RESEARCH PAPER

Survey: Impact, Detection and Mitigation Techniques of DDOS and EDOS attacks in Cloud Computing Services

Suneetha Bandeela[1], Suneetha Bulla[2], Sunanda N[3]

[1]*Research Scholar, Department of CSE, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur District, A.P., INDIA, 522 302*
[2]*Associate professor , Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur District, A.P., INDIA, 522 302*
[3]*Assistant Professor, VNR Vignana Jyothi Institute of Engineering and Technology, Nizampet, Hyderabad, Telangana, 500090*

ABSTRACT
Cloud computing emerges as the next revolution technology in the field of IT industry. Business organization shifts their traditional method of server-client based service to cloud –based service where customers are provided with subscription-based cloud services. On Contrary cloud computing services demands high level security due to centralized nature of operation. Lots of security breaches have been encountered in cloud environment as single point failure, eaves dropping, node hijacking and many more. At the same time discusses the security threat occurred due to Denial-of-Service attack (DDoS) which occurs when legitimate users are deprived of using cloud resources due to resource exhaustion. Even though services in cloud are available through service level agreement to the users, elasticity and auto scalability leads to increased use of cloud services during DDoS attack leading to creation of new type of attack named Economic Denial of Sustainability attack (EDoS). Even though this attack exists in small level it highly targets the financial loss of the company aimed. In term of clous application DDoS attacks plays important role. The elasticity property shows solution to the DDoS attack and at the same time leads new type of attack EDoS attack. Many researchers implemented DDoS and EDoS detection frameworks using DDoS impact, but there was variation. This paper conducted survey to differentiate EDoS and DDoS, DDoS Characterization, detection, mitigation, and prevention of these attacks. Further a detailed report of EDoS has been summarized in the paper..

Keywords: DDoS, EDoS, Cloud Datacentre, Elasticity, Detection Framework.
How to cite this article: Bandeela S, Bulla S, Sunanda N: Survey: Impact, Detection and Mitigation Techniques of DDOS and EDOS attacks in Cloud Computing Services .Int J Drug Deliv Technol. 2026;16 (3s): 951-959; DOI: 10.25258/ijddt.16.3s.115

Source of support:. None
Conflict of interest: None

INTRODUCTION

Evolution of Internet and internet Services facilitates business and all transaction to happen online. The demand of internet-based computing and services increases day –by-day what we called as cloud computing services. This technology is introduced by Prof. John McCarthy in 1960s. The standardisation of Cloud Computing is done by National Institute of Standards and Technology (NIST) by setting a framework which should be adopted by Federal Government standards. NIST describes cloud computing as model and the significance of adopting cloud infrastructure provides several features as on –demand service, unlimited storage, scalable resource, quick deployment with fast backup and retrieval of information with minimal human intervention [1]. The infrastructure provided by cloud are Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. Private clouds are owned by specific organization which services only internal community whereas public clouds provide cloud services to public organizations and common users. Hybrid cloud is a model framed by both private and public cloud. The cloud computing offers services as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Software as a service offers software application to be accessed clients provided by cloud providers whereas platform resource is provided by PaaS and a virtual infrastructure resource is given by IaaS.

Cloud Computing provides a promising solution to on premise fixed infrastructure. Many business environment and government sectors have shifted their infrastructure to cloud environment. The provision includes on demand resource allocation, pay on use, and no maintenance overhead with good hardware utilization. Despite its utilization a big question flashed regarding the security breach in cloud environment. One such visible attack is Denial of Service attack (DoS) where the victim acts as legitimate user and try to flood the network with active server thereby the requesting service becomes unavailable when needed. Many legitimate request and services will be overflowed in service queue. A variant to DoS is distributed DoS where group of victims targets a particular server [2]. It is reported that about 20% of world enterprise faced DDoS problem. Amazon EC2 cloud server, Rack space server are popular DDoS attack in the last decade. The attack imposes

**Author for Correspondence: Suneetha Bandeela*

heavy downtime and business losses over a long term. It is reported that one-third of the DDoS attack occurs over cloud services. One such consequence of DDoS attack causes “economic loss”. Report of 444k USD loss due to DDoS attack is estimated [3].

The consequence of DDoS attack leads another attack called economic Denial of Sustainability (EDoS) attack [4]. This is caused mainly due to elastic feature or auto scaling feature enabled due to virtualization of the server. In this paper, we provide a detailed survey of DDoS attack and EDoS attack in cloud environment. "Economic Denial of Sustainability (EDoS)" is a sophisticated form of cyberattack that aims to undermine the long-term economic viability and sustainability of businesses, organizations, or even entire industries. Unlike traditional cyberattacks that focus on immediate disruption or data theft, EDoS attacks are strategically designed to inflict financial harm and erode an entity's ability to maintain its operations over time.

