more response time when prevention is applied to legitimate users. Mitigation methods, in contrast, are used to help the server provide service to customers after DDoS has targeted the server cite (Somani et al., 2017). Therefore, attack detection mechanisms are an important element of defense (Bhuyan et al., 2016).

Attack detection is a process that involves analyzing running systems to identify malicious packets of DDoS attacks in network traffic or to identify malicious sources that lead to DDoS attacks (Shameli-Sendi et al., 2015). There are symptoms indicating that attack has occurred on the server, such as the decline of server performance before the server crashes; different performance measures may be used, such as more response times and timeouts for the server to respond to user requests. As a result, attack detection can be used before the server crashes (Somani et al., 2017).

Recently, detection approaches based on ML algorithms and deep learning (DL) and anomaly detection mechanisms based on information theory have become widely used to defend against DDoS attacks in cloud computing.

3. Method and materials

This section describes the proposed model and algorithm employed in this study, including data collection, data analysis, handling imbalanced data by using SMOTE, splitting the dataset into data training and testing, developing the model. The flowchart illustrates the process flow used to detect DDoS attacks using the ML model and the SMOTE technique in dealing with data imbalance problems. The process began with data collection from network traffic, followed by the preprocessing stage to clean and prepare the data before further analysis. After preprocessing, anomaly detection was carried out using the RF algorithm to identify suspicious or unusual data. The data detected as anomalous were then standardized to ensure that all features had a consistent scale, which is important for optimal model performance. After standardization, the data imbalance problem was addressed by applying the SMOTE technique to make the minority class more balanced. The balanced data are then reshaped to suit the RF model. For comparison, the data were also reshaped without and with SMOTE for training and testing respectively. The trained model was evaluated using the evaluation metrics to assess the effectiveness of the approach used in detecting DDoS attacks.

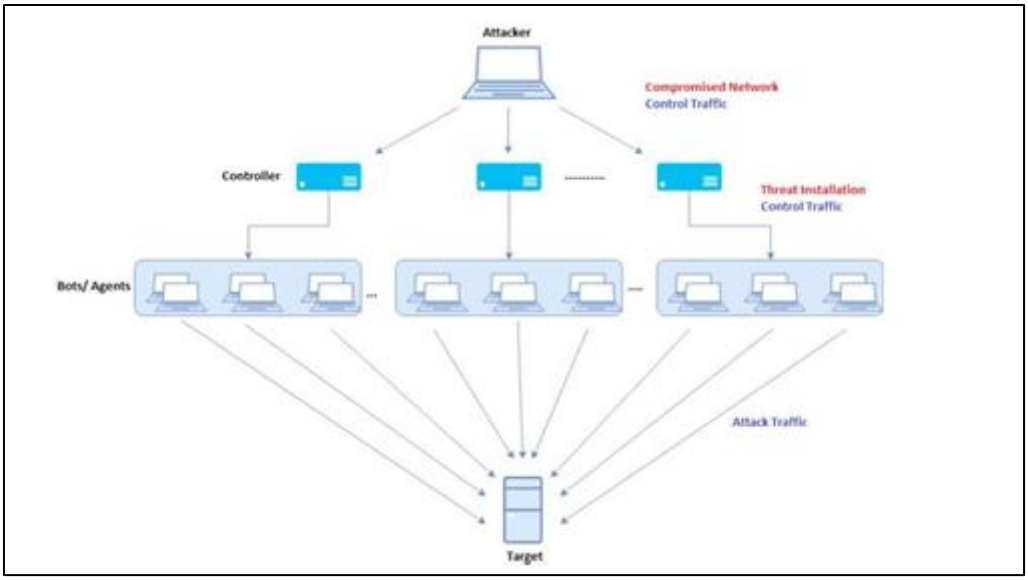

Figure 2 DDoS Attack Architecture (Heidenreich, 2018)

Table 1 Confusion Matric Explanation

Normal	Attack 1	Attack 2	Attack 3	Attack 4
Attack 1			-	
Attack 2	FP	TP	-	TN
Attack 3	TN	FP	-	TN
Attack 4			-	

To test the capability of the detection model, accuracy, precision, recall, F-measure, FPR, and specificity are used to evaluate the performance of the model. The mathematical equations of these measures are as follows (Rajput, 2019):

Where:

$$\text{Accuracy (ACC)} = \frac{TP+TN}{TP+TN+FP+FN}$$

$$\text{Precision (P)} = \frac{TP}{TP+FP}$$

$$\text{TPR/ Sensitivity/ Recall (R)} = \frac{TP}{TP+FN}$$

$$\text{F - Measure} = \frac{2(P*R)}{P+R}$$

$$\text{False-Positive Rate (FPR)} = \frac{FP}{FP+TN}$$

$$\text{Specificity} = \frac{TN}{TN+FP}$$

$$\text{FPR} = \frac{FP}{TN+FP} \text{ or } 1 - \text{Specificity}$$

True-Positive (TP): the number of attacks accurately identified as malware

Ture-Negative (TN): the number of normal accurately identified as benign

False-Positive (FP): the number of normal inaccurately identified as malware

False-Negative (FN): the number of attacks inaccurately identified as benign

3.1. Proposed Framework

Figure 3 highlights the DDoS attack detection framework. The framework has three phases. The first phase takes care of feature selection; the second phase handled the Imbalance class using and the third phase is the classification phase.

