Received: 18 April 2023 | Revised: 22 August 2023 | Accepted: 18 December 2023

DOI: 10.1002/ett.4934

SURVEY ARTICLE

WILEY

Uncovering collateral damages and advanced defense strategies in cloud environments against DDoS attacks: A comprehensive review

Priyanka Verma[1] | **Nitesh Bharot**[1] | **John G. Breslin**[1] | **Mukta Sharma**[2] | **Nisha Chaurasia**[3] | **Ankit Vidyarthi**[4]

[1]Data Science Institute, University of Galway, Galway, Ireland

[2]Great Lake Bioenergy Research Center, Michigan State University, East Lansing, Michigan, USA

[3]Department of Information Technology, Dr. B.R. Ambedkar National Institute of Technology Jalandhar, Jalandhar, Punjab, India

[4]Department of CSE&IT, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India

Correspondence
Priyanka Verma, Data Science Institute, University of Galway, Galway, Ireland.
Email: priyanka.verma@universityofgalway.ie
Ankit Vidyarthi, Department of CSE&IT, Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India.
Email: dr.ankit.vidyarthi@gmail.com

Abstract

Cloud computing (CC) offers on-demand computing and resources to users, and organizations, and is also used in many human-centric intelligent systems. Attacks in cloud networks cause huge damage to service providers and users. Distributed Denial of Service (DDoS) is one of them that greatly impacts the cloud network. The unavailability of resources is the major concern pertaining to cloud service and resources. Apart from the direct targets of a DDoS attack, there are also indirect effects on non-targets within a cloud network. These effects on the non-target stakeholders of the cloud are called collateral damages. However, this area of research is not explored much by researchers. Thus, the defense methods pertaining to direct and indirect effects need to be explored. This article aims to describe the consequences of DDoS attacks and the solutions available in the cloud network. The novelty of this article lies in shedding light on the indirect impacts of DDoS in cloud networks and possible solution approaches. The article also provides a comparative analysis of the existing defense solution under different categories and available tools and datasets to evaluate the proposed solutions. The article also mentions the solution considerations and effective solution scenarios. The idea behind this article is to impart guidelines to the researchers, for developing efficient defense solutions against direct target and indirect target DDoS attacks. Moreover, the research shortcomings, pros–cons, and existing challenges are outlined, and directions for future research are mentioned.

1 | INTRODUCTION

Cloud computing (CC) gives an on-demand mechanism through the internet for accessing services, assets, and applications over the internet. It has induced changes in the working of the IT industry by utilizing the CC platform for different needs such as infrastructure, storage, and processing. The five key features of the cloud identified by NIST are an on-demand resource, resource sharing, ubiquitously accessing the network, quick flexibility, and pay-as-you-go.[1] However, withstanding various benefits, cloud environments are powerless against different kinds of attacks. Perhaps Distributed Denial of Service (DDoS) is a supremely fabled attack, as it results in service interruption, bad client experience, and extreme financial losses prompting unsustainability, for organizations utilizing distributed computing. In this attack, an assailant expects to exhaust network bandwidth and limit or process assets by overpowering it with demands.

The significant motivation inspiring DDoS attacks can be coercion, an exhibit of attack abilities, defacement, hacktivism, business competition, interruption from exfiltration, and other data burglary exercises.

DDoS attack consequences in cloud networks are different from the ones in regular IT networks. Apart from the general effects of DDoS such as service disruption, economic loss, downfall in reputation, and mitigation costs. There are some additional consequences added to the cloud network are; extra costs caused due to auto-scaling, extra resources consumed by the attack, and collateral damages to non-targets. Moreover, DDoS in the cloud also results in an economic denial of sustainability (EDoS) attack.[2] Here, multiple malicious requests are sent by attackers for consuming the resources which are provisioned for the victim machine. As cloud uses a dynamic pricing model and can add extra resources using an autoscaling feature to maintain the desired quality of service (QoS), which results in high economic damages and billing costs. In this situation, due to attacks, more and more resources are added and eventually, the victim has to face economic unsustainability.

Alongside the inaccessibility of service and resources due to attack, some different damages which might happen because of service downtime are long and short-term damages to the business. According to recent DDoS statistics, one in every five businesses has been the subject of a DDoS attack. The average size of an attack is steadily increasing. Nowadays, attackers have advanced methods for enhancing the impact of the attack. The maximum data transfer rate during a DDoS had changed dramatically between 2000, when it was just 8 Gbps, rising to 600 Gbps in 2017.[3]

For DDoS attackers, there are different free devices accessible on the web and it has become a simple way for aggressors to complete the attack. There are different solutions available in the literature to defend against DDoS attacks in cloud networks such as detection, prevention, and mitigation techniques. Different datasets are publically available for training and testing of the proposed approaches, that is, these available datasets are utilized as benchmarks for attack detection. Thus, the defense frameworks can be effectively tried on these datasets, and if achieving good results, then the framework will work in any circumstance. The design of a defense against DDoS attacks must consider various execution challenges, compromises in setting protective mechanisms, and other factors.

1.1 | Attack statistics

Cloud resources are a primary target of DDoS attacks as whole data is stored at a single geographic location and is accessed via the internet. As a result, the cloud server is more vulnerable to such attacks. This section looks at data on DDoS attack consequences and penetration levels in cloud environments.

DoS attacks are presently listed by network security organizations as the top concern for service providers. DoS attacks account for 87% of malicious attacks on service providers, as per NETSCOUT Arbor's thirteenth report,[4] however the fourteenth report[5] characterized it as 95%. As per Akamai's State of the Internet, Summer 2018 report,[6] there is an increase of 16% of DoS attacks on their networks in the first half of 2018 compared to the first half of 2017. Amazon asserted that during the I_{st} quarter of 2020, they encountered DoS 2.3 Tbps.[7]

The time duration of the attack is an important factor, it can be 30 min or it might take longer than a month. This shows that the defense methods ought to be sufficiently quick to identify and filter these attacks on schedule before any damage is brought about. Arbor reports that Reference 8 biggest revealed attack, which spans under 6 h representing almost 50% of the answers from associations that were studied as displayed in Figure 1. Around 11% of organizations experienced spans of more than a multi weeks for their biggest observed attacks showing that aggressors can be extremely relentless in attacking.

DDoS attacks are bifurcated into protocol-based, application-layer, and volume-based attacks. A volume-based attack involves sending a lot of traffic to the target to use up all of its network bandwidth. The resources of the targeted machine are depleted in a protocol-based attack. In an attack at the application layer, the web server is destroyed by sending actual messages/signals that take advantage of the server program's flaws. According to Arbor Networks, 20% of organizations reviewed have dealt with application layer attacks, 24% have dealt with protocol-based attacks, and 61% have dealt with volume-based attacks.

1.2 | Motivation

In the last few years, various surveys on DDoS attacks along with their related solution techniques in cloud environments are reported. However, some of the effects of DDoS attacks and their solution methods are not much expressed in such pertaining literature and surveys. Therefore, the major reason behind formulating this survey paper is:

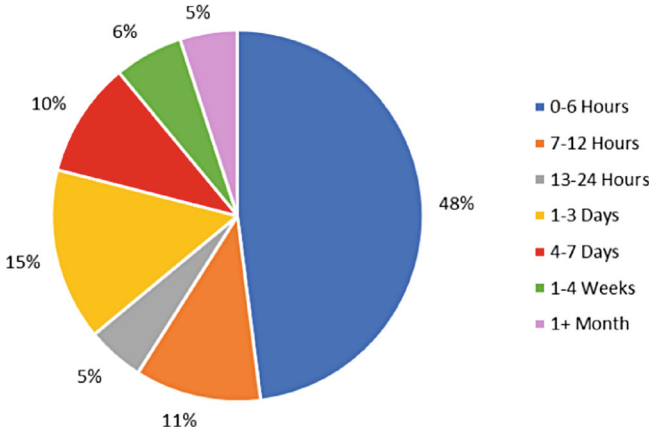

FIGURE 1 Duration of largest DDoS attack.[8]

- The available surveys do not adequately cover the specific classification of DDoS defense solutions for direct and indirect attack effects.
- The collateral consequences of DDoS attacks on non-targets in a cloud environment are not covered in the existing surveys.
- The parametric comparison between the existing defense approaches for the direct and indirect attack is not available in the existing surveys. This comparison helps the new researchers to get a benchmark above which they have to proceed with their research.

In order to reduce the effects of such attacks, it is imperative to review the DDoS solution, especially with regard to dealing with collateral damage from DDoS attacks on cloud networks.

1.3 | Contribution

This article shows the research work and development in the context of DDoS defense against the direct and indirect (collateral damages) attack effects in a cloud environment. A comprehensive survey and in-depth vision of the solution approaches for direct and indirect attack effects are also presented. To the best of the author's knowledge, this study is the first of its type to analyze the collateral harm brought on by a DDoS attack and the available remedy. The significant contributions of the comprehensive survey paper are given as:

- Detailed analysis of collateral damages at multiple levels: this research innovatively introduces a comprehensive exploration of collateral damages resulting from DDoS attacks at various levels of cloud infrastructure. The study provides an in-depth analysis of how such attacks can indirectly impact diverse facets of cloud networks, thereby broadening the overall understanding of DDoS implications.
- New taxonomy of DDoS attacks: this study considers DDoS attacks in a cloud context, highlighting both direct and indirect (collateral) damages. Significantly, this work introduce a novel taxonomy of DDoS attack techniques that encompasses both direct and indirect targets. This fresh perspective fosters a more holistic approach to understanding and combating DDoS threats.
- Comparative analysis of defense approaches: this work deliver a meticulous comparison of various defense approaches for both direct and indirect targets. This comparison takes into account key aspects such as the technique used, the dataset employed, a summary of findings, and the limitations of each approach. This nuanced analysis contributes to a data-driven evaluation of defense strategies, encouraging the refinement and development of more robust solutions.
- Alternate viewpoint of DDoS attacks: our study depicts a unique perspective of DDoS attacks in cloud infrastructure. It demonstrates the attack's effects on non-target stakeholders within the cloud environment, showcasing the breadth of potential damage. It also presents a range of solution spaces for mitigating such collateral damages, expanding the scope of current defense mechanisms.

- Effective solution scenarios: this research takes the crucial step of outlining solution considerations and proposing effective solution scenarios at different levels in the cloud environment. These aim to enhance DDoS defense mechanisms against both direct and indirect attacks. This practical contribution aids cybersecurity practitioners in designing and implementing improved defense strategies, offering valuable guidance for real-world applications.

Figure 2 shows the overall structure and flow of the article and Table 1 presents the comparison of our survey with other existing survey papers in the field.

1.4 | Paper selection criteria

To conduct a comprehensive review on uncovering the direct and indirect implications of DDoS attacks in cloud environments and crafting advanced defense strategies, this survey employed a systematic literature review process to select the most relevant papers. The paper selection process for the survey consisted of the following steps:

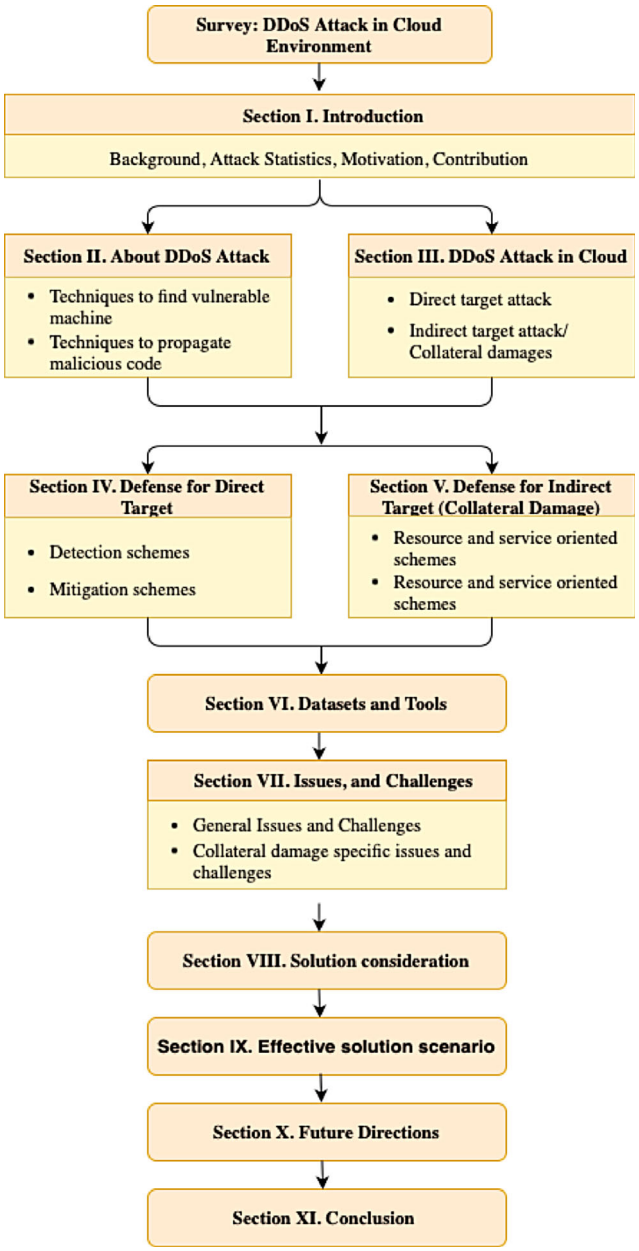

FIGURE 2 Structure of this survey paper.

TABLE 1 Comparison with existing survey.

Author	Focus	Coverage		Defence method			S.R.	Remark
		DT	IT	D	P	M		
Gupta and Badve[9]	Describing DoS and DDoS attack variants and their solution hierarchy.	√	×	√	√	√	×	Classified defense mechanism for direct targets, based on deployment location and the time of applying it. Defense for indirect targets not discussed.
Somani et al.[10]	Discuss DDoS in the cloud, its issues, taxonomy, and future direction.	√	√(L)	√	√	√	√	Categorize defense solutions in three categories namely, detection, prevention, and mitigation. Provided guidelines for developing better solutions.
Shamelisendi et al.[11]	DDoS mitigation taxonomy and mitigation approaches for DDoS defense.	√	×	×	×	√	×	Discussing mitigation approaches against DDoS attacks in the cloud. The behavior of these mitigation approaches is also compared under the cloud environment.
Somani et al.[12]	DDoS defense approach in cloud and requirement, trends, and future direction.	√	×	√(L)	√(L)	√(L)	√(L)	Lacks exhaustive review on defense approaches. Also, discusses the requirement and trends for designing better answers for direct targets.
Osanaiye et al.[13]	DDoS attacks in cloud and its conceptual cloud mitigation framework.	√	×	√	×	×	√(L)	Discuss detection mechanism for direct targets of attack. classify detection mechanisms as signature, anomaly, and hybrid approaches. These approaches are compared based on the deployment location.
Yan et al.[14]	SDN-based DDoS survey, research issues, and challenges.	√	×	√	√	√	√	Discuss the new trends and characteristics of DDoS attacks in cloud computing, and provide a comprehensive survey of defense mechanisms against DDoS attacks using SDN. The comparison between the defense approaches is not provided.
Chaudhary et al.[15]	DDoS attack and its defense mechanism.	√	×	√	√(L)	√(L)	×	Classification of defense approaches are done as an anomaly, signature, and hybrid. The defense mechanism discussed is limited to direct targets of attacks, and defense for collateral damages are not discussed.