These attacks can take various forms, including resource exhaustion, financial manipulation, or market manipulation. Resource exhaustion EDoS attacks involve overwhelming a target's infrastructure, such as a website or cloud service, with excessive demands on its resources, causing it to incur substantial operational costs. Financial manipulation EDoS attacks may involve exploiting vulnerabilities in financial systems, stock markets, or cryptocurrencies to manipulate prices or induce financial losses. Market manipulation EDoS attacks can disrupt supply chains, affect product availability, or create artificial scarcity, leading to economic instability. Detecting and mitigating EDoS attacks is challenging due to their covert nature and long-term impact. Many businesses and organizations are now turning to advanced technologies, including machine learning and artificial intelligence, to identify unusual patterns of behaviour that could signal an EDoS attack in progress. There was a necessity to analyse the impact of the EDoS attack to detect and mitigate attacks effectively

Objectives of the study

Study the background of DDoS and EDoS attack to categorize the attacks.

Identify the impact of the EDoS attack and DDoS attack in cloud computing data canter.

Study the detection and mitigation techniques, which was introduced by researchers to identify the nature of attack to propose accurate detection framework.

The rest of this paper is organized as follows, in Section 2 discussed about various DDoS attacks. The essentials and the scientific lining model of EDoS attacks are clarified in section

3. The comparative study of DDoS and EDoS detection mechanisms in Section 4. The results are presented in Section 5and finally the conclusions are discussed in section 6.

DDoS Attack impact and its Detection and Mitigation Mechanisms

Types of DDOS attacks

Distributed Denial of Service (DDoS) are security attacks in cloud environment by disturbing the normal operation on targeted server/device. DoS attack typically operates from one machine and targets the victim by flooding the target with continuous request and shut down its operation whereas DDoS attack targets the victim from multiple machines called botnet and flood traffic from their individual machines to the target. The main cause of DDoS attack in cloud is the resource unavailability in cloud. This occurs if multiple service request is floated to the server which makes the service unavailable to the legitimate client. The DDoS attack is mainly characterised by amount of traffic and vulnerable threat of the target node. The following briefs various types of DDoS attack due to network traffic [11,12]. The DDoS attacks classified into Reflection-based and Exploitation-based attacks.

Reflection-based DDoS

Are there attacks where the attacker's identity remains hidden using a legitimate third-party component? Attackers send packets to the reflection servers with the source IP address assigned to the victim and the IP address to mask the victim with reply packets. These attacks can be carried out by application layer protocols that use transport layer protocols, ie. Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or a combination of both. As shown in Figure 1, TCP-based attacks in this category include MSSQL, SSDP, while UDP-based attacks include CharGen, NTP, and TFTP. There are certain attacks that can be performed using either TCP or UDP, such as DNS, LDAP, NETBIOS and SNMP.

Exploitation-based attacks

Are there attacks where the attacker's identity is hidden by a legitimate third-party component? Attackers send packets to reflection servers with the source IP address set to the target victim's IP address to flood the victim with reply packets. These attacks can also be
performed through application layer protocols using transport layer protocols ie. TCP and UDP. TCP-based exploits include SYN Flood, and UDP-based attacks include UDP Flood and UDP-Lag. A UDP flood attack is initiated by sending multiple UDP packets to a remote host.

Impact of DDoS attack

DDoS attack pose a serious problem to network and network services. It has both direct and indirect impact on network services. Direct attack has greater impact as it directly connected with attack as cause the following serious consequences as a) Service downtime b)Economic losses c) Business loss d)Revenue loss d) interrupting dependent services. The impact of indirect attack is felt at later which a causes a) Energy Consumption costs b)Attack mitigation cost c)Resource and Economic loss [9-10]

The consequences of a DDoS assault, such as service outage and customer data theft, can undermine client side confidence. Customers have the option of switching to a rival company or using online social networking sites to express their resentment and dissatisfaction. The theft of important information is the attack's true goal. In this kind of assault, the risk performer directs a DDoS attack at a certain portion of the system while executing targeted attacks at several targets. The goal is to reconcile these various targets to either steal crucial data throughout the

DDoS assault or introduce a future access to the system and its resources via a backdoor. These assaults may because IT personnel are concentrated on controlling the DDoS attack itself while other nefarious conduct is overlooked.

DDoS Attack Detection and Mitigation techniques

The following section explains the DDoS attack mitigation techniques employed in cloud computing environment.

Challenge/Response Protocol

The technique of DDoS prevention in the cloud is thought of as a proactive strategy, where the presumptive attacker's requests are examined, segregated, or rejected before they begin to have an impact on the server. The "presence of attack" state, which is typically available to attack discovery and moderation procedures, is not present in this sort of preventative strategy. Therefore, regardless of whether a client is legitimate or not, the preventative tactics apply to all of them [25-28].