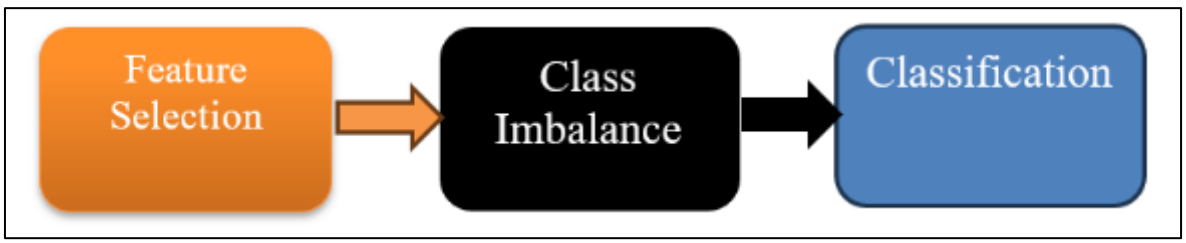

Figure 3 Summarized DDoS attack detection framework

4. Results

Table 2 Feature selection through SMOTE

No	Feature Name	No	Feature Name
1	Dst Port	21	Bwd Header Len
2	Flow Duration	22	Fwd Pkts/s
3	Tot Bwd Pkts	23	Bwd Pkts/s
4	TotLen Fwd Pkts	24	Pkt Len Max
5	TotLen Bwd Pkts	25	Pkt Len Mean

6	Fwd Pkt Len Max	26	Pkt Len Std
7	Fwd Pkt Len Mean	27	Pkt Len Var
8	Bwd Pkt Len Max	28	PSH Flag Cnt
9	Bwd Pkt Len Mean	29	ACK Flag C
10	Bwd Pkt Len Std	30	nt
11	Flow Byts/s	31	Pkt Size Avg
12	Flow Pkts/s	32	Fwd Seg Size Avg
13	Flow IAT Mean	33	Bwd Seg Size Avg
14	Flow IAT Max	34	Subflow Fwd Pkts
15	Flow IAT Min	35	SubFlow Bwd Byts
16	Fwd IAT TotFwd	36	SubFlow Bwd Pkts
17	IAT Mean	37	SubFlow Bwd Byts
18	Fwd IAT Max	38	Init Fwd Win Byts
19	Fwd IAT Min	39	Init Bwd Win Byts
20	Fwd Header Len		Fwd Seg Size Min

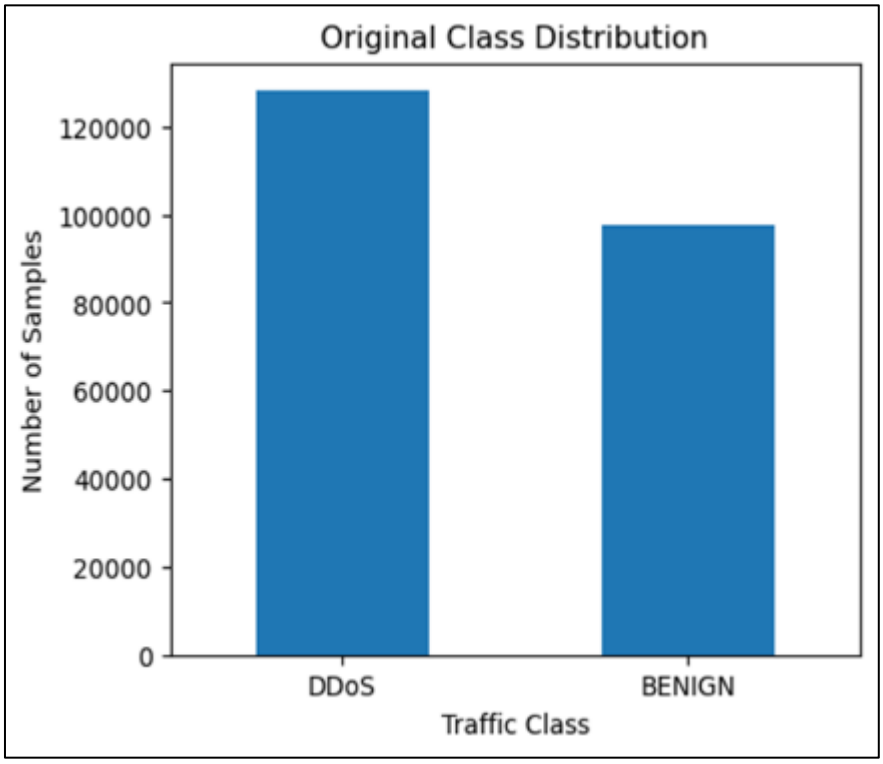

Figure 4 Class Distribution of the existing DDoS dataset as a result of class imbalance

