Survey on DDoS and EDoS Attack in Cloud Environment

Shruti Wadhwa and Vipul Mandhar

Abstract Cloud computing is a heterogeneous distributed environment that provides resources as service through Internet. Cloud consists of various resources like network, memory, computer processing, and user applications provided to the customer on pay-per-use scale. Cloud services are broadly divided as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Therefore, data that is stored in cloud needs to be secured from the attackers as it is remotely kept. However, security is one of the major challenges in cloud. EDoS is the latest kind of DDoS attack on the cloud. The purpose is to consume cloud resources although the price of services is pay off by the valid customer. The key intention of DDoS attack brings down the specific service by draining the server's resources whereas EDoS's objective is to create economic unsustainability in the cloud resources for the object and causes financial consequences by exhausting resources and leading to a heavy bill. This paper reviews several DDoS and EDoS modification methods that have been made known in the past years and presents the mechanism which is effective for the mitigation of DDoS and EDoS attack.

Keywords DDoS · EDoS · Cloud computing

S. Wadhwa
SBBS University, Hoshiarpur, India
e-mail: shrutiwadhwa99@gmail.com

V. Mandhar (✉)
NITTTR, Chandigarh, India
e-mail: vipulmandhar130793@gmail.com

P. K. Singh et al. (eds.), *Evolving Technologies for Computing, Communication and Smart World*, Lecture Notes in Electrical Engineering 694,
https://doi.org/10.1007/978-981-15-7804-5_24

1 Introduction

1.1 Cloud Computing

Cloud computing is new IT delivery model, which enables user to store and access data according to their need irrespective of time and place. The idea behind cloud computing is reducing the workload from user's computer to cloud making use of simple Internet connection. Cloud computing and its characteristics are represented by Fig. 1. It allows IT industries to focus on doing what they actually want without spending money on infrastructure and wasting time in arranging them. It gives user the facility of pay-per-use which means provides measured services like networks, servers, storage, and applications as per their demand. Due to cloud providing features like elasticity, pay-per-use, flexibility, scalability, it earns the attraction of big organization and company for hosting their services on the cloud. By means of any latest technology trends, cloud computing is not secured from risk and susceptibilities of security.

Sabahi [1] provides the various issues of security and availability in cloud computing and suggests some obtainable solution for them. Lekkas [2] has defined the requirements of threats, and security is present at the different stages of the cloud execution. Cloud is vulnerable to various attacks being malware injection, metadata spoofing, DNS and DDoS attacks, cross-site scripting, SQL injection, and wrapping attack. And, DDoS is the common type of attack among these attacks that has been performed against cloud infrastructure. The impact of DDoS attacks becomes larger

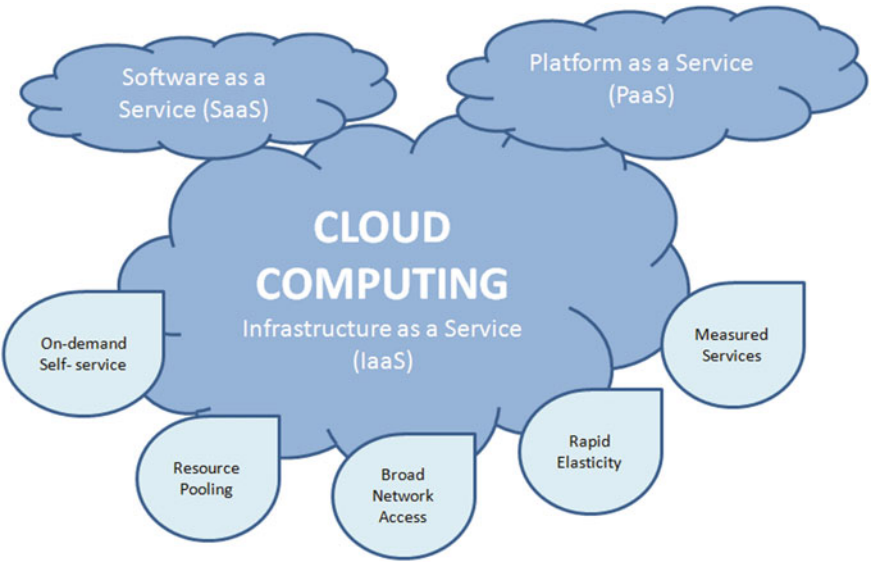

Fig. 1 Cloud computing [5]

and rigid to overlook each year. Though such attacks are rising, various industries have been tried to protect themselves with traditional firewall-based solutions. Alternatively industries had better invested in solutions that provide real protection from unprepared downtime and economic losses.