Hidden Server /Port Method

An essential tactic to eliminate a direct communication channel between the client and the server is to use hidden servers or hidden assets that incorporate characteristics like ports. By using a middle hub or proxy to act as a transmitting expert, it is accomplished. The primary duties of a transmitting specialist may include distributing the load across the servers, ensuring that they are error-resistant, recovering servers, and scanning incoming traffic for potential vulnerabilities. Hidden servers or ports are defence mechanisms to safeguard the
legitimate service against DDoS attacks. In this way, requests to hidden servers or ports are redirected by validation/proxy servers, and the customer experiences the key server[29-31]. Validation provides a layer of protection to protect the actual service. The hidden server assists in preventing malicious attempts to affect the primary server. Another justification for redirection and server load balancing may be aided by the additional layer. The drawback includes a time delay, the cost of the mediator servers, the extra work required to calculate redirection and manage it at the moderate hub.

Restrictive Source Access Method

To prevent DDoS attacks from occurring when access is reputation-based or delayed, nearly all admission control systems use prohibitive access. These approaches provide a good way to optimise server capacity by allowing requests that depend on the available resources [25, 32-34]. The computation of "ability" or "reputation" depends on the time it takes to solve the cryptographic problems or the prior access prototype.

Attack Anomaly Detection

It has been fixed, and the server-side can access the attack symptoms in terms of its services and performance measures. Some assault symptoms are early warning signs that the attack has just begun to take shape or might be an infrastructure [35-37]. The server's performance suffered because of the attack. The methods could appear to be similar in "attack prevention" at times, and many auxiliary contributions have been made.

Commonly used tools for this purpose include packet traces, web access logs, established linkages, and demand headers. The log file, which contains attack traces and past historic patterns, can be used to find the unusual pattern. A greater variety of criteria have been used to produce web behavioural activity, and assessments are focused on those qualities [38-40] The majority of the time, web developers have used typical web traffic as a baseline prototype. This type of common web activity is observed during the time the assault is not being carried out.

The necessary arrangements of activities that are associated with these recognition procedures include feature selection of this kind, dataset preparation, and testing against these researched principles. For a common type of frameworks, a thorough overview of identification strategies is provided in [41]. These kinds of attack tactics are becoming prevalent in many cloud-focused attacks. The behavioural differentiating in feature extraction and correlating preparation introduces the main challenges for DDoS assault identification strategies. The false alarms (both positive and negative) that the investigation criteria of methods uncover cause the testing period for incoming activity. The difficulty in preventing IP spoofing can defeat some detection approaches.

Resource usage

A virtual machine can also offer essential information or a prediction of the impending DDoS attack in the presence of the DDoS attack. Infrastructure as a Service clouds are often operated by virtualized servers in cloud infrastructures, allowing the hypervisor to continuously track the resource usage of each virtual machine running on a real server. Once these virtual computers start to approach the specified resource utilisation criteria, an attack can be suspected as being plausible. [42] Suggested options based on a resource that was easily accessible and had virtual machines as well as the resources' forthcoming requirements. Similar to [43], who employed performance counters and activity to identify resource use in a virtual machine and extract potential attack moderation. Asset utilisation is a very significant and indirect factor in determining the possibility of attack.

The success of the asset utilization-based profiling and recognition tactics is indirectly related to the DDoS attacks, which are evolving into asset-intensive attacks. A different approach, for instance, triggers auto-scaling techniques based on "over-burden" and "under-load" conditions of the chosen targeted virtual computers. The attribute suggests a potential link between the virtual machines asset utilisation and a DDoS-driven asset spike

EDoS Attack impact and its Detection and Mitigation Mechanisms

How EDoS attack variant from DDOS

Economic Denial of Sustainability attack (EDoS) **is** one of the crucial security problem threatening today’s internet is DoS and DDoS attack .The outcome of the attack fails to provide the intended service to the legitimate user. To overcome DDoS attack, a new technique named as sPOW has been introduced that continuously increases the

bandwidth of the devices /services. Although it restores the service availability of legitimate users it creates new problem of high cost to the clients demanding the service. Hence a new definition for this type of problem is cloud computing is coined as Economic Denial of Sustainability attack (EDoS) [49]. The attack targeted organization or individual. EDoS attacks are a variation of Distributed Denial of Service (DDoS) attacks, which are designed to overwhelm a target's resources, such as websites or online services, by flooding them with a massive amount of malicious traffic [49].