(Continues)

TABLE 1 (Continued)

Author	Focus	Coverage		Defence method			S.R.	Remark
		DT	IT	D	P	M		
Srinivasan et al.[16]	Impact analysis of DDoS and its detection, prevention, and mitigation approaches.	√	×	√	√	√	×	Discuss the impact of DDoS in the cloud environment and compared the defense approaches for direct target attack based on their strength, limitations, and challenges.
Alarqan et al.[17]	Detection mechanism against DDoS in the cloud.	√	×	√	×	×	×	Classify the detection mechanism and compared them based on their strength and limitation only for direct target attack.
This survey	Impact analysis of DDoS on direct and indirect targets. Defense approach for both the direct and indirect target DDos attack, issues, challenges, solution requirement, and future direction.	√	√	√	√	√	√	A detailed classification and comparison of DDoS attacks, tools, along with defense approaches for direct and indirect target attack. Analyzing collateral damages of DDoS on various stakeholders of the cloud. Complete analysis of defense solutions with their strength and limitations. Solution direction for both direct and indirect target attacks is also discussed.

Abbreviations: D, detection; DT, direct target; IT, indirect target; M, mitigation; P, prevention; S.R., solution requirements.

- *Database and search query selection*: Identified relevant databases and search engines, such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar, to conduct a thorough search for research papers on DDoS attacks in cloud environments and defense strategies. The search queries are formulated using appropriate keywords and phrases related to the topic, such as DDoS attacks, cloud environments, indirect attacks, collateral damages, EDoS attacks, defense strategies, detection methods, and mitigation methods to ensure a wide range of results.
- *Initial screening*: Upon retrieving the search results, an initial screening is performed by selecting a time window from 2006 to January 2023. Then further shortlisting is done by analyzing the title, abstract, and keywords of the papers to determine their relevance to the survey's scope. Irrelevant or unrelated papers were excluded at this stage.
- *Full-text review*: After the initial screening, a full-text review of the remaining papers was conducted. During this phase, papers were assessed based on their contributions, methodology, findings, and relevance to the survey topic. The papers are excluded that did not meet our inclusion criteria or lacked significant contributions to the field of DDoS attacks and defense strategies in cloud environments for direct and indirect effects.
- *Reference and citation analysis*:To ensure that no relevant papers were overlooked, a reference and citation analysis on the included papers is also performed. The bibliography of the selected papers is also analyzed and identified additional relevant papers that were not discovered during the initial search.
- *Final paper selection*: After completing the above steps, a final list of papers is compiled that met our inclusion criteria and offered valuable insights into the indirect implications of DDoS attacks in cloud environments and advanced defense strategies. These papers were then thoroughly analyzed and discussed in the survey.

By following this systematic process, we ensured that the selected papers were relevant, comprehensive, and representative of the current state of research in the field, providing a solid foundation for the comprehensive review of DDoS attacks and defense strategies in cloud environments.

Further, the papers on defense approaches under each category are majorly considered and compared in the respective tables based on the technique used, summary, limitation, and dataset/solution level within each defense category.

The rest of the article is organized as follows: Section 2 briefly discusses DDoS attacks and techniques to launch DDoS attacks. Section 3 describes the effects of DDoS attack in a cloud environment and introduces collateral damages. Sections 4 and 5 present the review of techniques available to handle direct and indirect/collateral damages, respectively. Section 6 discusses the available DDoS tools and datasets. Section 7 outlines the identified issues and challenges. Sections 8 and 9 present the solution consideration and effective solution scenario while designing the new solution. Section 10 gives the future direction and Section 11 concludes the work.

2 | ABOUT DDOS ATTACK

Cloud security is governed by three main components confidentiality, integrity, and availability. Hindering any of one component may cause security issues for the system. The main trouble caused by DDoS attacks is the unavailability of resources. The attacker deteriorates the QoS. Figure 3 shows the DDoS attack launched to affect the target network. It is launched on the system by sending many malformed packets, upon which the system or victim is not able to handle such packets and gets shut down or reboots the system or may get busy in processing these malformed packets. Because of this activity, real cloud users will be denied access to the services which they want to use. The main targets of DDoS attacks are bandwidth, infrastructure, and applications.

2.1 | Techniques to find vulnerable machine

- **Random scanning:** The malicious system, whether it is the attacker or one of the infected machines, randomly chooses the IP address and looks for a machine vulnerability. When it finds the vulnerability, then its code will forcefully enter the machine and install itself. It is a very fast way of recruiting the zombie machine because it propagates in a very fast manner in the network.

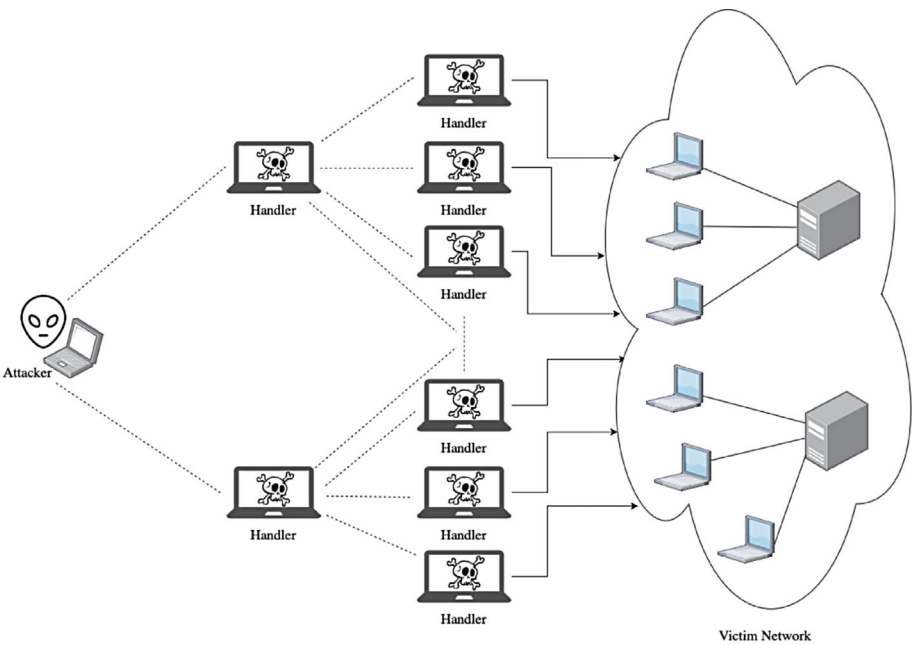

FIGURE 3 DDoS attack launched towards the target cloud network.

- **Hit-list scanning:** Before launching of attack, the attacker prepares a list of potentially vulnerable machines. From the list, it installs the malicious code in the machine and divides the rest of the list in two half, and give one half of the list to the new zombie machine, and will continue with the other part, and the process goes on.
- **Topological scanning:** The information present in the existing victim machine is used by the topological scanning process to find the next victim machine. The compromised machine looks for the URL of the next target machine that it wants to infect. The accuracy of finding vulnerable machines in this scheme is very high, and this technique is much more similar to hit list scanning.
- **Local subnet scanning:** The attacker or the compromised machine search for the target in its local subnet using the information mentioned in the local address space. So it cannot be identified by the firewall. This technique can be used with other techniques in conjunction to prepare an army for launching the attack.
- **Permutation scanning:** All the machines share a single pseudo-random permutation set of IP addresses. This permutation list was created using a 32-bit block cipher's pre-selected key. A machine will randomly begin scanning if it becomes infected while performing permutation scanning.

2.2 | Techniques to propagate malicious code

- **Central source propagation:** This method transfers malicious malware from a central point to the newly compromised system when a vulnerable machine is found and turns into a zombie machine. The tool kit will instantly launch in the compromised machine after being transferred.
- **Back chaining propagation:** The attack tool kit is transferred by the attacker to the newly compromised system. The attack tool installed in the attacker contains some special methods that allow the attacker to accept the connection from the newly compromised system to transfer the tool kit.
- **Autonomous propagation:** Here the attack tool is broken up and simultaneously transferred by the host attacker to build a zombie machine.

3 | CLOUD AND DDOS ATTACKS

DDoS attack in a cloud environment poses unique challenges compared to a traditional network. The elastic and decentralized nature of the cloud offers advantages such as rapid scaling, resilience, and global distribution, which aids in mitigating the consequences of DDoS attacks. However, cloud environments can be more susceptible to advanced, multi-vector attacks that exploit application vulnerabilities and infrastructure weaknesses. Additionally, due to shared resources, cloud customers may experience collateral damage from attacks targeting other users. So considering the effects of characterization, a brand-new taxonomy of DDoS attack is shown in Figure 4. Based on brand-new taxonomy, DDoS attacks are classified as direct and indirect attack.

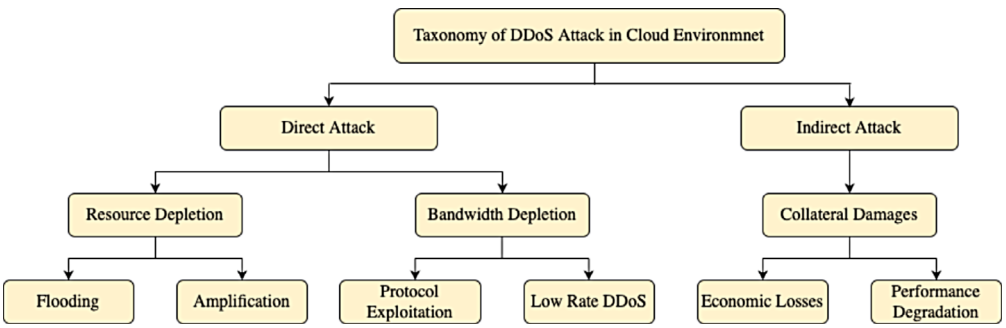

FIGURE 4 DDoS attacks taxonomy for a cloud computing environment.

3.1 | Direct attack

An intentional effort to shut down a specific network, server, or website from operating normally by saturating it with an influx of malicious traffic, is called a direct DDoS attack. This request surge overwhelms the target system, exhausting its resources and bandwidth and causing a service outage or slowdown. DDoS attacks could be broadly divided into resource depletion and bandwidth depletion. The former attack exhausts the target's processing capacity, memory, or other system resources. Examples include SYN flood attacks and application layer attacks, which exploit vulnerabilities in server software or protocols to overwhelm server resources. On the other hand, bandwidth depletion attacks aim to saturate the target's network capacity, making it difficult for legitimate traffic to pass through. These attacks, such as volumetric or UDP flood attacks, generate massive traffic to consume the target's bandwidth. Both types of DDoS attacks ultimately aim to disrupt services and cause negative impacts on the targeted organization.

3.2 | Indirect attack/collateral damages

DDoS attacks in traditional networks and cloud infrastructure have distinct effects, making cloud infrastructure more susceptible to harm. Cloud infrastructure's on-demand computing, auto-scaling, virtualization, and load-balancing features allow it to continue servicing requests during attacks. However, DDoS attacks in the cloud can consume all resources, affecting the targeted virtual machine (VM) and other stakeholders and causing collateral damage. These effects will result in either economic losses or may result in performance degradation. Figure 5 shows the DDoS attack launched for VM 1 of host 1 in the cloud with target resources like CPU, bandwidth, memory, and disk.

The victim VM, sibling VMs, host physical machine, other host physical machines, VMs on other host machines, users of attacked and co-hosted VMs, cloud providers, and cloud consumers are just a few of the stakeholders in a cloud system.[18]

Collateral damages can be divided into multiple tiers, from internal to higher levels, taking into account the presence of stakeholders at various levels within the cloud architecture. Collateral damages can now be defined and understood more clearly because of this categorization. Collateral damages[18] can occur at various levels, including within the victim VM (Level 0), co-hosted VMs (Level 1), other physically present hosts and their related VMs (Level 2), and entire cloud (Level 3). As a result, DDoS attacks in cloud environments can have widespread and severe consequences, impacting various stakeholders and potentially capturing the entire cloud infrastructure if not detected and stopped promptly. The levels taken into account in this situation can be described as follows[19]:

- **Level 0—Internal collateral damage:** This level of collateral damage occurs within the victim VM itself. As shown in Figure 6, when a specific service inside the VM is under attack, it consumes all the available resources allocated to that VM. Consequently, other services within the same VM are starved of resources and indirectly affected by the attack. This internal collateral damage impacts the performance and availability of all services running within the targeted VM, leading to a degraded user experience.[20-22]

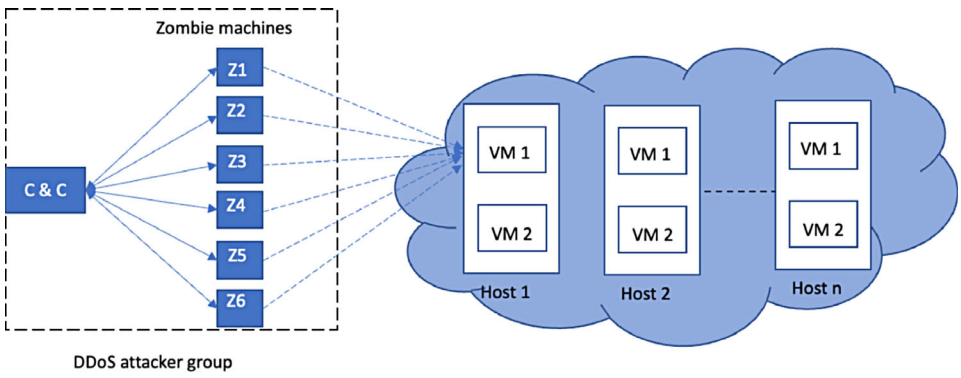

FIGURE 5 DDoS attack in cloud infrastructure.