As with Incapsula Survey, key findings follow [3]:

- 49% of DDoS attacks likely to end amid 6–24 h. It means that with a projected budget of $40,000 per hour, the usual cost of DDoS can be evaluated at about approximately $500,000.
- Budgets are not only constrained to the IT group nonetheless they similarly have a huge impact on risk and security management, sales, and customer service.
- Companies having 500 or more employees are major victim of DDoS attack; experience complex attack costs and involves additional personnel to combat the attack.

Cloud computing is elastic and scalable in nature which allows resources that can be expanded whenever there is demand of more resources. A special kind of DDoS attack is specific to only cloud infrastructure. This is called economic denial of sustainability (EDoS). The main aim of EDoS is to make cloud resources carefully untenable for the victim, whereas DDoS attack focuses on worsen or block cloud services. The time period of DDoS attacks is short while EDoS attacks are more indefinable and performed over a longer time period. EDoS attack takes place just beyond the average movement threshold and beneath the threshold of DDoS attack. Hence, it is tough to be identified by customary systems of intrusion detection and furthermore the procedures practiced to overcome application layer DDoS attacks are not valid to EDoS attack [4]. In this paper, we will evaluate EDoS attacks and several practices to moderate the EDoS attacks.

1.2 Challenges and Issues in Cloud Computing

1. Privacy and Security

The key task to cloud computing is the way it addresses the privacy and security concerns of organizations rational of implementing it. The fact that the crucial enterprise information will exist outside the enterprise firewall increases severe concerns. Hacking and several attacks against cloud infrastructure will probably have an impact on many customers despite the fact that merely one site is subjected to attack.

2. Billing and Service Delivery

Because of the on-demand behavior of the services, it is relatively difficult to measure the costs incurred. Budgeting and valuation of the cost will not be very easy except if the provider proposes comparable and up right benchmarks. The service-level agreements (SLAs) of the supplier are not sufficient to assure the scalability and

accessibility. Organizations will be reluctant to shift to cloud without any surety of a high quality of service.

3. Manageability and Interoperability

Organizations must have the control of moving inside and outside of the cloud and swapping providers each time they need, and there should not be any lock-in period. The services of cloud computing should be capable of integrating easily using the on-premise IT.

4. Consistency and Accessibility

Cloud providers still fall short in providing constant service; as a result, there are repeated outages. It is essential to check the service being delivered via internal or third-party tools. It is necessary to have policies to organize usage, service-level agreements, strength performance, and corporate reliance of these services.

5. Bandwidth Cost and Performance

Enterprises can cut back hardware costs but then they need to expend further for the bandwidth. This could be a less cost for the small applications; however, it can be considerably big for the applications that are data-intensive. Appropriate bandwidth is necessary to provide concentrated and composite data across the network. Due to this reason, several organizations are waiting for a lesser cost prior to shifting to the cloud.

1.3 DDoS Attack

Distributed denial of service (DDoS) can be described as an aim to create a machine or network resources unavailable to legitimate users. This attack restrains the availability of resources. It is kind of denial-of-service (DoS) attack where numerous compromise systems usually are contaminated with viruses specially Trojan Horses which are used to aim single system. DDoS attacks are different from that of DoS attacks in such a way that DDoS encompasses multiple systems to attack victim. The widely popular DDoS attacks on Amazon, Yahoo, ebay, and numerous popular Web sites in February 2000 exposed weakness of still fine equipped network and massive Internet users. DDoS has turn out to be a main risk to the entire Internet users. There are various DDoS available tools which can be used with purpose to attack any Internet user. DDoS harms are likely to grow to be more ruthless in future in comparison to other attacks as there may be short of valuable solutions to protect these attacks. Behind major DDoS attacks are botnets and other new emerging DDoS techniques. The botnet makes use of flooding to block the availability of the resources of benign user. Among all prevailing attack weapons, flooding packets are mainly general and efficient DDoS approach. This attack is different from other attacks because it deploys its weapons in “distributed way” across the Internet. The main

aim of DDoS is to harm a victim either for individual reasons, for material gain, or to gain popularity. Enormously high-level, "user-friendly" and prevailing DDoS tool kits are accessible to attackers which rise the threat of becoming a sufferer in a DoS or a DDoS attack. The straightforward logic structures and small memory size of DDoS attacking programs make them comparatively simple to employ and hide. There are various detection and mitigation techniques available for preventing DDoS attack. One of the major challenges is the data to be protected from the attacks like DDoS. The data presently is stored in data centers of clouds. Therefore, it is very important to protect data and prevent attacks like DDoS.

DDoS can be categorized into three types [6] and represented by Fig. 2.