The main aim of an EDoS attack is not only to disrupt the target's online operations temporarily but also to inflict long-term financial damage. Unlike traditional DDoS attacks that focus on disrupting availability, EDoS attacks specifically aim to cripple an organization's financial sustainability by causing significant financial losses, reputation damage, or by exploiting specific vulnerabilities in their business model [50]. It typically target organizations that rely heavily on their online presence and transactions, such as e- commerce platforms, financial institutions, or online service providers. Attackers employ various techniques to carry out an EDoS attack, including generating many fraudulent transactions, overwhelming customer support systems, exploiting weaknesses in payment processing mechanisms, or manipulating supply chain processes. The consequences of an EDoS attack can be severe, leading to financial losses, customer dissatisfaction, erosion of trust, and potentially even business shutdown. Therefore, organizations need to implement robust cybersecurity measures, such as network monitoring, traffic analysis, and application- level security solutions, to detect and mitigate the impact of EDoS attacks

Impact of EDoS attack

The main objectives of an EDoS attack is to disrupt the economic sustainability of the targeted entity, causing financial harm and long-term damage.

Financial Impact: EDoS attacks aim to inflict significant financial losses on the target, potentially leading to reputational damage, customer churn, and even bankruptcy in extreme cases [33].

Exploitation of Vulnerabilities: Attackers may exploit vulnerabilities in an organization's business model, payment systems, supply chain, or customer support processes to disrupt operations and cause financial harm [33]

Targeted Industries: EDoS attacks often target industries that rely heavily on online operations, such as e-commerce platforms, financial institutions, cloud service providers, and digital market places [51-54]

Significance of EDoS attack

While it is important to understand the concept of EDoS (Economic Denial of Sustainability) attacks for security purposes, it is essential to note that these attacks are considered malicious and illegal activities. The intent behind EDoS attacks is to cause financial harm and disrupt the economic sustainability of targeted entities. As such, there are no legitimate or ethical advantages associated with EDoS attacks. Instead, EDoS attacks can lead to severe consequences for both the targeted entity and the attackers themselves, including legal repercussions, reputational damage, and potential financial losses. It is always advisable to adhere to ethical principles and legal boundaries when it comes to cybersecurity and engage in responsible online behaviour.

Impact of EDoS attack

Legal Consequences: EDoS attacks are illegal activities and can lead to severe legal repercussions for the attackers. Engaging in such attacks can result in criminal charges, fines, and potential imprisonment.

Reputational Damage: EDoS attacks can severely damage the reputation of the attackers. Once their involvement in such malicious activities is discovered, it can lead to distrust from peers, colleagues, and potential employers.

Countermeasures: Organizations invest significant resources in implementing cybersecurity measures to detect and mitigate EDoS attacks. As a result, attackers may encounter robust defence mechanisms that make it more challenging to successfully execute an EDoS attack.

Collateral Damage: EDoS attacks can have unintended consequences and cause collateral damage. In some cases, innocent individuals or organizations may be affected by the attack, resulting in financial losses and disruptions to their operations

Loss of Opportunities: Engaging in EDoS attacks can prevent individuals from pursuing legitimate opportunities in the cybersecurity field or related industries. Employers and organizations are unlikely to consider candidates involved in illegal activities.

Financial Losses: EDoS attacks can lead to financial losses for the targeted entities, but they can also backfire on the attackers themselves. If the attackers are identified and brought to justice, they may be held financially responsible for the damages caused, resulting in significant financial consequences for them.

Ethical Considerations: EDoS attacks violate ethical principles and moral standards. Engaging in activities that intentionally harm others for personal gain or satisfaction is widely considered unethical and can have long-term consequences on an individual's personal and professional life.

Diminished Opportunities for Dialogue: Rather than engaging in harmful attacks, constructive dialogue and ethical hacking practices provide better avenues for addressing vulnerabilities and improving the security of digital systems.

Disruption of Financial Operations: The primary objective of an EDoS attack is to disrupt the targeted entity's financial operations. This can include disrupting payment processing systems, compromising financial transactions, or manipulating supply chain processes. As a result, the organization may experience difficulties in conducting its normal business operations and managing financial transactions.

Financial Losses: EDoS attacks can lead to significant financial losses for the targeted entity. The disruption of financial operations can result in missed sales opportunities, transaction failures, or the inability to process payments. These financial losses can have a direct impact on the organization's revenue, profitability, and overall financial sustainability.