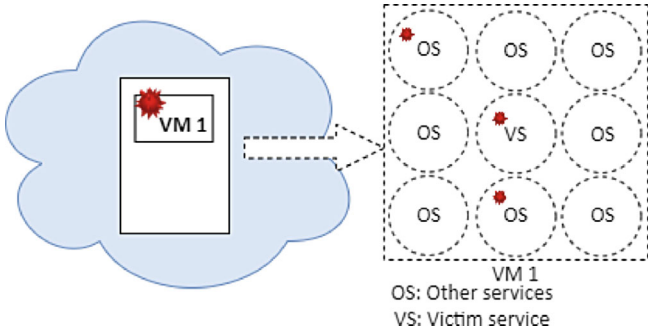

FIGURE 6 Level 0: Victim machines facing Internal collateral damages.[19]

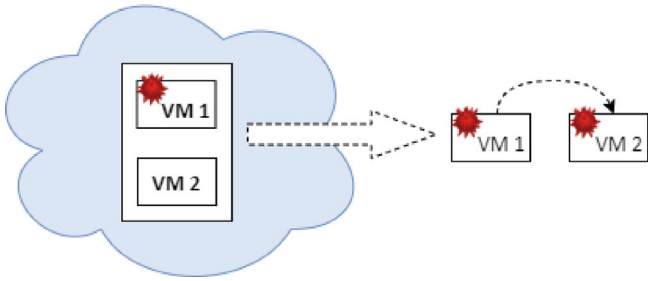

FIGURE 7 Level 1: Collateral damages on sibling VM's inside the same host.[19]

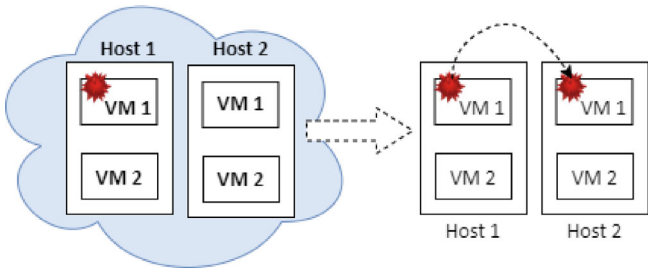

FIGURE 8 Level 2: Collateral damages at the sibling host level and on its VMs.[19]

- **Level 1—Co-hosted VM collateral damage:** At this level, the collateral damage extends to other VMs co-hosted on the same physical host as the victim VM.[12,18] When the attacked VM becomes overloaded, the load balancer may transfer some of its load to the co-hosted VMs to maintain service continuity as shown in Figure 7. The co-hosted VMs then unwittingly serve malicious requests, wasting their resources and potentially impacting their performance. This level of collateral damage affects other VMs sharing the same host, even though they were not the actual targets.
- **Level 2—Host level collateral damage:** This level of collateral damage occurs when the attack impacts other physically present hosts and their associated VMs in cloud infrastructure, as shown in Figure 8. If the host machine becomes overloaded and unable to handle the attack, it may perform VM migrations to meet the demands.[18] This migration process can affect other hosts and their associated VMs, even if they were not the actual victims of the attack. The attack can impact the overall performance and availability of these non-targeted hosts and VMs.
- **Level 3—Cloud-wide collateral damage:** At this level, the DDoS attack is so severe that it can potentially capture and disrupt the entire cloud infrastructure.[12,23] When the attack strength is intense, it can spread across host physical machines, affecting all the associated VMs and services as depicted in Figure 9. In case of unidentified or unresolved attacks for an extended period, it can eventually consume the entire cloud's resources, leading to widespread service

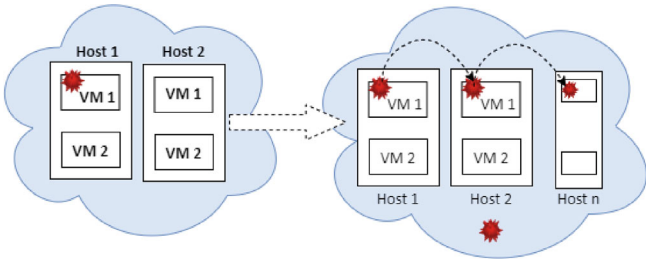

FIGURE 9 Level 3: Collateral damages on whole cloud infrastructure.[19]

degradation or outage. This level of collateral damage has the most significant impact, affecting all stakeholders within the cloud ecosystem, including cloud providers, customers, and users.

There are several potential issues and challenges associated with the indirect effects of DDoS attacks in cloud networks:

- Shared resource drain: Cloud services rely on shared resources. A DDoS attack, even if targeted at a single user or service, can drain resources affecting others sharing the same infrastructure.
- Service degradation: Indirect effects of DDoS attacks may cause degradation of service quality, resulting in slow performance or unexpected downtimes for users not initially targeted by the attack.
- Mitigation challenges: The indirect effects can be subtle and may not trigger traditional DDoS defense mechanisms. Developing mitigation strategies that can handle these effects is a complex challenge.
- Difficult detection: Detecting the indirect effects of DDoS attacks can be difficult, as they can be masked as normal network congestion or other non-malicious issues.
- Inadequate isolation: In cloud environments, isolation between different users' resources can be imperfect. A DDoS attack may exploit these imperfections, causing effects that spill over onto other users.
- Economic costs: Collateral damage from DDoS attacks can result in significant economic costs. These can include compensation to affected users, revenue losses from service disruptions, and increased expenses for improved security measures.
- Reputation damage: If customers experience service disruptions due to a DDoS attack targeted at another user, this could result in damage to the reputation of the service provider.
- Regulatory and compliance issues: Indirect effects of DDoS attacks might lead to potential breaches of compliance regulations, as they might affect data integrity, availability, and confidentiality.

Thus it is quite important to handle and mitigate collateral damages of the DDoS attack because these damages are more dangerous than the direct effects of the DDoS attack.

4 | DEFENSE MECHANISM FOR DIRECT ATTACK

4.1 | Detection

Detection of attack is required when the attack symptoms are present and verified by the monitoring services. These signs are observed and reported by the monitoring services at the initial stage of the attack or it could already have negatively impacted the target system's performance. This attack detection is performed using the behavior pattern of the traffic.[24] The behavioral pattern of the legitimate users is recorded when attack signs are not present and considered as baseline traffic. Whenever a deviation is observed, the alarm for the existence of an attack is launched. This section is further classified into three subcategories:

- Statistical.
- Machine learning.
- Meta-heuristic approach.

4.1.1 | Statistical

Application layer DoS targets web services by consuming resources through malicious Simple Object Access Protocol (SOAP) requests. It's arduous to identify such attacks on the network or transportation layer. Vissers et al.[25] proposed a system to identify XML and HTTP application layer attacks by extracting several features and constructing a model for typical requests, and detecting malicious requests through outlier detection.

Dou et al.[26] investigate the challenge of DDoS attacks in cloud environments and propose a confidence-based filtering (CBF) methodology for attack detection. The CBF mechanism is employed in two parts; normal scenario and attack period, the legitimate packets collected in the no-attack period to generate a nominal profile for attribute pairs. In the attack period, the CBF scores of each packet are calculated based on the nominal profile to decide whether or not to eliminate it. Extensive simulations show that the proposed method has high speed, fewer storage requirements, and respectable filtering accuracy, enabling it to be a feasible solution for real-time filtering in cloud environments.

Wang et al.[27] set out a "DaMask" approach consisting of a great programmable monitoring technique capable of detecting attacks and responding with a highly manageable control structure. DaMask consists of three layers such as switches, controllers, and applications. It also consists of two modules to detect and mitigate DDoS attacks in the cloud. DaMask-D detects the attack and sends alert and packet information to the DaMask-M module. DaMask-M carries out two tasks, that is, countermeasure selection and log generation.

Girma et al.[28] presents a hybrid model utilizing entropy and covariance matrix to classify DDoS by computing intense data independence. Whereas another author also uses a covariance matrix-based mathematical technique to defend against the DoS flood attack in the cloud. In the initial stage, a nominal traffic profile model is used and acts as baseline traffic. Thereafter, the captured normal traffic is mapped to the matching covariance matrix and helps in detecting the attack.

Dehkordi et al.[30] introduced an entropy-based classification algorithm to detect low and high-level rated DDoS attacks. Here, the classifier will classify the request as normal and attack flow. The proposed approach consists of collector and entropy-based classification sections which will help to detect the DDoS attack.

Bouyeddou et al.[31] presented an innovative approach to detect various forms of DoS and DDoS attacks using the Kullback-Leibler distance (KLD) mechanism. This method involves quantitatively differentiating between two distributions and leveraging the sensitivity of an exponential smoothing scheme. This enables the detector to capture even the slightest of anomalies and incorporate all the information from past and current samples in the decision-making process. By combining these techniques, the proposed KLD-based mechanism can effectively identify variants of DoS and DDoS attacks in a timely and accurate manner. Overall, this approach offers a promising solution to enhance the security of cloud networks against such attacks.

Tsobdjou et al.[32] proposed an online solution to handle flood attacks in a client-server setup. To detect the malicious activity entropy of the source IP is calculated and if it exceeds a threshold limit, it is considered as an attack. To calculate the threshold value Chebyshev's theorem is used. They evaluated their approach using attack simulations and publically available datasets as well. Results indicated that their novel approach achieved commendable accuracy in comparison to other similar techniques.

A summary of existing statistical techniques along with their limitations are mentioned in Table 2.

4.1.2 | Machine learning and deep learning techniques

Sreeram et al.[33] propose an approach aimed to have fast and early detection of application layer HTTP flood attacks. The proposed approach uses a bat algorithm for detection and classification. Here the data for the testing set is first preprocessed using the dataset preprocessing process. In this process, the dataset is prepared with five attributes. Now the complete weight of the testing records is calculated individually. Using the cosine similarity the testing record is classified as attack or benign with the help of defined rules.

Shenfield et al.[34] presents an artificial neural network (ANN) based approach for detecting malicious traffic. ANN is used for deep inspection in intrusion detection systems. The simulation results show that the proposed approach is robust, accurate, and precise. The proposed approach can potentially improve the performance of intrusion detection systems for both conventional and cyber-physical systems network traffic. Das et al.[35] propose an ensemble-based unsupervised machine learning approach as an intrusion detection that is capable of detecting DDoS attacks. The main aim of the proposed approach is to raise the detection accuracy of the DDoS attack with the deterioration in the false positive rate.

TABLE 2 Comparison of statistical approaches.

Author	Technique	Dataset used	Summary	limitation
Vissers et al.[25]	Filtering based on normal profile	Attack generating tool	An attack generating tool is formalized to launch the attack and an adaptive system to detect XML and HTTP attack.	Unable to detect new variants of DDoS with the same feature set.
Dou et al.[26]	Characteristics correlation	MAWI traffic archive	During non-attack period feature pairs are extracted and used to built nominal profile. Incoming traffic is examined with the nominal profile at the time of the attack to identify it.	High processing time.
Wang et al.[27]	Graphic model	UNB ISCX	Using realistic network traffic, DaMask-D identifies the attack, sends information and an alert to the DaMask-M mitigation framework, and reports various attacks.	Less detection accuracy.
Girma et al.[28]	Covariance matrix	Simulated attack traffic	Covariance matrix is used for the detection of flood attack.	False alarm rate due to flash crowds.
Bhuyan et al.[29]	Extended entropy	MIT Lincoln Laboratory tcpdump data, CAIDA, and TUIDS	Using an expanded entropy method, DDoS and IP traceback detection is carried out.	Difficulty in detecting low-rate DDoS when it's in the early stages.
Dehkordi et al.[30]	Entropy-based classification	UNB-ISCX, CTU-13, and ISOT	Entropy-based classification is applied in the detection of the high and low-level rated DDoS attacks.	If the controller is failed, then the detection system will collapse.
Bouyeddou et al.[31]	Exponential smoothing and Kullback–Leibler distance	DARPA99, MAWI, and ICMPv6	Proposed approach use Kullback–Leibler distance to detect different variants of DDoS and Dos	Unable to identify low-level rated DDoS attacks.
Tsobdjou et al.[32]	Information entropy and Chebyshev's theorem	Traffic was generated using simulation setup	Used normalized Shannon entropy in suspicious activity detection module.	Unable to identify low-level rated DDoS attacks.

The proposed approach involves ensembling the various classifiers from the families of outliers and novelty detection to build the framework.

A novel intrusion detection approach for joining Fuzzy C Mean (FCM) clustering and support vector machine (SVM) is proposed by Jaber et al.[36] The proposed system has the ability to improve detection accuracy in cloud infrastructure. The proposed approach consists of three phases. In the first phase cluster groups are formed based on the membership function using FCM. In the second phase, these clusters are used to test and train the genetic programming (GP) and SVM algorithms. At last in the third phase, the performance of FCM using different soft computing methods, such as ANN, GP, and SVM is evaluated.

Zekri et al.[37] presents a C.4.5 algorithm designed to detect and mitigate DDoS attacks. C.4.5 is coupled with a signature detection technique for efficient detection of signatures of the attack to identify flooding. The system is validated by comparing the proposed approach with existing machine-learning approaches.

An ensemble flow-based application layer DDoS attack detection method using a data mining approach is proposed by Prasad et al.[38] Here the new features are used, which represent or show the properties of the traffic flow. This will show the distribution diversity in a traffic flow, which is attached to specific classifiers. To discover the distribution

resemblance Adaboost and ensemble classifiers are used. The experiments are carried out on heavy traffic flow having a clear distribution variety.

Verma et al.[39] proposed an adaptive threshold-based feature selection approach for classifying requests under DDoS in the cloud network. The approach selects the most relevant features using dynamic threshold selection to detect DDoS accurately. The proposed approach is evaluated on the NSL-KDD dataset, and the results show that it can detect DDoS with high accuracy and low false positive rates.

De et al.[40] propose an attack detection method based on fuzzy logic (FL), MLP, and Euclidean distance (ED). The proposed approach is evaluated on real as well as emulated traffic traces. To detect the RoQ attack, MPL achieves the best classification results. However, the proposed approach outperforms MLP at the cost of high execution time.

Early detection is the major concern to fight against DDoS attacks. Cil et al.,[41] proposed a deep neural network (DNN) model to detect DDoS attacks in cloud environments. The authors evaluate the model by using four different types of DDoS attacks and benign traffic. They compare the performance of their proposed DNN model with other state of art techniques and results show that the proposed DNN model outperforms traditional machine learning algorithms in terms of all the performance metrics used.