5. Conclusion/Recommendations

Distributed Denial of Service (DDoS) attacks have emerged as a formidable threat, aiming to disrupt the availability of services by overwhelming network resources (Jin et al., 2024). The detection and mitigation of such attacks are paramount to maintaining the integrity and reliability of network infrastructures. Therefore, Intrusion detection systems (IDSs) should be used to build a system that should be able to identify and enhance DDoS attacks using artificial intelligence.

This paper comprehensively surveys the state-of-the-art detection solutions for DDoS attacks in cloud computing. It examined cloud computing environment components and characteristics that attackers exploit to launch attacks, particularly the ways in which botnets compromise service availability and deny legitimate users access to victim servers hosted in cloud computing. The paper provides a detailed taxonomy of DDoS attacks targeting cloud infrastructure and applications, offering valuable insights for security researchers to manage cloud vulnerabilities better and present an effect feature selection with SMOTE as seen in table 2. The study provides a uniform framework for enhancing DDoS attack detection methods in cloud computing while highlighting future research directions.

Compliance with ethical standards

Acknowledgements

Our sincere thanks go to the authors whose works have help to achieve this research. We also appreciate our colleagues who contributed in one way or the other to the realization of this research.

Disclosure of Conflict of interest

The authors declare no conflict of interest.

References

[1] Alanazi, S., Anbar, M., Karuppayah, S., Al-Ani, A. K., & Sanjalawe, Y. K. (2019). Detection techniques for DDoS attacks in cloud environment. In V. Piuru, V. E. Balas, S. Borah, & S. S. S. Ahmad (Eds.), Intelligent and Interactive Computing: Proceedings of IIC 2018. (pp. 337–354). Springer.

[2] Amin, A., Li, Z., & Zhang, H. (2023). DDoS attack detection using machine learning: Challenges and approaches. Journal of Cybersecurity and Network Security, 11(2), 129- 145. https://doi.org/10.1002/jcn.2023

[3] Bagui S. and K. Li, "Resampling imbalanced data for network intrusion detection datasets," Journal of Big Data, vol. 8, no. 1, p. 40537, 2021, doi: 10.1186/s40537-020-00390- x.

[4] Behal, S., Kumar, K., & Sachdeva, M. (2021). D-FAC: A novel ϕ-Divergence based distributed DDoS defense system. Journal of King Saud University. Computer and Information Sciences, 33(3), 291–303. DOI: 10.1016/j. jksuci.2018.03.005

[5] Bonguet, A., & Bellaiche, M. (2017). A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing. Future Internet, 9(3), 43. DOI: 10.3390/fi9030043

[6] Deepali & Bhushan. K. (2017). DDoS attack defense framework for cloud using fog computing. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT) (pp. 534–538). IEEE.

[7] Gupta, R., & Kumar, S. (2024). Improving network intrusion detection using data balancing techniques. International Journal of Network Security, 19(2), 135-150. https://doi.org/10.1016/j.ijnse.2024.01.007

[8] Gupta, B. B., Gaurav, A., & Peraković, D. (2021). A big data and deep learning based approach for dDoS detection in cloud computing environment. In 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE).(pp. 287–90). IEEE. DOI: 10.1109/GCCE53005.2021.9622091

[9] Islamia, J. M., & Delhi, N. (2018). Comparative Study of Big Ten Information Security Management System Standards, 5(2), 5–14.

[10] Jin, Z., Zhang, H., & Lee, S. (2024). A survey on DDoS attack detection techniques in modern networks. Nature Communications, 13(1), 45-60. https://doi.org/10.1038/s41598- 024-84879y

[11] Johnson, J.M.; Khoshgoftaar, T.M. Survey on deep learning with class imbalance. J. Big Data 2019, 6, 27. [Google Scholar] [CrossRef]

[12] Jonker et al. (2024) - Real-Time DDoS Detection Using Machine Learning [IEEE Transactions on Dependable and Secure Computing]

[13] Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications, 111, 120–141. DOI: 10.1016/j.comcom.2017.07.006

[14] Kumar, A., Kumar, S., & Meena, R. (2021). Hybrid CNN-XGBoost model for DDoS attack detection. International Journal of Computational Intelligence Systems, 14(1), 35-50. https://doi.org/10.1080/18756891.2020.1845357.