Reputational Damage: EDoS attacks can cause reputational damage to the targeted entity. Customers, partners, and stakeholders may view the organization negatively due to the disruption of services, financial difficulties, or perceived security vulnerabilities. Rebuilding trust and restoring a positive reputation can be challenging and time-consuming.
Customer Dissatisfaction and Churn: If an organization's services or operations are significantly disrupted by an EDoS attack, it can lead to customer dissatisfaction. Customers may experience difficulties in accessing services, making transactions, or receiving support. This can result in customer churn, as they may seek alternative providers who can offer more reliable and secure services.
Legal and Regulatory Issues: EDoS attacks may violate various laws and regulations, leading to legal consequences for the attackers and potential legal liabilities for the targeted entity. Depending on the jurisdiction, the targeted organization may be required to notify affected customers, report the incident to regulatory authorities, or face legal actions from customers, partners, or shareholders.
Operational and Recovery Costs: Recovering from an EDoS attack can be costly for the targeted entity. It may involve investing in additional cybersecurity measures, conducting forensic investigations, implementing enhanced monitoring systems, and hiring external experts for incident response and recovery. These operational and recovery costs can further impact the organization's financial stability.
Business Disruption and Downtime: EDoS attacks can cause significant disruption to the targeted entity's business operations. It may result in service outages, website unavailability, or slowdowns in online transactions. The organization may need to invest time and resources to restore normal operations and address the vulnerabilities that led to the attack.
Regulatory Scrutiny and Compliance Issues: EDoS attacks can attract regulatory scrutiny, especially in industries that handle sensitive customer data or financial transactions. Regulatory authorities may investigate the incident, assess the organization's security.
EDoS Attack Detection and Mitigation Mechanisms
Most CC and network monitoring researchers use predefined thresholds and entropy methods to detect anomalies in network traffic. The following are some well-known EDoS defense strategies.
Self-verifying proof of work (sPoW): Self-verifying Proof of Work (sPoW) is a concept that is used to modify network-level DDoS traffic, identify EDoS attacks, implement on-demand network filtering, and give priority to genuine traffic. There are two primary activities in sPoW: 1) Isolating and filtering network level DDoS traffic using direct packet pattern matching and 2) enabling the remaining genuine traffic flow. A mix of both legitimate and application-level DDoS traffic competes for server resources when resolving Self-Verifying Proof-of-Work (sPoW). The initialization function rejects DDoS activity at the network level before starting the download mechanism. Another measure reduces the total amount of expensive cloud resources required for application-level DDoS by using a puzzle-solving technique that enables true traffic competition. Second, the server must allocate separate channels for each request. When there are many incoming requests, the server generates many puzzles, which can lead to a puzzle stack attack if the puzzles are not solved in time[58].
Cloud Trace Back: The Deterministic Packet Marking (DPM) method is the basis of CTB [14]. To be close to the origin of the cloud network, CTB is implemented in the edge routers. This is placed in front of the web server as an instruction to use the Cloud Trace Back Mark (CTM) in the CTB header. All service requests are first sent to the CTB for tagging to prevent effective interception and direct attack against the service provider and address. If the attack crashes the web service, the target server recovers and rebuilds the CTM token to reveal the source of the attack. Cloud Protector (CP) is required for CTB to stop a DDoS attack. CP works as a filter engine. To facilitate DDoS detection and filtering, CP is a self- learning back-propagation neural network (NN) [33]. A neural network consists of input, hidden, and output layers and consists of several connected units. In neural networks, the focus is on the Threshold Logic Unit (TLU). TLU calculates specified thresholds for verification and comparison after entering inputs into a set of biased quantities [59].
EDoS Shield: The Virtual Firewall (VF) and Verifier Nodes that make up the EDoS-Shield mitigation mechanism work together to carry out the EDoS mitigation tasks. The whitelist and blacklist are the two lists used by the firewall to filter inbound requests. The control node performs a Turing test on each initial access request made by the client. The client's IP address will be added to the white list and subsequent requests from the same client will be directed directly to the cloud scheduler, who will approve resource allocations, if the client passes the Turing test. Al-Haidari and co-researchers [60] introduced an improved version of the EDoS-Shield in 2012 that appends a TimeTo-Live (TTL) field to the IP address of end- users requesting cloud services. By employing a TTL field, the authors hope to distinguish between hostile clients using spoofed IP addresses and legitimate clients, thereby counteracting the threat posed by faked IP addresses.
Scrubber service: Scrubber Service, an on-demand EDoS mitigation web service, launched an In-Cloud Scrubber that also inspects encryption tasks sent from the client side [61]. There are two modes available to the service provider: normal mode and suspicious mode. The web server operates in normal mode when the service provider believes that everything is normal. In the suspicious state, the user or consumer brute force solves the created encryption problem to ensure the legitimacy of the service. If a service provider notices that the web server and resources are being used at a high rate and beyond what is acceptable, this may be a sign of an advanced DDoS attack. To create and verify a hard puzzle, the service provider activates the suspect state and calls the Scrubber service on demand. The Scrubber service develops and monitors a moderation puzzle when a service provider detects low-level DDoS attacks, ie. whether the level of resource depletion on a web server is within acceptable limits in relation to normal bandwidth usage.
EDoS Armor: With **access** and congestion control, it is a **dual** solution. This **defense** system has **several** layers;

initially, when a user starts a session, the server sends a challenge to the user, which **can be in** the form of a GTT or a cryptographic puzzle. **When** the user completes the challenge, **access** control **receives a** request. If the user was unable to resolve, their session would be ended and their ability to connect to the server would be restricted. Users are restricted by this system using the port-hiding technique since an attack cannot be launched without a valid port number. The following stage involves monitoring user browsing activity for ongoing learning. If unusual behaviour is noticed, the service priority for those users is decreased, slowing down service response and reducing application DDoS [62]