Aydin et al.[42] propose an LSTM-based solution for DDoS attacks in public cloud network environments. The system consists of two phases: the detection phase and the defense phase. In the detection phase, the LSTM model is used to classify traffic as normal or DDoS traffic. In the defense phase, traffic identified as DDoS is blocked by the defense module. The proposed system is evaluated using real-world DDoS attack data and compared with other state-of-the-art detection methods. The results show that the proposed system achieves higher detection accuracy and lower false-positive rates, making it a promising solution for such systems.

Pateriya et al.[43] used an ensemble XGBoost algorithm to detect Cyber threats in IIoT environments. They used SMOTE technique to handle the unbalanced nature of the UNSW-NB15 dataset. Results show that the proposed approach achieves good accuracy in comparison to another state of art techniques.

A summary of existing ML and DL techniques along with their limitations are mentioned in Table 3.

4.1.3 | Meta-heuristic approach

Gillani et al.[44] proposed a defense mechanism against DDoS attacks by varying the trace of resources in an unforeseeable manner. This will puzzle the attacker's knowledge and plan of attack toward the network resources. In their proposed approach virtual networks (VNs) are hired. These VNs will randomly reallocate resources of the network with the aid of placement of VNs along with persistent migration of the VN towards new resources. The approach has two constituents such as (i) a correct-by-construction migration of VN organization that will remarkably raise the uncertainty about tedious links of various VNs and also maintain the VN placement properties, (ii) an effective migration process of VN that recognizes the suitable sequence of configuration to enable migration of nodes along with maintaining the security of the network.

Jafarian et al.[45] used the open flow to build the architecture that mutates the IP with elevated unpredictability and rate, while keeping the integrity of the configuration and reducing the operational overhead. The proposed technique is known as OpenFlow Random Host Mutation (OFRHM). The OpenFlow controller assigns random IP to each host and it translates the real IP of the host. In this process the original IP is persist untouched, this makes the IP mutation process absolutely crystal clear to end hosts. Through virtual IP addresses given by DNS, named hosts get reachable. However, it can only be reached by authorized entities.

In Reference 46 cuckoo search algorithm-based methods are used to separate attack and benign requests and compared with firefly and bat. The firefly method is based on randomization and best solution selection. These are the two critical steps to have an accurate classification. Similarly, the bat algorithm is based on swarm intelligence. Separate files of attack and benign traffic datasets are given as input. Each record in the benign dataset is considered as one bat and distance is calculated towards the remaining bats. The records are updated and carried to the next iteration. When iterations are completed, then benign and attack classifiers are extracted and marked as benign and attack signatures. For the classification of the incoming request, cosine similarity is used with normal and attack signatures and helps in identifying the type of traffic.

Velliangiri et al.[47] proposed a new classifier called FT-EHO-DBN, which combines the fuzzy logic and deep belief network (DBN) classifiers with the Taylor elephant herd optimization (T-EHO) algorithm to detect DDoS attacks. The fuzzy logic is used to handle uncertainty in the input data, while the DBN is used for feature extraction. The T-EHO

TABLE 3 Comparison of machine learning and deep learning approaches.

Author	Technique	Dataset used	Summary	Limitation
Sreeram et al.[33]	Cosine similarity and bat algorithm	CAIDA	The devised bat algorithm amplified the detection accuracy with minimal process complexity.	Proposed approach is fast. However, fails to achieve good accuracy.
Shenfield et al.[34]	IDS with ANN	-	ANN-based classifier is used for the identification of patterns in the network traffic.	Need long training time and lots of data, especially for architectures with many layers.
Das et al.[35]	Ensemble classifiers	NSL-KDD	Ensemble based unsupervised machine learning approach to classify DDoS attack and benign traffic.	Lot of scopes to improve the accuracy of the system.
Jaber et al.[36]	FCM and SVM	NSL-KDD	A FCM and SVM hybrid approach are used for the detection of DDoS attacks.	Needs multiple parameters to get tuned.
Zekri et al.[37]	C.4.5	Attack is generated using Hpng3	Detecting flooding based DDoS attack detection using C.4.5 algorithm.	Large detection time.
Prasad et al.[38]	Adaboost + classifiers	KDD cup 99	Along with different classifier Adaboost is used. It is also validated that the detection accuracy is dominated over other state-of-art approaches.	High complexity.
Verma et al.[39]	Adaptive threshold and random forest classifier	NSL-KDD	The proposed method selects the dynamic threshold value based on incoming traffic stream for feature selection and random forest classifier for the classification of attack.	Flash crowd and other variants of attack are not considered.
De et al.[40]	Fuzzy logic (FL), MLP and Euclidean distance (ED)	IFTO, and CAIDA	Proposed approach is based on fuzzy logic (FL), MLP and Euclidean distance (ED) to detect the RoQ attack.	High execution time.
Cil et al.[41]	Deep neural network	CICDDoS2019	Deep neural network is used as a deep learning model for detecting the DDoS attack.	Proposed approach needs to be verified on the real attack.
Aydin et al.[42]	LSTM	CICDDoS2019	Used LSTM-based DDoS detection and defense system for public cloud network environments.	Unable to classify DDoS into its variants.
Pateriya et al.[43]	XGBoost	UNSW-NB15	Used XGBoost algorithm to detect Cyber threats in IIoT environment.	There is large scope to improve the accuracy.

optimization algorithm is used to optimize the weights in the classifier. The proposed FT-EHO-DBN classifier is compared with other state-of-the-art DDoS detection algorithms, and the results show that it outperforms in terms of accuracy and detection rate.

Vidal et al.[48] proposed a method for mitigating DDoS attacks involving the use of artificial immune systems. The method operates by constructing networks of distributed sensors, which are tailored to the monitored environment's requirements. These sensors can efficiently identify an attack and react in a manner similar to the biological defense mechanisms present in humans.

Agarwal et al.[49] propose a novel FS-WOA-DNN method for detecting DDoS attacks in cloud environments. The approach involves preprocessing data using min-max normalization, selecting optimal features using the FSWOA method, and using them in a deep neural network to classify data as either benign or an attack. To enhance security, the article also uses homomorphic encryption on normal data before securely storing it in the cloud. The proposed method is evaluated against several state-of-the-art approaches, and the results demonstrate that FS-WOA-DNN achieves superior performance in terms of accuracy and detection rate.

Krishna et al.[50] proposed a novel hybrid approach called ML-F is proposed for DDoS attack detection in CC. ML-F combines two meta-heuristic optimization algorithms, lion optimization algorithm (LOA) and firefly algorithm (FA), to enhance the feature selection process. Recursive feature elimination (RFE) is used to select the optimal features, and the random forest (RF) classifier is employed for the classification task. The ML-F approach outperforms the existing gradient boosting classifier (GBC) method in terms of accuracy, precision, recall, and F1 score. The experimental results demonstrate the effectiveness of the proposed approach in detecting DDoS attacks in CC environments.

Alam et al.[51] presents a security algorithm for detecting DDoS attacks that consists of four phases: database training, data preprocessing, feature selection, and classification. The data samples are first trained and preprocessed before selecting optimal features through kernel principal component analysis (KPCA). A SVM-DEHO classifier is used to identify normal and malicious data. The proposed approach is tested on four databases, and the results show that SVM-DEHO approach outperforms other approaches in terms of detection system performance.

Alohali et al.[52] propose an improved meta-heuristic intrusion detection system that utilizes an individual sample of IDS for every client in a distributed CC platform. The system uses an enhanced Chimp optimization algorithm-based feature selection method followed by an adaptive neuro-fuzzy inference system model to recognize intrusions. Finally, the hybrid Jaya shark smell optimization algorithm is used to optimize membership functions. The proposed technique achieves high detection efficiency with an accuracy of 99.31%, precision of 92.03%, recall of 78.25%, and F-score of 81.80% as validated through extensive simulation analysis.

A summary of existing meta-heuristic techniques along with their limitations is mentioned in Table 4.

4.2 | Mitigation

The mitigation method helps the victim server to continue serving requests even in the presence of an attack. This section discusses the methods which keep the victim alive which are under attack. Until the attack is detected, these methods usually run in parallel to the detection schemes. A summary of existing mitigation techniques along with their limitations is mentioned in Table 5.

- *Scalable cloud defense*[54]: The mitigation of attack is achieved through the migration and scaling of resources. The federated cloud infrastructure is extended to handle the DDoS attack. The design constructs on the capacity of federated IaaS to scale and move virtual execution environment (VEE) inside the organization. The objective of the countermeasure is to hinder the attack adequately to migrate all victim VEE toward machines outside the affected zone, consequently ensuring availability. Results show that the proposed approach confirms that the attack is delayed sufficiently to migrate attacked VEEs.

  Similarly, work present in Reference 64 uses a scaling-based method for selective server access based on client reputation. Another DDoS-aware resource scaling approach is proposed in Reference 57, which scales up the resources if the request is made by the benign user. Whenever the scaling of resources is demanded, then all the requests are analyzed first. If the requests are attack requests, the scaling is not performed. However, if all the request belongs to the benign request group then the resources are scaled up to service such requests.

TABLE 4 Comparison of meta-heuristic approaches.

Author	Technique	Dataset used	Summary	limitation
Gillani et al.[44]	Dynamic VN placement.	PlanetLab.	A correct-by-construction agile VN framework is proposed. It will detect the sophisticated attack by re-arranging the VN to a new secure resource.	Real attack traces and their behavior is not examined.
Jafarian et al.[45]	Random host mutation.	-	A moving target OF-RHM defense approach using software-defined networking is proposed. The main goal is to thwart scanning via random and unpredictable mutation of host IP addresses.	Low detection rate and inability to detect unknown attacks.
Prasad et al.[46]	Cuckoo search.	Attack data is generated using JMETER	Cuckoo search is used classify application DDoS attack on web and the benign traffic.	Still, there is a scope to improve the performance of the proposed approach.
Velliangiri et al.[47]	Fuzzy and Taylor-elephant herd optimization.	KDD cup, database1 and database2.	An fuzzified bio-inspired approach are used for the detection of DDoS attack.	The proposed approach persists in high training and testing time as it is inspired by the deep belief network.
Vidal et al.[48]	Artificial immune network.	KDD'99, CAIDA'07, and CAIDA'08.	Emulation of the behavior of the immune system of the human beings is used for the detection and mitigation of DoS flooding attack.	Unable to detect low and constant rate attacks.
Agarwal et al.[49]	Whale optimization and deep neural network.	CIC-IDS 2017.	Whale optimization is used to select the optimal features and deep neural network is applied to classify the attack and normal data.	Further accuracy, sensitivity, and specificity can be improved.
Krishna et al.[50]	Meta-heuristic lion optimization algorithm and firefly optimization algorithm.	NSL-KDD and NBaIoT.	Used hybrid meta-heuristic technique to identify DDoS attack.	Complexity analysis needs to be determined.
Alam et al.[51]	SVM and elephant herding optimization.	NSL-KDD, UNSW-NB15, ISCX ID, and CIC-IDS2017.	A support vector machine-based discrete elephant herding optimization (SVM-DEHO) classifier is used to identify normal and malicious data.	Proposed approach will be computationally expensive to train and optimize, especially with large datasets.
Alohali et al.[52]	Chimp optimization, adaptive neuro-fuzzy inference system, Jaya shark smell optimization.	Used a hybrid meta-heuristic for an intrusion detection system for cloud platform.	Unable to handle outliers in the system.	

TABLE 5 Summary of approaches for DDoS attack mitigation in cloud.

Author	Technique	Summary	Dataset	Limitations
Zhao et al.[53]	Migration.	During the attack, duplicate the OS and resume it to other VM.	-	Results in migration cost and wastage of resources when there is no attack.
Lataniciki et al.[54]	Scaling and migration.	To mitigate the DDoS attack in different scenarios, the concept of scaling and migration is used.	Testbed.	False alarm may result in EDoS and effects the other VMs as well.
Yu et al.[55]	Resource scaling.	Provided a cloud firewall with dynamic resource allocation to handle anomalies.	-	Results in resource wastage due to false alarm which eventually turns to collateral damages.
Yu et al.[56]	Resource scaling.	Use resource scaling to counter DDoS attack in the cloud.	Simulated the traffic.	Resources are scaled due to false alarm then collateral damages may occur.
Somani et al.[57]	Request aware resource allocation.	During attack resources are scaled up based on request awareness, that is, attack or normal.	Testbed for traffic generation.	Resource scaling due to false alarm may turn to collateral damages.
Wang et al.[58]	Software defined security networking mechanism (SDSNM).	Deployed SDSNM at the edge network and applied strict access policies.	DARPA 2000	Useful only at network boundaries, unable to handle the internal attack.
Lopez et al.[59]	SDN in IDPS.	Used traffic analyzer and SDN in intrusion detection and prevention system for attack mitigation.	Traffic is generated using testbed.	Added an extra cost for installing bro flow traffic analyzer sensors.
Gilad et al.[60]	Resource scaling and migration.	Used CDN on demand for service scaling during the DDoS attack.	Simulation of network.	Migration during an attack may result in the spread of the attack and may also result in subsequent migrations.
Sahay et al.[61]	SDN.	Used advantages of SDN to mitigate DDoS attack. Based on the user's request to ISP for mitigation, the traffic is redirected accordingly.	Simulated network for traffic generation.	Unable to detect the internal attack.
Dahiya et al.[62]	Bayesian game theory.	Using Bayesian game theory employing incentives and pricing rules on the users of a network.	Simulated network for traffic generation.	Unable to handle smart attacks.
Kautish et al.[63]	Greedy feature selection and HCS clustering.	SDMTA apply feature selection and HCS clustering and then train the model for DDoS detection.	KDD-999.	Limited to dataset shift issue.

- *Low-cost cloud firewall*: Yu et al.[55] proposes a framework for cloud firewall to protect cloud data centers as traditional packet level firewall mechanisms are not suitable for cloud platforms in case of complex attacks. An event-level detection chain with dynamic resource allocation is used for anomaly detection at the event level, and a mathematical model is established for the proposed framework. The framework features a linear resource investment function for economical dynamic resource allocation for cloud firewalls. The proposed framework provides a reference for cloud service providers and designers to enhance the security of cloud data centers.
- *Software-defined networking*: Utilizing the SDN for DDoS mitigation is an emerging and reconfigurable network paradigm. SDN is divided into two planes, that is, data and control, and can support network reconfigurability on the fly. There exists many projects which are utilizing SDN-based mitigation for the DDoS attack. Sahay et al.[61] present the solution utilizing the SDN to keep a watch on traffic. To route, the attack traffic, specially designed secure switches are used. Whomsoever is the victim can communicate with the ISP for mitigation of the attack. ISP has knowledge about the incoming traffic, and it uses OpenFlow for traffic labeling. The evaluated malicious traffic is forwarded to the security middle box, here the access strategies are applied to the traffic.