[15] Luque A., A. Carrasco, A. Martín, and A. de las Heras, "The impact of class imbalance in classificationperformance metrics based on the binary confusion matrix," Pattern Recognition, vol. 91, pp. 216– 231, Jul. 2019, doi: 10.1016/j.patcog.2019.02.023.

[16] Mohammad A., Bahari B., Ammar A., Mohammad A., Mohammed A., & Varsha A. (2025) 'Information Theory-Based DDoS Attack Detection in Cloud Computing: A Systematic Survey of Approaches, Challenges, and Future Directions' International Journal of Cloud Applications and Computing Volume 15 • Issue 1 • January-December 2025

[17] Wang, S., & Yao, X. (2013). Multiclass imbalance problems: Analysis and potential solutions. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 43(4), 1119-1130.

[18] Raghuwanshi B. S. and S. Shukla, "SMOTE based class-specific extreme learning machine for imbalancedlearning," Knowledge Based Systems, vol. 187, p. 104814, 2020, doi: 10.1016/j.knosys.2019.06.022.

[19] Santanna, J. J., Van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). Booters — An analysis of DDoS-as-a-service attacks. In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 243– 251). IEEE. DOI: 10.1109/INM.2015.7140298

[20] Shameli-Sendi, A., Pourzandi, Fekih-Ahmed, M., & Cheriet, M. (2015). Taxonomy of distributed denial of service mitigation approaches for cloud computing. Journal of Network and Computer Applications 58, 165–179. DOI: 10.1016/j.jnca.2015.09.005

[21] Saravanan, R., Shanmuganathan, S., & Palanichamy, Y. (2016). Behavior-based detection of application layer distributed denial ofservice attacks during flash events. Turkish Journal of Electrical Engineering and Computer Sciences, 24, 510–523. DOI: 10.3906/elk-1308- 188

[22] Singh, R., Kumar, A., & Pandey, R. (2023). DDoS attack detection using deep learning techniques:A systematic review. Computers & Security, 111, 102462. https://doi.org/10.1016/j.cose.2021.102462

[23] Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30–48. DOI: 10.1016/j.comcom.2017.03.010

[24] Sookhak, M., Talebian, H., Ahmed, E., Gani, A., & Khan, M. K. (2014). A review on remote data auditing in single cloud server: Taxonomy and open issues. Journal of Network and Computer Applications, 43, 121–141. DOI: 10.1016/j.jnca.2014.04.011

[25] Tao, Y., & Yu, S. (2013). DDoS attack detection at local area networks using information theoretical metrics. In 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 233–240). IEEE. DOI: 10.1109/TrustCom.2013.32

[26] Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Interconnected cloud computing environments: Challenges, taxonomy, and survey. ACM Computing Surveys, 47(1), 1–47. DOI: 10.1145/2593512

[27] Triguero I., M. Galar, D. Merino, J. Maillo, H. Bustince, and F. Herrera, "Evolutionary undersampling for extremely imbalanced big data classification under apache spark," 2016 IEEE Congress on Evolutionary Computation (CEC), pp. 640– 647, 2016, doi: 10.1109/CEC.2016.7743853.

[28] Van J. Hulse, T. M. Khoshgoftaar, and A. Napolitano, "Experimental perspectives on learning from imbalanced data," ICML '07: Proceedings of the 24th international conference on Machine learning, 2007, vol. 227, pp. 935–942, doi: 10.1145/1273496.1273614.

[29] Xiao, P., Qu, W., Qi, H., & Li, Z. (2013). Detecting dDoS attacks against data center with correlation analysis. Computer Communications, 67, 66–74. DOI: 10.1016/j.comcom.2015.06.012

[30] Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y., & Tang, F. (2012). Discriminating DDoS attacks from flash crowds using flow correlation coefficient. IEEE Transactions on Parallel and Distributed Systems, 23(6), 1073–1080. DOI: 10.1109/TPDS.2011.262

[31] Zang, M., E. O. Zaballa, and L. Dittmann, ''SDN-based in-band DDoS detection using ensemble learning algorithm on IoT edge,'' in Proc. 25th Conf. Innov. Clouds, Internet Netw. (ICIN), Mar. 2022, pp. 111–115.

[32] Zargar, S. T., Joshi, J., & Tipper, D. (2023). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046-2069.

[33] Zhou, J., Yang, Z., & Zhao, L. (2023). Detecting DDoS attacks in highly imbalanced network datasets: A deep learning approach. IEEE Access, 11, 34567-34580. https://doi.org/10.1109/ACCESS.2023.1234567