Classification of EDoS and DDoS Impact in Cloud Computing Services

S.No	Aspect	DDoS	EDoS
1	Objective	Disrupt availability of a target system, service, or network	Undermine the economic sustainability of a target; inflict financial harm or
			erode long-term viability
2	Method	Flood the target with traffic from a botnet or multiple sources to consume resources	Various forms, including resource exhaustion, financial manipulation, or market manipulation
3	Duration	Typically short-lived, lasting hours or less	May be prolonged, potentially causing long-term economic damage
4	Visibility	More visible, as it directly disrupts services, often quickly detected	Can be stealthier and not immediately apparent, involving financial manipulation or other tactics that are not as easily detected as network traffic floods
5	Primary Impact	Service unavailability, network congestion	Financial losses, erosion of economic stability
6	Target	Network infrastructure, websites, online services	Financial institutions, businesses, industries, markets
7	Prevention/Mitigation	Network security measures, traffic filtering, content delivery networks	Risk management, financial security protocols, anomaly detection
8	Typical Tools Used	Botnets, amplification techniques (e.g., DNS amplification)	Social engineering, financial manipulation, supply chain disruptions

Open Issues in Research

Since many defensive mechanisms has been proposed by many researchers still there is a need of wide-spread unique solution for solving primary cloud problem is needed. There is a need of integrated security solution for different security problem to easily implement in security devices. Another challenge faced in cloud is improper server resource utilization due to multi tenancy and if DDoS attack focus multi tenancy issue resource will become unavailable to the requested service

Conclusion

In this work we concluded the nature of DDoS attack, the types of DDoS attack, its impact, detection, and Prevention strategies. With the aid of these kinds of solutions, a cloud environment can be developed with a variety of characteristics, such as resource allocation based on demand services, bot cloud, and topology management utilising software defined networks. These surveys make it easier to evaluate the benefits and drawbacks of various attacks and their remedies. Further the impact of DDoS in terms of financial aspects in the form of EDoS has been briefly explained. This survey opens the current existing security patterns available for DDoS attack and briefs the open research problems

REFERENCE

1. NIST, S. (2011). 800-145,“. A NIST definition of cloud computing”,[online] http://csrc. nist. gov/publications/nistpubs/800-145/SP800-145. pdf.
2. Kaufman, L. M. (2009). Data security in the world of cloud computing. IEEE Security & Privacy, 7(4), 61-64.
3. Geluvaraj, B., BV, S. K., Umesh, M., & Yaqoob, Y.