  Similarly, Wang et al.[58] utilize the SDN for the detection and mitigation mechanism. The main concept of this work lies in imposing hard access control policies for incoming traffic, which is very difficult to break. Again in Reference 65 SDN is used for deep packet inspection for attack mitigation.

  Wang and Lopez[58,59] proposed a method based on software-defined networking (SDN) for mitigating and detecting DDoS attacks using an elastic intrusion prevention system. Meanwhile, Conti et al.[66] proposed a lightweight approach for preventing route spoofing and resource exhaustion attacks in SDN networks. Their proposed method involves selective blocking and periodic monitoring as countermeasures for these types of attacks. Both methods aim to enhance the security of SDN networks against various types of attacks while minimizing performance overhead.
- *CDN on-demand*: Authors in Reference 60 present a method which utilizes scaling the services economically. The proposed method is an inexpensive and less reliable cloud server. To support the mechanism, content delivery network (CDN) on-demand is developed.
- *Dynamic resource allocation*: The contribution by Yu et al.[56] considers the most important area in the cloud-specific domain related to DDoS mitigation. The work utilizes the dynamic allocation of resource features to avail the resources to the victim server during the attack. Therefore by utilizing this feature, individual cloud customers can be saved from the attack effects. Results on the real-time data show that the proposed queuing theory is successful in mitigating the attack.
- *Duplication of OS and isolation of application*[53]: To detect the DDoS attack, a monitoring function is added to the virtual machine monitor (VMM). When the resource demand exceeds the tolerable demand, then VMM duplicates the OS and isolates the tagged application. This allows the OS and application to continue working and overcome the effects of a DDoS attack. The defending system can be extended to be utilized to escape from viruses or malware. When the OS and application are affected by viruses and malware, then it is detected by the VMM. Once the VMM confirms it, the isolated environment is invoked.
- *Multilevel attack detection*:Alqahtani et al.[67] advocates the detection of DDoS attacks in the service cloud and proposes an effective and fast algorithm to sort out the arising services for the attack. The solution approach consists of four levels, that is, service, tenant, application, and cloud; at each level based on the local data, the symptoms of a DDoS attack are detected. Further, the results from all the levels are compiled to find the attacking service and the victim machine.
- *Bayesian game theory based mitigation*: Dahiya et al.[62] proposes a game theory-based solution for service providers by incorporating the incentives and pricing rules on the users of a network. It is assumed that legitimate users and the service provider are observing the network for so long and gaining probabilistic information about another user being malicious or not. Therefore, this probabilistic information is used by the provider and legitimate users to change their actions to deal with malicious users present in the network.
- *Mitigation tree architecture*: Kautish et al.[63] proposed scattered denial-of-service mitigation tree architecture (SDMTA) mitigation architecture that integrates network monitoring for efficient DDoS detection mechanisms. With businesses operating globally, network devices like routers, switches, firewalls, VMs, and storage devices must be connected and monitored. Integrated monitoring offers continuous visibility, enabling attack prevention. Network administrators need to measure, manage, and prioritize data traffic. The proposed architecture incorporates batch normalization and provides flexible control for immediate response to attacks. In SDMTA input data undergo preprocessing and feature

selection using the greedy stepwise selection algorithm. Data is then clustered with highly connected subgraphs (HCS), and the proposed DDoS detection and mitigation configuration is trained.

5 | DEFENSE MECHANISM FOR INDIRECT ATTACK

DDoS attacks are more serious in cloud networks than in traditional ones because of characteristics like multitenancy, pay-as-you-go, autoscaling, and migrations that create a unique landscape. In a virtualized environment, a DDoS attack has effects that go beyond the targeted service and frequently affect unintended services within the cloud infrastructure. These unintended consequences are known as "collateral damages" to non-targets.[18]

In addition to service-related consequences, economic and sustainability impacts are substantial in the form of EDoS attacks. It is crucial to understand that there are many stakeholders other than the victim's computer in a multi-tenant public cloud. Key stakeholders include co-hosted VMs, physical server(s), network infrastructure, and cloud service providers.

The effects on these stakeholders encompass performance interference, web service performance degradation, resource contention, indirect EDoS, downtime, and business losses. In such scenarios, it is crucial to deploy advanced mitigation techniques and continuous monitoring to minimize the effects of DDoS attacks in cloud networks, ensuring the protection of both target and non-target stakeholders. The available solutions to handle such collateral damages at different levels are classified into two categories as; (i) resource and service-oriented collateral damages and (ii) economic damages.

5.1 | Resource and service-oriented collateral damages

- *Fraudulent resource consumption*: Idziorek et al.[72] investigated the vulnerability of cloud utility models to various cyber-attacks, particularly DDoS and EDoS attacks. The article highlights the unique challenges these attacks pose in cloud environments, including multitenancy, pay-as-you-go, autoscaling, and migrations. By examining the impact on multiple stakeholders, such as co-hosted VMs, physical servers, network infrastructure, and cloud service providers, the study emphasizes the need for advanced mitigation techniques and continuous monitoring to minimize both direct and collateral damages, ultimately ensuring the security and stability of cloud-based services. The study on similar attack types is presented in the work.[73-75]
- *Internal collateral damages*: Somani et al.[18] explore the cloud environment's far-reaching consequences of DDoS attacks, particularly the impact aimed at non-targeted services and stakeholders. The research highlights the unique challenges of cloud networks, which exacerbate collateral damage caused by DDoS attacks. The study emphasizes the importance of implementing advanced mitigation strategies and continuous monitoring to minimize both direct and indirect consequences. By understanding and addressing the ripple effects of DDoS attacks, cloud providers and users can work together to enhance the security and resilience of cloud-based services.
- *Resource limiting*: Recent DDoS attacks on cloud services have revealed many consequences, with collateral and economic losses included. The work[20] investigates strategies for reducing the impact of DDoS attacks on non-targeted services within cloud environments. It proposes a novel resource containment approach to apply resource limits for the victim, minimizing internal collateral damage. By reframing DDoS elimination as an OS-level resource management problem, the study demonstrates that the devised approach can reduce reporting time of attack and victim service downtime while ensuring the availability of other critical services.
- *Resource re-sizing*: Somani et al.[21] proposes a service resizing technique that dynamically adjusts resource allocation for the victim and other functionalities, minimizing the impact of the attack. By focusing on efficient resource management and adaptive measures, the study depicts that the devised approach could effectively reduce the time needed to mitigate DDoS attacks, maintain the availability of critical functionalities, and improve the overall resilience of cloud-based systems.
- *Scale inside out*: Somani et al.[22] proposes an approach that focuses on efficiently managing resources and promptly scaling services to counteract the effects of DDoS attacks. Their proposed approach minimizes the "Resource Utilization Factor" during attacks to expedite absorption. By reallocating resources from victim services to mitigation and

co-located services, this method substantially reduces attack downtime, improves detection and reporting times, and lessens the impact on co-located services.

- *CS-IDR*: Verma et al.[19] proposes a novel approach to tackle the collateral damages occurring at VM level. During DDoS attack not only does the victim VM gets affected but the other VM co-hosted with victim VM on the same host will also get affected. While performing load balancing attack requests will get transferred to VM which is co-hosting. Therefore, to save the co-hosted VM from such collateral damage, a request-aware approach using cuckoo search-based identification of requests using bi-variate flight is used. Here, before performing load balancing, the CS-IDR module was used in identifying the malicious/attack requests and remove these from the request group. This will prevent the transfer of attack requests from one VM to another and also reduces VM-level collateral damages.
- *AVDR*: Since DDoS attacks in CC have increased recently, non-target stakeholders like VMs, host computers, users, and cloud providers have suffered collateral harm. These damages are a result of cloud capabilities including resource sharing, virtualization, auto-scaling, and migrations. In case of DDoS attacks, the large number of requests causes host overload, which existing migration policies struggle to handle efficiently when attacked VMs are present. Verma et al.[68] proposed the attacked VM detection and recovery (AVDR) framework which enhances existing migration policies performance and reduces collateral damages. AVDR is based on attack strength "Y_{as}," for which a linear model is developed using a dataset generated on AWS VM instances, including both attack and benign request traces. The outcomes show how well the suggested methodology works to reduce the effects of DDoS attacks in cloud systems.
- *Service isolation*: In cloud-hosted services, VMs often run co-located services sharing resources with the same OS. When a DDoS attack targets one functionality, it could impact co-located services also, causing "internal collateral damages." This study aims to mitigate these damages in a cloud environment by addressing the problem as an OS-level resource governance and isolation issue. Existing methods in the literature are not sufficiently effective at handling internal collateral damages. In order to provide resource governance and separation between co-located services and improve service performance for good users, the author[69] thus proposes a novel service containerization technique. The outcomes show that by improving service performance, the suggested technique can lessen the side effects of DDoS attacks on co-located services like SSH and disc I/O.
- *Container separation*: Kumar et al.[70] proposed an approach that aims to mitigate DDoS attacks by separating incoming requests at the container level and applying scale-inside-out for attack requests within a separate container. The approach prioritizes serving benign requests without interruption while minimizing the resources used to handle requests from attackers. Results indicate a decrease in response time for normal requests across various page types and a positive enhancement in the number of failures to normal requests, suggesting the devised approach is efficient in mitigating DDoS attacks.
- *Resource isolation*: Kumar et al.[71] proposes resource isolation with the help of service separation at two levels: physical machine level and VM level, to mitigate the performance interference caused by DDoS attacks. The study compares four methods of resource segregation for authorized and valid users at different levels, including container level and page level. Experimental results demonstrate that adopting different separation levels improves response time for valid and authorized user requests even under DDoS attacks, and increases the service availability time of target machines. The frequency of request failures and response times for target and co-located services have also significantly improved.

A summary of an existing resource and service-oriented solutions for collateral damages along with the level for which the solution is provided and limitations are mentioned in Table 6.

5.2 | Economical damages

- *EDoS-shield*: EDoS attacks target the economic resources of cloud users, who are billed on a pay-as-you-use basis, making the cloud system economically unsustainable. Haidari et al.[85] investigate the efficiency of the EDoS-Shield approach in combating EDoS attacks in CC environments. EDoS-Shield is a significant technique for mitigating such attacks by detecting and dropping malicious requests before they reach cloud service nodes. It employs queuing theory modeling to study the performance of EDoS-Shield under various scenarios, analyzing and comparing key performance metrics such as response time, CPU utilization of allocated cloud resources, and system throughput.

TABLE 6 Summary of solution approaches for resource and service targeted based DDoS collateral damages in cloud.

Author	Technique	Summary	Sol. level	Limitations
Somani et al.[57]	Resource scaling.	During the attack, request-aware resource scaling is performed to mitigate the attack.	Level 0	False alarms may engage the resources for serving the attack requests.
Somani et al.[18]	-	Work demonstrates that DDoS attacks create collateral damage.	Level 0-4	Solution for collateral damages is not provided.
Somani et al.[20]	Fixing resources.	The remaining resources become the upper limit for victim assistance when the minimum necessary resources for other services are frozen.	Level 0	Limits the performance of other services.
Somani et al.[21]	Resource management.	During the attack, allocated minimum resources required to the victim service, and the rest of the resources are allotted to mitigation service.	Level 0	Limits the performance of benign/normal users of the victim service.
Somani et al.[22]	Reduce resource utilization factor.	During an attack resource utilization factor of victim service/facility gets minimized to expedite the reduction process.	Level 0	Reducing the utilization factor affects the benign user service performance.
Verma et al.[68]	Recovery of attacked VM before migration.	During DDoS attack before performing VM migration attacked VMs are removed based on the modeled equation $'Y'_{as}$ and then then the migration of VMs are performed if required.	Level 2	Robustness of the proposed approach needs to be verified on other network conditions and different datasets.
Verma et al.[19]	Identifying attack request using Cuckoo search.	For each incoming request load balancer will take the decision based on the available loads carried by the VM. However, before allocating requests to the selected VM, the CS-IDR module is used to identify and remove the attack requests.	Level 1	Unable to handle the low rate DDoS which behaves like legitimate requests and eventually results in a miss rate.
Verma et al.[69]	Service isolation.	All of the VM's services are containerized once the DDoS attack has been identified and its collateral effects have been quantified in order to isolate the services and reduce internal collateral damage.	Level 0	Utilizing containers may result in slow processing speed in comparison to bare metal.
Kumar et al.[70]	container separation.	Applying scale-inside-out for attack requests into a different container and splitting incoming requests at the container-level.	Level 0	Does not provide a comprehensive evaluation of the devised approach under different scenarios of attack.
Kumar et al.[71]	Resource isolation.	Used resource isolation through service separation to mitigate the performance interference caused by DDoS attacks.	Level 3	Scalability of the proposed approach in larger cloud environments.