(2023, January). DDoS Attack Detection and Analytics. In 2023 International Conference for Advancement in Technology (ICONAT) (pp. 1-4). IEEE.
4. Dennis, J. B., & Priya, M. S. (2021). A Profile-Based Novel Framework for Detecting EDoS Attacks in the Cloud Environment. Wireless Personal Communications, 117(4), 3487- 3503
5. Kushwah, G. S., & Ranga, V. (2021). Distributed denial of service attack detection in cloud computing using hybridextreme learning machine. Turkish Journal of Electrical Engineering and Computer Sciences, 29(4), 1852-1870.
6. Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS attack & its effect in cloud environment. Procedia Computer Science, 49, 202-210.
7. Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M., & Cheriet, M. (2015). Taxonomy of distributed denial of service mitigation approaches for cloud computing. Journal of Network and Computer Applications, 58, 165-179.
8. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30-48.
9. Srinivasan, K., Mubarakali, A., Alqahtani, A. S., & Dinesh Kumar, A. (2020). A survey on the impact of DDoS attacks in cloud computing: prevention, detection and mitigation techniques. In Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019 (pp. 252-270). Springer International Publishing.
10. Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. Computer Networks, 57(2), 378-403.
11. Abliz, M. (2011). Internet denial of service attacks and defense mechanisms. University of Pittsburgh, Department of Computer Science, Technical Report, 1-50.
12. Specht, S. (2004). M. and RB Lee. Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, 543-550
13. Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. Computer Networks, 57(2), 378-403.
14. Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2013). Evolution, detection and analysis of malware for smart devices. IEEE Communications Surveys & Tutorials, 16(2), 961-987.
15. Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813-80828.
16. Anstee, D., Bowen, P., Chui, C. F., & Sockrider, G. (2016). Worldwide Infrastructure Security Report. Arbor Networks.
17. Brief, A. A. (2011). The growing threat of application-Layer DDoS attacks. Arbor Networks, Feb, 28.
18. Ben-Porat, U., Bremler-Barr, A., & Levy, H. (2012). Vulnerability of network mechanisms to sophisticated DDoS attacks. IEEE Transactions on Computers, 62(5), 1031- 1043.
19. Gonsalves, A. (2013). Mobile Devices Set to Become Next DDoS Attack Tool.
20. Goel, R., Garuba, M., & Girma, A. (2014, April). Cloud computing vulnerability: DDoS as its main security threat, and analysis of IDS as a solution model. In 2014 11th International Conference on Information Technology: New Generations (pp. 307-312). IEEE.
21. Stevanovic, D., & Vlajic, N. (2014, December). Next generation application-layer DDoS defences: applying the concepts of outlier detection in data streams with concept drift. In 2014 13th International Conference on Machine Learning and Applications (pp. 456-462). IEEE.
22. Shea, R., & Liu, J. (2012). Performance of virtual machines under networked denial of service attacks: Experiments and analysis. IEEE Systems Journal, 7(2), 335-345.
23. Tsai, H. Y., Siebenhaar, M., Miede, A., Huang, Y., & Steinmetz, R. (2011). Threat as a service?: Virtualization's impact on cloud security. IT professional, 14(1), 32-37.
24. Godfrey, M., & Zulkernine, M. (2014). Preventing cache-based side-channel attacks in a cloud environment. IEEE transactions on cloud computing, 2(4), 395-408.
25. Al-Haidari, F., Sqalli, M. H., & Salah, K. (2012, June). Enhanced EDoS-shield for mitigating EDoS attacks originating from spoofed IP addresses. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (pp. 1167-1174). IEEE.
26. Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., & Stavrou, A. (2014). A moving target DDoS defense mechanism. Computer Communications, 46, 10-21.
27. Karnwal, T., Sivakumar, T., & Aghila, G. (2012, March). A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (pp. 1-5). IEEE
28. Masood, M., Anwar, Z., Raza, S. A., & Hur, M. A. (2013, December). EDoS Armor: A cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments. In INMIC (pp. 37-42). IEEE.
29. Jeyanthi, N., & Mogankumar, P. (2014). A virtual firewall mechanism using army nodes to protect cloud infrastructure from ddos attacks. Cybernetics and Information Technologies, 14(3), 71-85.
30. Baig, Z. A., & Binbeshr, F. (2013, December). Controlled virtual resource access to mitigate economic

denial of sustainability (EDoS) attacks against cloud infrastructures. In 2013 International Conference on Cloud Computing and Big Data (pp. 346-353). IEEE.
31. Saini, B., & Somani, G. (2014). Index page based EDoS attacks in infrastructure cloud. In Recent Trends in Computer Networks and Distributed Systems Security: Second International Conference, SNDS 2014, Trivandrum, India, March 13-14, 2014, Proceedings 2 (pp. 382-395). Springer Berlin Heidelberg.
32. Jeyanthi, N., & Mogankumar, P. (2014). A virtual firewall mechanism using army nodes to protect cloud infrastructure from ddos attacks. Cybernetics and Information Technologies, 14(3), 71-85.
33. Idziorek, J., Tannian, M., & Jacobson, D. (2011, October). Detecting fraudulent use of cloud resources. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop (pp. 61-72).
34. Ismail, M. N., Aborujilah, A., Musa, S., & Shahzad, A. (2013, January). Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach. In Proceedings of the 7th international conference on ubiquitous information management and communication (pp. 1-6).
35. Shamsolmoali, P., & Zareapoor, M. (2014, September). Statistical-based filtering system against DDOS attacks in cloud computing. In 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1234-1239). IEEE.
36. Chen, Q., Lin, W., Dou, W., Yu, S.: CBF: a packet filtering method for DDoS attack defense in cloud environment. In: IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 427–434. IEEE (2011)
37. Vissers, T., Somasundaram, T. S., Pieters, L., Govindarajan, K., & Hellinckx, P. (2014). DDoS defense system for web services in a cloud environment. Future Generation Computer Systems, 37, 37-45.
38. Graham, M., Winckles, A., & Sanchez-Velazquez, E. (2015, July). Botnet detection within cloud service provider networks using flow protocols. In 2015 IEEE 13th International Conference on Industrial Informatics (INDIN) (pp. 1614-1619). IEEE.
39. Yu, S., Tian, Y., Guo, S., & Wu, D. O. (2013). Can we beat DDoS attacks in clouds?
40. IEEE Transactions on parallel and distributed systems, 25(9), 2245-2254
41. Gilad, Y., Herzberg, A., Sudkovitch, M., & Goberman, M. (2016, February). CDN-on- Demand: An affordable DDoS Defense via Untrusted Clouds. In NDSS.
42. Mansfield-Devine, S. (2015). The growth and evolution of DDoS. Network Security, 2015(10), 13-20.
43. [42]. Gilad, Y., Herzberg, A., Sudkovitch, M., & Goberman, M. (2016, February). CDN-on- Demand: An affordable DDoS Defense via Untrusted Clouds. In NDSS.
44. Sahay, R., Blanc, G., Zhang, Z., & Debar, H. (2015, February). Towards autonomic DDoS mitigation using software defined networking. In SENT 2015: NDSS workshop on security of emerging networking technologies. Internet society.
45. Yu, S., Tian, Y., Guo, S., & Wu, D. O. (2013). Can we beat DDoS attacks in clouds?. IEEE Transactions on parallel and distributed systems, 25(9), 2245-2254.
46. Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D. (2003, April). Statistical approaches to DDoS attack detection and response. In Proceedings DARPA information survivability conference and exposition (Vol. 1, pp. 303-314). IEEE.
47. Yan, Q., & Yu, F. R. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 53(4), 52-59.
48. Wang, X., Chen, M., & Xing, C. (2015, August). SDSNM: A software-defined security networking mechanism to defend against DDoS attacks. In 2015 ninth international conference on frontier of computer science and technology (pp. 115-121). IEEE.
49. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Rajarajan, M., & Buyya, R. (2017). Combating DDoS attacks in the cloud: requirements, trends, and future directions. IEEE Cloud Computing, 4(1), 22-32.
50. Singh, P., Manickam, S., & Rehman, S. U. (2014, October). A survey of mitigation techniques against Economic Denial of Sustainability (EDoS) attack on cloud computing architecture. In Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization (pp. 1-4). IEEE.
51. Bhushan, K., & Gupta, B. B. (2019). Network flow analysis for detection and mitigation of Fraudulent Resource Consumption (FRC) attacks in multimedia cloud computing. Multimedia Tools and Applications, 78, 4267-4298.
52. Shah, S. Q. A., Khan, F. Z., & Ahmad, M. (2021). The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network. Computer Networks, 187, 107825.
53. Palmieri, F., Ricciardi, S., & Fiore, U. (2011, October). Evaluating network-based DoS attacks under the energy consumption perspective: new security issues in the coming green ICT area. In 2011 international conference on broadband and wireless computing, communication and applications (pp. 374-379). IEEE.
54. Hoff, C. (2008). Cloud computing security: From DDoS (distributed denial of service) to EDoS (economic denial of sustainability). Rational Survivability.

55. Baig, Z. A., Sait, S. M., & Binbeshr, F. (2016). Controlled access to cloud resources for mitigating Economic Denial of Sustainability (EDoS) attacks. Computer Networks, 97, 31-47.
56. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.
57. Grobauer, B., Walloschek, T., & Stocker, E. (2010). Understanding cloud computing vulnerabilities. IEEE Security & privacy, 9(2), 50-57.
58. Choo, K. K. R. (2010). Cloud computing: Challenges and future directions. Trends and Issues in Crime and Criminal justice, (400), 1-6.
59. Khor, S. H., & Nakao, A. (2009, June). spow: On-demand cloud-based eddos mitigation mechanism. In HotDep (Fifth Workshop on Hot Topics in System Dependability).
60. Horikawa, S. I., Furuhashi, T., & Uchikawa, Y. (1992). On fuzzy modeling using fuzzy neural networks with the back-propagation algorithm. IEEE transactions on Neural Networks, 3(5), 801-806.
61. Al-Haidari, F., Sqalli, M. H., & Salah, K. (2012, June). Enhanced EDoS-shield for mitigating EDoS attacks originating from spoofed IP addresses. In 2012 IEEE 11th international conference on trust, security and privacy in computing and communications (pp. 1167-1174). IEEE.
62. Kumar, M. N., Sujatha, P., Kalva, V., Nagori, R., Katukojwala, A. K., & Kumar, M. (2012, November). Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service. In 2012 Fourth international conference on computational intelligence and communication networks (pp. 535-539). IEEE.
63. Masood, M., Anwar, Z., Raza, S. A., & Hur, M. A. (2013, December). EDoS Armor: A cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments. In INMIC (pp. 37-42). IEEE.
64. Sqalli, M. H., Al-Haidari, F., & Salah, K. (2011, December). Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. In 2011 Fourth IEEE international conference on utility and cloud computing (pp. 49-56). IEEE.
65. Thaper, R., & Verma, A. (2015, December). Adaptive pattern attack recognition technique (APART) against EDoS attacks in cloud computing. In 2015 Third International Conference on Image Information Processing (ICIIP) (pp. 31-34). IEEE
.