- *EDoS armor*: Masood et al.[77] presents a dual approach to address EDoS attacks; (i) admission control and (ii) congestion control. Admission control limits the concurrent requests from clients, maintaining the web server's efficiency within its resource capacity. Congestion control alters client priority based on accessed resources and performed activities, optimizing resource allocation for legitimate clients. By integrating this solution into a Web Application Firewall, the researchers observed a significant improvement in resource distribution between good and bad clients.
- *In-cloud scrubber*: In the cloud, DDoS attacks can create economic Distributed Denial of Service (eDDoS) situations in which the cloud's elasticity causes service scaling to exceed the provider's ability of payment for cloud-based service bills, leading EDoS attacks. To keep CC appealing, DDoS threats must be addressed before activating billing mechanisms. This challenge can be tackled using a reactive/on-demand in-cloud eDDoS mitigation service (scrubber service), which mitigates DDoS attacks from the application layer to the network layer through an efficient client-puzzle approach.[78]
- *Controlled accessed resources*: Biag et al.[79] resents an innovative reactive rate-limiting technique with minimal overhead to address EDoS attacks targeting cloud-based services. This method grants limited access permissions to resources for each user. The results demonstrate that the suggested technique effectively detects EDoS attacks while maintaining low overhead and cost.
- *FLNL EDoS mitigation*: Author in Reference 80 proposed a fuzzy entropy and lion neural learner (FLNL) approach for the classification and mitigation of EDoS attacks in a cloud environment. The methodology comprises two crucial steps: feature selection and classification. The feature selection is performed using fuzzy entropy, ensuring no information loss, while the lion neural learner performs the classification task.
- *Profile-based EDoS detection*: Dennis et al.[81] proposed profile-based framework is used for the detection of EDoS attacks. It consists of a feature classification algorithm that highly improves the performance parameters. The limited resources are allowed to be allocated to the VMs, which reduces the misuse of resources.
- *A semi-Markov approach*: Lalropuia et al.[2] developed a state-based model using a semi-Markov process for the availability of resources in the cloud under EDoS attack. Using this, the availability of steady states of the cloud is determined. Moreover, the mean failure time of the cloud is determined under the existence of an EDoS attack. This will describe the time frame during which there will be an unsustainable condition on the cloud. In addition, a cost management strategy using a cloud shutdown feature is utilized to prevent cloud adopters from unnecessary high billings.
- *Stochastic recurrent neural network*: Dinh et al.[82] devised an enhanced scheme for the identification and mitigation of EDoS attacks. The proposed approach implements a gated recurrent unit which helps in reducing the vanishing gradient problem and can also capture complex temporal dependence relations. To reduce the error rate, a self-adjusting threshold is also introduced, whereas the present solutions generally utilize a fixed threshold to analyze the anomalies, which somehow results in increased error rates.
- *EDOS-TSM*: Shah et al.[83] introduces EDoS-TCP SYN mitigation model (EDOS-TSM), an SDN-based statistical anomaly detection methodology for quick and effective TCP SYN flooding attack mitigation. To identify source-based and spoofing-based attacks, EDOS-TSM employs binomial probability, TTL field values from IP packet headers, and multiple TCP SYN requests. The model exhibits enhanced performance compared to existing techniques, with fewer false negatives and increased effectiveness in combating both source-based and spoofing attacks, when implemented on an OpenStack production-based cloud.
- *ADS-PAYG*: Karthika et al.[84] presents a new technique called ADS-PAYG (Attack Defense Shell-Pay As You Go) using the trust factor method to combat EDoS attacks in CC. The ADS-PAYG system comprises three significant stages: cloud service data, load balance, and DDoS shield, aiming to tighten cloud service security. The ADS-PAYG sets a threshold value to increase the number of authenticated users. Implemented in MATLAB, this method outperforms other trust factor estimation techniques, achieving 83.43% detection accuracy.

A summary of existing solution approaches for the economical aspect targeted collateral damages in the cloud along with the level to which the solution is provided and limitations are mentioned in Table 7.

TABLE 7 Summary of solution approaches for economical aspect targeted collateral damages in cloud.

Author	Technique	Summary	Sol. level	Limitations
Haidari et al.[76]	Queuing theory, virtual firewall and authentication.	An analytical model on queuing theory is made to analyze the performance of EDoS shield. Here EDoS shield detects the attack traffic using the virtual firewall and cloud-verifiable node.	Level 3	Results in extra cost as an overhead for the system.
Masood et al.[77]	Limiting incoming requests and prioritizing clients.	Limiting the simultaneous requests towards the web server and prioritizing the clients based on their previous activities.	Level 3	Limiting the number of clients will sometime affect the service of legitimate users.
Kumar et al.[78]	Puzzle generation and verification.	With the use of an effective client-puzzle strategy, a reactive/on-demand in-cloud DDoS mitigation service is employed to mitigate the application-layer and network-layer DDoS attacks.	Level 3	Generating the puzzles will create an overhead on the server.
Baig et al.[79]	Controlled resource access.	A threshold parameter restricts incoming requests if they exceed the defined threshold. The threshold depends on the triggering conditions for auto-scaling.	Level 1	Does not only auto-scaling even if triggered due to legitimate requests.
Bhingarkar et al.[80]	Fuzzy entropy and lion neural learner.	EDoS attack is detected using the FLNL approach in which fuzzy entropy is used for the feature selection and lion neural learner is used for the classification purpose.	Level 3	Performance parameters can be improved.
Dennis et al.[81]	Profile-based detection.	Profile-based framework in which feature classification algorithm is used for EDoS attack detection.	Level 3	If the database and HTTP attack occur simultaneously then it results in degradation in attack accuracy.
Lalropuia et al.[2]	A semi-Markov approach.	Using semi-Markov process, a state-based model is developed to save the cloud from EDoS attack.	Level 3	If limited resources are used to launch the attack then the proposed approach fails to detect such attacks.
Dinh et al.[82]	Stochastic recurrent neural network.	A self-adjusting threshold with a gated recurrent unit is used to tackle EDoS attack.	Level 3	There is a lot of scope to improve the performance parameters.
Shah et al.[83]	Binomial distribution.	EDOS-TSM uses binomial probability, TTL field values of IP packet headers, and multiple TCP SYN requests.	Level 3	Limited to specific EDoS attacks.
Karthika et al.[84]	Trust factor method.	By setting a threshold value, it is suggested to increase the number of authenticated users in the approach using the trust factor method against the EDoS attack.	Level 3	Unclear how well the proposed approach would perform in a real-world scenario as it is tested on a simulated dataset.

6 | AVAILABLE DDOS DATASET AND TOOLS

6.1 | Dataset

DDoS datasets are valuable resources for researchers, cybersecurity professionals, and organizations working in the domain of networks and network security. Primary uses of these datasets include: (i) By analyzing the traffic patterns and characteristics of DDoS attacks in these datasets, researchers can gain insights into the techniques used by attackers and the vulnerabilities exploited. (ii) To train machine learning models or create rule-based algorithms for real-time DDoS attack detection, DDoS datasets are employed. Organizations can more efficiently identify and mitigate DDoS using these models. (iii) Datasets with DDoS attacks enable researchers and security professionals to evaluate the performance of various DDoS mitigation techniques and tools. This helps in determining the effectiveness of different approaches in preventing or minimizing the impact of DDoS attacks. (iv) DDoS datasets are used as comparison tests to evaluate the precision and effectiveness of intrusion detection systems. By comparing the performance of various unique systems on one kind of dataset, researchers can identify the strengths and weaknesses of various approaches. (v) DDoS datasets can be used in educational settings to help students learn about DDoS attack patterns, detection techniques, and mitigation strategies. By working with real-world data, students can gain practical experience and develop their skills.[86-96] Some of these publically available datasets are:

- *CAIDA DDoS attack dataset*: The Center for Applied Internet Data Analysis (CAIDA)* provides anonymized DDoS attack data, comprising network traces of various DDoS attack types, like TCP SYN floods and ICMP floods. This dataset aids researchers in studying and understanding DDoS attack patterns and developing detection and mitigation techniques.
- *DARPA intrusion detection evaluation dataset*: Created by MIT Lincoln laboratory under the DARPA† intrusion detection evaluation program, containing labeled network traffic data, including DDoS attacks. It serves as a benchmark for evaluating intrusion detection systems and helps researchers develop DDoS detection techniques.
- *ISCX intrusion detection evaluation dataset*: The Information Security Centre of Excellence (ISCX)‡ dataset includes network traces with various types of attacks, such as DDoS, for intrusion detection research. It helps researchers develop and evaluate DDoS detection algorithms and improve cybersecurity solutions.
- *CTU-13 dataset*[97]: Created by the Czech Technical University in Prague, this dataset contains labeled network traffic data with 13 different scenarios, including DDoS attacks. It enables researchers to study DDoS attack patterns, develop detection techniques, and evaluate the performance of these techniques.
- *CIC-DDoS2019 dataset*[98]: The Canadian Institute for Cybersecurity (CIC) released this dataset containing DDoS attack traffic and benign traffic to facilitate DDoS detection research. It helps researchers develop, train, and evaluate machine learning models for detecting DDoS attacks in network traffic.
- *TUIDS DDoS dataset*:[99] This dataset, developed by the Thammasat University Intrusion Detection System (TUIDS), consists of benign traffic and DDoS attack traffic, including HTTP flood and SYN flood attacks. It is suitable for training and evaluating DDoS detection models.
- *CIC-IDS2017 dataset*:[100]: Another dataset by the Canadian Institute for Cybersecurity (CIC), CIC-IDS2017 includes various cyber attacks, including DDoS, as well as benign traffic. It is designed for evaluating intrusion detection systems and developing DDoS detection techniques.
- *MAWI Working Group Traffic Archive*:[101]: The MAWI (Measurement and Analysis of the WIDE Internet) working group traffic archive contains network traffic traces collected from the WIDE backbone. It includes various types of network attacks, including DDoS, and is useful for studying network traffic patterns and developing attack detection techniques.
- *The UNSW-NB15 dataset*: Developed by the University of New South Wales,§ containing labeled network traffic data, including a variety of cyber attacks such as DDoS. It evaluates intrusion detection systems and trains machine learning models for attack detection.

While DDoS datasets are valuable for research purposes, they come with several limitations that can affect the quality and applicability of the research conducted. Some of these limitations include:

- Outdated data: DDoS datasets may contain data that is no longer representative of current DDoS attack trends, techniques, or strategies. As attackers constantly evolve their methods, outdated datasets may not capture the latest threats or attack patterns.
- Limited attack types: some datasets may focus only on specific DDoS attacks or target systems, limiting the researcher's ability to generalize findings to other attack types or systems.
- Data quality: datasets may have incomplete, inconsistent, or inaccurate data, which can impact the accuracy of the models or algorithms developed. Data collection methods and preprocessing techniques can also affect data quality.
- Data privacy and anonymization: to protect privacy and maintain legal compliance, datasets often require anonymization, which can remove or obscure important information about the attacks or the network infrastructure. This can make it challenging to conduct an in-depth analysis or understand the full context of the attack.
- Lack of ground truth: in some cases, datasets may not have clear labels or ground truth information about the traffic's nature, enhancing the difficulty for researchers to distinguish between benign and malicious traffic or accurately evaluate their detection models.
- Ethical concerns: collecting and sharing DDoS datasets can raise ethical concerns about user privacy, data handling, and potential data misuse by malicious actors.
- Limited availability and accessibility: high-quality DDoS datasets are not always readily available or accessible, as organizations may be reluctant to share sensitive data about their networks or security incidents. Additionally, datasets may be restricted to specific research groups, and institutions, or require special permissions to access, limiting the broader research community's ability to work with the data.
- Imbalanced data: DDoS datasets may be imbalanced, with a disproportionately large amount of benign traffic compared to malicious traffic. This imbalance can lead to biased models that perform poorly in real-world scenarios where the attack traffic might be more prevalent.
- Scalability issues: datasets may not always be large enough to test the scalability of detection and mitigation techniques effectively. Smaller datasets may not adequately represent the complexity and scale of real-world DDoS attacks, limiting the applicability of research findings.
- Lack of diversity: datasets may not cover a diverse range of network environments, attack types, or targets, which can limit the generalization of research findings. Researchers may need to work with multiple datasets or collect their data to account for this limitation.

6.2 | Attack tools

DDoS attack tools are software programs designed to generate a massive amount of traffic or requests to overwhelm and incapacitate targeted systems or websites. These tools vary in terms of the attack types they employ, such as TCP, UDP, ICMP, or HTTP floods, and their level of sophistication in evading security measures. Some tools also allow for anonymized attacks, using networks like Tor to conceal the attacker's identity. As DDoS attacks continue to evolve, so do the tools used to launch them. Some of these tools are:

- *LOIC (Low Orbit Ion Cannon)*: LOIC is an open-source network stress testing and DDoS attack application. It allows users to generate massive network traffic by flooding a target server with TCP, UDP, or HTTP requests. LOIC has been widely used by hacktivist groups like anonymous for launching DDoS attacks.
- *Slowloris*: Slowloris is a DDoS attack tool that targets web servers by establishing and maintaining many slow HTTP connections, eventually exhausting the server's resources. It operates by sending partial HTTP requests and keeping the connections open for as much as possible, thus increasing the difficulty for the server to handle legitimate traffic.
- *HOIC (High Orbit Ion Cannon)*: HOIC is an upgrade to LOIC, designed to generate more significant traffic volumes and evade basic network defenses. It uses a booster script functionality to enable multiple users to attack a target simultaneously, increasing the effectiveness of the DDoS attack.
- *hping*: hping is a command-line-oriented TCP/IP packet assembler/analyzer that could be used for various purposes, including DDoS attacks. It supports multiple protocols and can generate custom packets, enabling users to create tailored attacks targeting specific vulnerabilities.

- *XOIC*: XOIC is a simple DDoS attack tool that allows users to launch attacks using three methods: test mode, HTTP mode, and TCP/UDP mode. It features an easy-to-use interface and is suitable for beginners looking to experiment with DDoS attacks.
- *RUDY (R-U-Dead-Yet)*: is a DDoS attack tool designed for exploiting the weakness in web applications that use POST data submissions. Instead of flooding the target with massive traffic, RUDY uses a low-and-slow approach by sending partial HTTP POST requests on the target server. It builds and maintains many simultaneous connections, slowly transmitting data packets to consume server resources.
- *Tor's Hammer*: Tor's Hammer is a slow-rate DDoS attack tool that uses the Tor network to anonymize its traffic. It begins by initiating various connections to the target server and slowly sending traffic, making it difficult for the server to handle the connections. Its use of the Tor network provides an additional layer of anonymity for the attacker.
- *PyLoris*: PyLoris is a DDoS attack tool that focuses on testing and exploiting vulnerabilities in server software that rely on thread-based architectures. It sends specially crafted requests to the target server, enforcing the server for allocating resources for handling requests, eventually exhausting its resources and becoming unresponsive.
- *GoldenEye*: GoldenEye is a Python-based DDoS tool that targets web applications by launching a combination of application-layer (HTTP) and transport-layer (TCP and UDP) attacks. It generates randomized requests, headers, and user agents to bypass basic security measures and overwhelm the target server.

7 | ISSUES AND CHALLENGES

7.1 | General issues and challenges

Detecting DDoS attacks presents a unique set of issues and difficulties compared to traditional network environments in cloud environments.

- Dynamic nature of the cloud: cloud environments are characterized by elasticity, auto-scaling, and virtualization, which make it difficult to establish static baselines for detecting anomalies or malicious traffic patterns.
- Shared resources: in cloud environments, multiple tenants share resources, making it challenging to isolate the effects of DDoS attacks on the specific tenants or differentiate between legitimate spikes in traffic and malicious traffic.
- Encrypted traffic: the increasing use of encryption (e.g., HTTPS) makes it difficult for traditional deep packet inspection techniques in analyzing the contents related to network traffic, potentially allowing DDoS traffic to go undetected.
- Multi-layer attacks: DDoS attacks can target different layers from the network stack, ranging from the network layer to the application layer. Detecting and mitigating these diverse attack types require sophisticated, multi-layer detection techniques.
- Large-scale attacks: cloud environments can be targeted by large-scale, high-volume DDoS attacks that can quickly consume available resources, thus increasing the challenge of detection and mitigation of such attacks before significant damage occurs.
- Distributed nature of attacks: DDoS attacks often involve a huge number of geographically distributed sources, thus increasing difficulty to detect and trace the attack traffic back to its origin.
- Evolving attack techniques: attackers are continually developing new DDoS attack techniques, such as reflection and amplification attacks, low-and-slow attacks, or IoT-based botnets. Staying ahead of these evolving techniques and developing effective countermeasures is a constant challenge.
- False positives and false negatives: accurate detection of DDoS attacks is crucial to avoid false positives, which can lead to blocking legitimate traffic, and false negatives, which can result in undetected attacks. Striking the right balance between sensitivity and specificity in detection methods is a significant challenge.
- Real-time detection and mitigation: DDoS attacks can cause damage quickly, making it essential to detect and mitigate them in real-time. Developing efficient and fast detection algorithms that can handle large volumes of traffic without introducing significant latency is a challenge.

- Data privacy and legal concerns: monitoring traffic in cloud environments for DDoS detection can raise data privacy concerns, as well as legal and compliance issues, particularly when dealing with multi-tenant environments and cross-border data flows.

7.2 | Collateral damage specific issues and challenges

Collateral damages, or the unintended negative consequences of a DDoS attack on non-targeted systems or stakeholders, can be particularly challenging in cloud environments. The shared characteristic of cloud resources and the interconnectedness among services can lead to broader impacts. Some key issues and challenges related to collateral damages in DDoS detection in cloud environments include:

- Resource contention: DDoS attacks can cause resource contention in cloud environments, affecting co-hosted VMs or even other host machines when resources are redirected to handle the attack. This can lead to reduced performance or availability of services for non-targeted users.
- Auto-scaling issues: in cloud environments with auto-scaling features, a DDoS attack may trigger the automatic allocation of additional resources to the targeted service. This can lead to increased costs for the victim and potentially reduce available resources for other tenants.
- Load balancing complications: load balancing mechanisms can distribute the attack traffic among multiple VMs or hosts, causing collateral damages to non-targeted services. This can make it more difficult to isolate the attack and protect unaffected systems.
- Migration effects: in response to a DDoS attack, cloud providers may migrate VMs to other hosts or data centers, impacting non-targeted VMs and services that are moved as a result.
- Network congestion: DDoS attacks can cause network congestion in cloud environments, affecting not only the targeted service but also other services sharing the same network infrastructure.
- Reputational harm: cloud provider's reputations could be harmed due to collateral damages from a DDoS attack. This may result in a loss of customer trust and potential business for both the targeted and non-targeted service providers.
- Difficulty in attack attribution: the presence of collateral damages can make it challenging to determine the sole target of attack and to attribute the attack to a specific source or actor. This can complicate the response and mitigation efforts.
- Increased complexity of detection and mitigation: collateral damages introduce additional complexity to the DDoS detection and mitigation process, as it becomes necessary to protect not only the targeted service but also the non-targeted services that may be affected.
- Legal and compliance implications: collateral damages may result in violations of service level agreements (SLAs) or regulatory requirements, leading to potential legal and financial consequences for cloud providers and their customers.
- Economic impact: the broader economic impact of collateral damages in cloud environments can be significant, affecting not only the targeted business but also other stakeholders in the cloud ecosystem, such as service providers, customers, and partners.

8 | SOLUTION CONSIDERATION

When providing solutions for direct DDoS defense mechanisms and minimizing collateral damages, it's important to consider several factors:

- Scalability: the defense mechanism should be able to scale and adapt to the increasing size and complexity of DDoS attacks. Solutions should also be flexible enough to accommodate future growth in network traffic and infrastructure.
- Cost-effectiveness: implementing DDoS defense mechanisms can be expensive, so it's crucial to find a balance between the level of protection and the associated costs. This might involve prioritizing critical systems and determining an acceptable level of risk.

- Integration: ensure that the DDoS defense solution could be seamlessly integrated with already available security infrastructure, like firewalls, intrusion detection systems, and log management tools.
- Real-time monitoring and analysis: effective defense mechanisms should have real-time monitoring and analysis capabilities to detect and respond to DDoS attacks quickly. This helps minimize downtime and potential collateral damages.
- Automation: automated responses can help reduce the time it takes to mitigate an attack and minimize human intervention, which can lead to quicker resolution and reduced impact on services.
- Incident response plan: build a hardcore response plan that defines the steps that are to be taken in case of DDoS attacks. This should include communication protocols, roles, and responsibilities, and procedures for escalation and recovery.
- Collaboration and information sharing: collaborate with other organizations and share information about DDoS attack trends and defense strategies. This can help improve overall preparedness and response capabilities across the industry.
- Training and awareness: ensure that staff members are well-trained and aware of the potential risks and impacts of DDoS attacks. This can help them recognize and respond to incidents more effectively.
- Redundancy and failover: implement redundant systems and failover mechanisms to minimize the impact imparted by DDoS attacks on critical services. It can help ensure the continued availability of essential services during an attack.
- Legal and regulatory compliance: make sure that your DDoS defense mechanisms and strategies comply with any relevant legal and regulatory requirements, such as data protection laws and industry-specific regulations.

9 | EFFECTIVE SOLUTION SCENARIO

To address collateral damages caused by DDoS attacks in cloud environments, defense solutions should be implemented at various levels. Here are some strategies to nullify the effects of DDoS attacks and minimize collateral damages:

9.1 | Level 0—Victim VM

- Anomaly detection: implement machine learning and statistical techniques to detect unusual traffic patterns or resource usage within the VM.
- Rate limiting: apply rate limit to prevent a single service from consuming excessive resources and affecting other services within the VM.
- Intrusion prevention systems (IPS): deploy an IPS to monitor and block malicious traffic targeting specific services within the VM.

9.2 | Level 1—Co-hosted VMs

- Resource isolation: enforce strict resource isolation policies between co-hosted VMs to prevent resource contention.
- Intelligent load balancing: implement smart load balancing algorithms that can differentiate between legitimate and harmful traffic, thus preventing the spreading of attacks to co-hosted VMs.
- VM migration: migrate unaffected VMs to other hosts or data centers to minimize the impact of the attack on co-hosted VMs.

9.3 | Level 2—Host physical machines and associated VMs

- Network segmentation: segment the network to contain the attack within a specific segment and prevent it from spreading to other hosts and their associated VMs.

- Traffic filtering: employ traffic filtering techniques at the host level to block malicious traffic before it reaches the targeted VMs.
- Distributed defense mechanisms: implement distributed defense mechanisms across multiple hosts to detect and mitigate attacks collaboratively.

9.4 | Level 3—Cloud infrastructure

- Global threat intelligence sharing: collaborate with other cloud providers and security organizations to share threat intelligence, enabling the early identification of emerging DDoS threats.
- Infrastructure redundancy: build redundancy into the cloud infrastructure to minimize the impact of DDoS attacks on overall system availability and performance.
- Multi-layered security: deploy a multi-layered security approach, including network, transport, and application layer defenses, to protect against various DDoS attack types.

By implementing these defense solutions at different levels for collateral damages, cloud providers can minimize the impact of DDoS attacks on non-targeted systems and stakeholders while maintaining the performance and availability of their services.

10 | FUTURE DIRECTION

Addressing the challenges and issues surrounding both direct and indirect effects of DDoS attacks in the cloud is crucial for the security and reliability of cloud services. Here are some key directions for future research:

- Advanced DDoS detection mechanisms: develop advanced algorithms and AI models that can detect DDoS attacks in real-time, identifying not only direct attacks but also subtler, indirect ones.
- Comprehensive impact analysis: investigate the full spectrum of direct and indirect effects of DDoS attacks, looking at factors such as service downtime, resource consumption, and collateral damage to non-targeted services and users.
- Quantum computing: explore the potential of quantum computing in enhancing DDoS attack detection and mitigation strategies, considering both direct and indirect effects.
- Enhanced network security protocols: improve network security protocols in cloud environments to limit the direct and indirect impact of DDoS attacks.
- Adaptive defense strategies: research into adaptive defense strategies that can dynamically respond to evolving DDoS attacks, mitigating both direct and indirect effects.
- Interdisciplinary approach: incorporate insights from behavioral science, economics, and other fields to understand the motivations behind DDoS attacks and devise strategies to deter them.
- Improved isolation techniques: develop better techniques to isolate the affected resources and contain the impact of a DDoS attack, limiting both direct and collateral damage.
- Distributed and decentralized cloud services: explore the feasibility of distributed and decentralized cloud models as potential solutions to mitigate the effects of DDoS attacks.
- Legal and regulatory implications: study the legal and regulatory implications of DDoS attacks in a cloud environment, and how these can be designed to minimize both direct and indirect impacts.
- Resilience and recovery mechanisms: research robust recovery mechanisms that can ensure the swift restoration of services following a DDoS attack, reducing the direct impact on users and limiting indirect effects.
- Multi-cloud and hybrid cloud strategies: analyze the specific challenges and advantages of multi-cloud and hybrid cloud environments when facing DDoS attacks. Develop mitigation strategies tailored to these setups.

Through focusing on these research directions, researchers can strive towards more secure and reliable cloud environments, resilient to both the direct and indirect effects of DDoS attacks.

11 | CONCLUSION

This article begins with a discussion of various security issues in cloud networks followed by the background, history, attack statistics, and motivation of the work. The availability of cloud services and resources is of major concern in CC. The cyber threat that affects the availability of the cloud is the DDoS attack and will restrict the adoption of the cloud in many advanced technologies such as human-centric intelligent systems as well. Further, the article discusses launching the DDoS attack, that is, finding the vulnerable machine and propagating the malicious code to launch the attack. In this survey, direct and indirect (collateral) effects of the DDoS attack in the CC environment are considered. A new taxonomy based on the direct and indirect effects of the attack and the associated solutions is also discussed. Various detection and mitigation approach for handling the direct target DDoS attack are discussed. However, the solutions for indirect attacks are described based on the service and resources-oriented collateral damages and economic damages. The defense approaches and their behavior in the cloud are also compared. The next section of the article discusses the performance parameters for the evaluation purpose and the available datasets and tools for DDoS attacks in the cloud. To the best of our knowledge, collateral damages and their solution are not well addressed in the literature. Therefore the major novelty of this work lies in providing the discussion against the collateral damages of DDoS attacks in the cloud, and the categorization of the defense approaches used in the literature till now. This article provides insight into the collateral damages and helps the researchers to formulate the defense approaches against such attacks in the cloud environment.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ENDNOTES

*https://www.caida.org/data/passive/ddos-20070804dataset.xml.
†https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset.
‡https://www.unb.ca/cic/datasets/ids.html.
§https://research.unsw.edu.au/projects/unsw-nb15-dataset.

ORCID


Ankit Vidyarthi https://orcid.org/0000-0002-8026-4246

REFERENCES

1. Brown E. NIST issues cloud computing guidelines for managing security and privacy (Report No. 800-144). National Institute of Standards and Technology Special Publication; 2012.
2. Lalropuia K, Khaitan V. Availability and reliability analysis of cloud computing under economic denial of sustainability (EDoS) attack: a semi-Markov approach. *Cluster Comput*. 2021;24:2177-2191.
3. Anstee D, Bussiere D, Sockrider G, Morales C. *Worldwide Infrastructure Security Report*. Arbor Networks Inc.; 2017.
4. Anstee D, Bussiere D, Sockrider G, Morales C. Arbor's 13th annual worldwide infrastructure security report. Technical Report. Arbor Networks Inc; 2018:9.
5. Netscout. Netscout Arbor's 14th annual worldwide infrastructure security report; 2019. https://www.netscout.com/report
6. Akamai Security Research; 2018. http://www.akamai.com/stateoftheinternet-security
7. Threat landscape report—Q1, AWS Shield Inc; 2020.
8. ArborNetworks, Inc. Worldwide infrastructure security report volume IX; 2014. http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
9. Gupta B, Badve OP. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. *Neural Comput Appl*. 2017;28(12):3655-3682.
10. Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. DDoS attacks in cloud computing: issues, taxonomy, and future directions. *Comput Commun*. 2017;107:30-48.
11. Shameli-Sendi A, Pourzandi M, Fekih-Ahmed M, Cheriet M. Taxonomy of distributed denial of service mitigation approaches for cloud computing. *J Netw Comput Appl*. 2015;58:165-179.
12. Somani G, Gaur MS, Sanghi D, Conti M, Rajarajan M, Buyya R. Combating DDoS attacks in the cloud: requirements, trends, and future directions. *IEEE Cloud Comput*. 2017;4(1):22-32.
13. Osanaiye O, Choo KKR, Dlodlo M. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *J Netw Comput Appl*. 2016;67:147-165.
14. Yan Q, Yu FR, Gong Q, Li J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges. *IEEE Commun Surv Tutor*. 2015;18(1):602-622.
15. Chaudhary D, Bhushan K, Gupta BB. Survey on DDoS attacks and defense mechanisms in cloud and fog computing. *Cloud Security: Concepts, Methodologies, Tools, and Applications*. IGI Global; 2019:1927-1951.

16. Srinivasan K, Mubarakali A, Alqahtani AS, Kumar AD. A survey on the impact of DDoS attacks in cloud computing: prevention, detection and mitigation techniques. *Intelligent Communication Technologies and Virtual Mobile Networks*. Springer; 2019:252-270.
17. Alarqan MA, Zaaba ZF, Almomani A. Detection mechanisms of DDoS attack in cloud computing environment: a survey. *International Conference on Advances in Cyber Security*. Springer; 2019:138-152.
18. Somani G, Gaur MS, Sanghi D, Conti M. DDoS attacks in cloud computing: collateral damage to non-targets. *Comput Netw*. 2016;109:157-171.
19. Verma P, Tapaswi S, Godfrey WW. A request aware module using CS-IDR to reduce VM level collateral damages caused by DDoS attack in cloud environment. *Cluster Comput*. 2021;24:1917-1933.
20. Somani G, Gaur MS, Sanghi D, Conti M, Rajarajan M. DDoS victim service containment to minimize the internal collateral damages in cloud computing. *Comput Electr Eng*. 2017;59:165-179.
21. Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. Service resizing for quick DDoS mitigation in cloud computing environment. *Ann Telecommun*. 2017;72(5-6):237-252.
22. Somani G, Gaur MS, Sanghi D, Conti M, Rajarajan M. Scale inside-out: rapid mitigation of cloud DDoS attacks. *IEEE Trans Dependable Secure Comput*. 2017;15(6):959-973.
23. Deshmukh RV, Devadkar KK. Understanding DDoS attack & its effect in cloud environment. *Procedia Comput Sci*. 2015;49:202-210.
24. Bakshi A, Dujodwala YB. Securing cloud from DDoS attacks using intrusion detection system in virtual machine. *2010 Second International Conference on Communication Software and Networks*. IEEE; 2010:260-264.
25. Vissers T, Somasundaram TS, Pieters L, Govindarajan K, Hellinckx P. DDoS defense system for web services in a cloud environment. *Future Gener Comput Syst*. 2014;37:37-45.
26. Dou W, Chen Q, Chen J. A confidence-based filtering method for DDoS attack defense in cloud environment. *Future Gener Comput Syst*. 2013;29(7):1838-1850.
27. Wang B, Zheng Y, Lou W, Hou YT. DDoS attack protection in the era of cloud computing and software-defined networking. *Comput Netw*. 2015;81:308-319.
28. Girma A, Garuba M, Li J, Liu C. Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment. *2015 12th International Conference on Information Technology-New Generations*. IEEE; 2015:212-217.
29. Bhuyan MH, Bhattacharyya D, Kalita JK. E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric. *Secur Commun Netw*. 2016;9(16):3251-3270.
30. Dehkordi AB, Soltanaghaei M, Boroujeni FZ. The DDoS attacks detection through machine learning and statistical methods in SDN. *J Supercomput*. 2021;77(3):2383-2415.
31. Bouyeddou B, Harrou F, Kadri B, Sun Y. Detecting network cyber-attacks using an integrated statistical approach. *Cluster Comput*. 2021;24(2):1435-1453.
32. Tsobdjou LD, Pierre S, Quintero A. An online entropy-based DDoS flooding attack detection system with dynamic threshold. *IEEE Trans Netw Serv Manag*. 2022;19(2):1679-1689.
33. Sreeram I, Vuppala VPK. HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. *Appl Comput Inform*. 2019;15(1):59-66.
34. Shenfield A, Day D, Ayesh A. Intelligent intrusion detection systems using artificial neural networks. *ICT Express*. 2018;4(2):95-99.
35. Das S, Venugopal D, Shiva S. A holistic approach for detecting DDoS attacks by using ensemble unsupervised machine learning. *Future of Information and Communication Conference*. Springer; 2020:721-738.
36. Jaber AN, Rehman SU. FCM–SVM based intrusion detection system for cloud computing environment. *Cluster Comput*. 2020;23:3221-3231.
37. Zekri M, El Kafhali S, Aboutabit N, Saadi Y. DDoS attack detection using machine learning techniques in cloud computing environments. *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*. IEEE; 2017:1-7.
38. Prasad KM, Siva VS, Nagamuneiah J, Nelaballi S. An ensemble framework for flow-based application layer DDoS attack detection using data mining techniques. *ICT Analysis and Applications*. Springer; 2020:9-19.
39. Verma P, Tapaswi S, Godfrey WW. An adaptive threshold-based attribute selection to classify requests under DDoS attack in cloud-based systems. *Arab J Sci Eng*. 2019;45:2813-2834.
40. Miranda Rios dV, Inacio PR, Magoni D, Freire MM. Detection of reduction-of-quality DDoS attacks using fuzzy logic and machine learning algorithms. *Comput Netw*. 2021;186:107792.
41. Cil AE, Yildiz K, Buldu A. Detection of DDoS attacks with feed forward based deep neural network model. *Expert Syst Appl*. 2021;169:114520.
42. Aydin H, Orman Z, Aydin MA. A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. *Comput Secur*. 2022;118:102725.
43. Pareriya R, Verma P, Suhana P. An ensemble Xgboost approach for the detection of cyber-attacks in the industrial IoT domain. *Big Data Analytics in Fog-Enabled IoT Networks: Towards a Privacy and Security Perspective*. Vol 125. CRC Press; 2023.
44. Gillani F, Al-Shaer E, Lo S, Duan Q, Ammar M, Zegura E. Agile virtualized infrastructure to proactively defend against cyber attacks. *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE; 2015:729-737.
45. Jafarian JH, Al-Shaer E, Duan Q. Openflow random host mutation: transparent moving target defense using software defined networking. *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. ACM; 2012:127-132.
46. Prasad KM, Reddy ARM, Rao KV. BARTD: bio-inspired anomaly based real time detection of under rated App-DDoS attack on web. *J King Saud Univ Comput Inf Sci*. 2017;32:73-87.

47. Velliangiri S, Pandey HM. Fuzzy-Taylor-elephant herd optimization inspired deep belief network for DDoS attack detection and comparison with state-of-the-arts algorithms. *Future Gener Comput Syst*. 2020;110:80-90.
48. Vidal JM, Orozco ALS, Villalba LJG. Adaptive artificial immune networks for mitigating DoS flooding attacks. *Swarm Evol Comput*. 2018;38:94-108.
49. Agarwal A, Khari M, Singh R. Detection of DDOS attack using deep learning model in cloud storage application. *Wirel Pers Commun*. 2021;127:419-439.
50. Krishna EP, Thangavelu A. Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm. *Int J Syst Assur Eng Manag*. 2021:1-14.
51. Gowthul Alam MM, Jerald Nirmal Kumar S, Uma Mageswari R, Michael Raj TF. An efficient SVM based DEHO classifier to detect DDoS attack in cloud computing environment. *Comput Netw*. 2022;215:109138.
52. Alohali MA, Elsadig M, Al-Wesabi FN, Al Duhayyim M, Mustafa Hilal A, Motwakel A. Enhanced chimp optimization-based feature selection with fuzzy logic-based intrusion detection system in cloud environment. *Appl Sci*. 2023;13(4):2580.
53. Zhao S, Chen K, Zheng W. Defend against denial of service attack with VMM. *2009 Eighth International Conference on Grid and Cooperative Computing*. IEEE; 2009:91-96.
54. Latanicki J, Massonet P, Naqvi S, Rochwerger B, Villari M. Scalable cloud defenses for detection, analysis and mitigation of DDoS attacks. *Towards the Future Internet*. IOS Press; 2010:127-137.
55. Yu S, Doss R, Zhou W, Guo S. A general cloud firewall framework with dynamic resource allocation. *2013 IEEE International Conference on Communications (ICC)*. IEEE; 2013:1941-1945.
56. Yu S, Tian Y, Guo S, Wu DO. Can we beat DDoS attacks in clouds? *IEEE Trans Parallel Distrib Syst*. 2013;25(9):2245-2254.
57. Somani G, Johri A, Taneja M, Pyne U, Gaur MS, Sanghi D. DARAC: DDoS mitigation using DDoS aware resource allocation in cloud. *International Conference on Information Systems Security*. Springer; 2015:263-282.
58. Wang X, Chen M, Xing C. SDSNM: a software-defined security networking mechanism to defend against DDoS attacks. *2015 Ninth International Conference on Frontier of Computer Science and Technology*. IEEE; 2015:115-121.
59. Lopez MA, Mattos DMF, Duarte OCM. An elastic intrusion detection system for software networks. *Ann Telecommun*. 2016;71(11-12):595-605.
60. Gilad Y, Herzberg A, Sudkovitch M, Goberman M. CDN-on-demand: an affordable DDoS Defense via untrusted clouds. *Network and Distributed System Security Symposium*. Internet Society; 2016.
61. Sahay R, Blanc G, Zhang Z, Debar H. Towards autonomic DDoS mitigation using software defined networking; 2015.
62. Dahiya A, Gupta BB. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. *Future Gener Comput Syst*. 2021;117:193-204.
63. Kautish S, Reyana A, Vidyarthi A. SDMTA: attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment. *IEEE Trans Industr Inform*. 2022;18(9):6455-6463.
64. Wood P, Gutierrez C, Bagchi S. Denial of service elusion (DoSE): keeping clients connected for less. *2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS)*. IEEE; 2015:94-103.
65. Tsai SC, Liu IH, Lu CT, Chang CH, Li JS. Defending cloud computing environment against the challenge of DDoS attacks based on software defined network. *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Springer; 2017:285-292.
66. Conti M, Lal C, Mohammadi R, Rawat U. Lightweight solutions to counter DDoS attacks in software defined networking. *Wirel Netw*. 2019;25(5):2751-2768.
67. Alqahtani S, Gamble RF. DDoS attacks in service clouds. *2015 48th Hawaii International Conference on System Sciences*. IEEE; 2015:5331-5340.
68. Verma P, Tapaswi S, Godfrey WW. AVDR: a framework for migration policy to handle DDoS attacked VM in cloud. *Wirel Pers Commun*. 2020;115(2):1335-1361.
69. Verma P, Tapaswi S, Godfrey WW. A service governance and isolation based approach to mitigate internal collateral damages in cloud caused by DDoS attack. *Wirel Netw*. 2021;27(4):2529-2548.
70. Kumar A, Somani G. DDoS attack mitigation in cloud targets using scale-inside out assisted container separation. *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE; 2022:1-6.
71. Kumar A, Somani G. Service separation assisted DDoS attack mitigation in cloud targets. *J Inf Secur Appl*. 2023;73:103435.
72. Idziorek J, Tannian M. Exploiting cloud utility models for profit and ruin. *2011 IEEE 4th International Conference on Cloud Computing*. IEEE; 2011:33-40.
73. Anwar Z, Malik AW. Can a DDoS attack meltdown my data center? A simulation study and defense strategies. *IEEE Commun Lett*. 2014;18(7):1175-1178.
74. Idziorek J, Tannian MF, Jacobson D. The insecurity of cloud utility models. *IT Prof*. 2012;15(2):22-27.
75. Sides M, Bremler-Barr A, Rosensweig E. Yo-Yo attack: vulnerability in auto-scaling mechanism. *ACM SIGCOMM Comput Commun Rev*. 2015;45(4):103-104.
76. Sqalli MH, Al-Haidari F, Salah K. EDoS-shield—a two-steps mitigation technique against EDoS attacks in cloud computing. *2011 Fourth IEEE International Conference on Utility and Cloud Computing*. IEEE; 2011:49-56.
77. Masood M, Anwar Z, Raza SA, Hur MA. EDoS armor: a cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments. INMIC. IEEE; 2013:37-42.

78. Kumar MN, Sujatha P, Kalva V, Nagori R, Katukojwala AK, Kumar M. Mitigating economic denial of sustainability (EDoS) in cloud computing using in-cloud scrubber service. *2012 Fourth International Conference on Computational Intelligence and Communication Networks*. IEEE; 2012:535-539.
79. Baig ZA, Sait SM, Binbeshr F. Controlled access to cloud resources for mitigating economic denial of sustainability (EDoS) attacks. *Comput Netw*. 2016;97:31-47.
80. Bhingarkar S, Shah D. FLNL: fuzzy entropy and lion neural learner for EDoS attack mitigation in cloud computing. *Int J Model Simul Sci Comput*. 2018;9(06):1850049.
81. Dennis JB, Priya MS. A profile-based novel framework for detecting EDoS attacks in the cloud environment. *Wirel Pers Commun*. 2021;117(4):3487-3503.
82. Dinh PT, Park M. R-EDoS: robust economic denial of sustainability detection in an SDN-based cloud through stochastic recurrent neural network. *IEEE Access*. 2021;9:35057-35074.
83. Shah SQA, Khan FZ, Ahmad M. Mitigating TCP SYN flooding based EDOS attack in cloud computing environment using binomial distribution in SDN. *Comput Commun*. 2022;182:198-211.
84. Karthika A, Muthukumaran N. An ADS-PAYG approach using trust factor against economic denial of sustainability attacks in cloud storage. *Wirel Pers Commun*. 2022;122(1):69-85.
85. Al-Haidari F, Salah K, Sqalli M, Buhari SM. Performance modeling and analysis of the EDoS-shield mitigation. *Arab J Sci Eng*. 2017;42(2):793-804.
86. Schmidt D, Suriadi S, Tickle A, et al. A distributed denial of service testbed. *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*. Springer; 2010:338-349.
87. Calvet J, Fernandez JM, Bureau PM, Marion JY. Large-scale malware experiments: why, how, and so what? *Proceedings of the 2010 Virus Bulletin Conference (VB)*. Welivesecurity; 2010.
88. Hussain A, Schwab S, Thomas R, Fahmy S, Mirkovic J. DDoS experiment methodology. *Proceedings of the DETER Community Workshop on Cyber Security Experimentation*. Vol 8. ResearchGate; 2006.
89. Özçelik İ, Brooks RR. Deceiving entropy based DoS detection. *Comput Secur*. 2015;48:234-245.
90. Bhuyan MH, Bhattacharyya D, Kalita JK. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recogn Lett*. 2015;51:1-7.
91. Ma X, Chen Y. DDoS detection method based on chaos analysis of network traffic entropy. *IEEE Commun Lett*. 2013;18(1):114-117.
92. Shiaeles SN, Katos V, Karakos AS, Papadopoulos BK. Real time DDoS detection using fuzzy estimators. *Comput Secur*. 2012;31(6):782-790.
93. Devi SR, Yogesh P. Detection of application layer DDoS attacks using information theory based metrics. *The Second International Conference on Computer Science, Engineering*. Vol 10. Department of Information Science and Technology, College of Engineering Guindy; 2012:213-223.
94. Hermenier F, Ricci R. How to build a better testbed: lessons from a decade of network experiments on Emulab. *International Conference on Testbeds and Research Infrastructures*. Springer; 2012:287-304.
95. Wu YC, Tseng HR, Yang W, Jan RH. DDoS detection and traceback with decision tree and grey relational analysis. *Int J Ad Hoc Ubiquitous Comput*. 2011;7(2):121-136.
96. Bhatia S, Schmidt D, Mohay G, Tickle A. A framework for generating realistic traffic for distributed denial-of-service attacks and flash events. *Comput Secur*. 2014;40:95-107.
97. Garcia S, Grill M, Stiborek J, Zunino A. An empirical comparison of botnet detection methods. *Comput Secur*. 2014;45:100-123.
98. Sharafaldin I, Lashkari AH, Hakak S, Ghorbani AA. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE; 2019:1-8.
99. Bhuyan MH, Bhattacharyya DK, Kalita JK. Towards generating real-life datasets for network intrusion detection. *Int J Netw Secur*. 2015;17(6):683-701.
100. Sharafaldin I, Lashkari AH, Ghorbani AA. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. Vol 1. SciTePress; 2018:108-116.
101. Cho K, Mitsuya K, Kato A. Traffic data repository AT the wide project. *Project Usenix Freenix Track*. Usenix; 2000.

How to cite this article: Verma P, Bharot N, Breslin JG, Sharma M, Chaurasia N, Vidyarthi A. Uncovering collateral damages and advanced defense strategies in cloud environments against DDoS attacks: A comprehensive review. *Trans Emerging Tel Tech*. 2024;35(4):e4934. doi: 10.1002/ett.4934