I. Attacks targeting network resources
II. Attacks targeting server resources
III. Attacks targeting application resources.

Attacks targeting network resources: The attacks aim for network resources making a struggle to exploit entire bandwidth of a victim's network by applying a vast size of illegal traffic to infuse the corporation's Internet pipe.

Attacks targeting server resources: The attacks aim at server resources making an effort to break down a server's processing proficiency or recollection, which possibly results in denial-of-service state. The scheme of an attacker is to take advantage of an existing exposure or a fault in a communication protocol in a way which aims the target server to turn out to be busy for executing the illegal requests so that it does not have enough resources anymore that it can handle legal request.

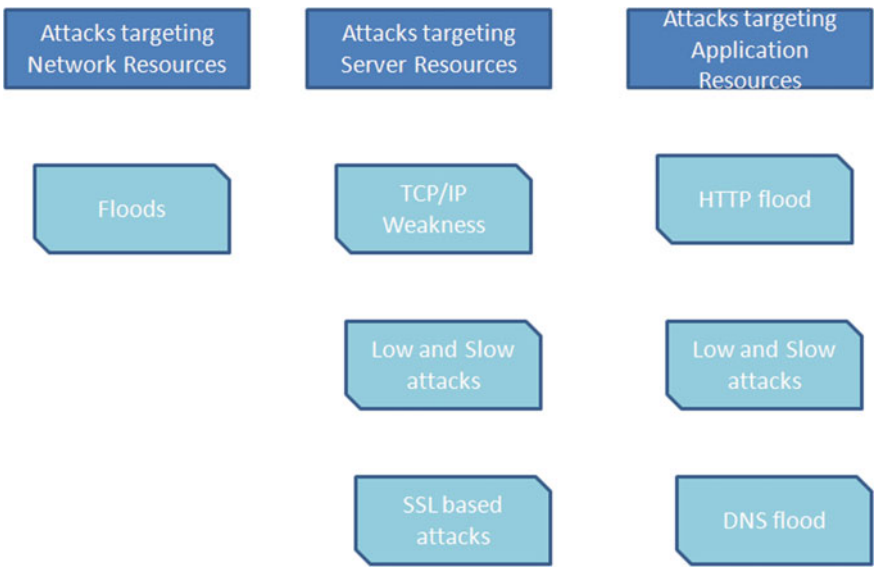

Fig. 2 DDoS attack types [7]

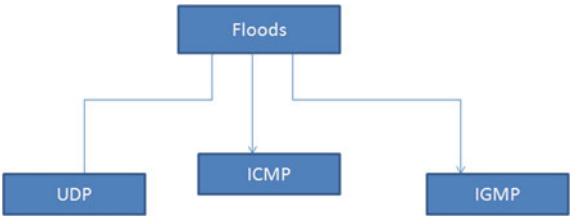

Fig. 3 Types of flood attack [7]

Attacks targeting application resources: The attacks which not only target the Hypertext Transfer Protocol (HTTP), but also other important protocols such as SMTP, HTTPS, FTP, DNS, and VOIP and also the other application protocols which acquire vulnerable weaknesses which can be used for DoS attacks.

Floods: Types of floods are represented by Fig. 3.

UDP: A User Datagram Protocol (UDP) flood attack is that which simply corrupts the normal behavior of victim at a great sufficient level which causes network congestion for the victim network instead of exploiting a specific vulnerability. Attacker sends a large number of UDP packets to random ports on a target server, and the target server is not capable that it processes each request which leads to utilization of its entire bandwidth by attempt to send ICMP "destination unreachable" as a reaction to each spoofed UDP packets to make sure that there was no listening of application on the objected ports.

ICMP Flood: An Internet Control Message Protocol (ICMP) flood is a non-defenselessness-based attack as it does not depend on some certain susceptibility to attain denial of service. An ICMP flood comprises ICMP message of echo request which is sent to the target server as quick as possible that it becomes affected to process all requests which result in a denial-of-service state.

IGMP Flood: An Internet Group Management Protocol (IGMP) deluge is also non-vulnerability-based attack. This flood attack comprises gigantic sum of IGMP message which is directed to a network or router which noticeably detains and finally blocks legal traffic from being transport over the aimed network.

TCP/IP weaknesses: TCP/IP is connection-based protocol unlike UDP and other which are connectionless protocols which means that there should be a full connection established between the packet sender and the intended recipient for sending the packets. These sorts of attacks misuse the TCP/IP procedure by compelling the use of certain of its design flaws. With the intention to dislocate the standard methods of TCP traffic, attacker misuses the TCP/IP protocol's six control bits such as URG, SYN, ACK, RST, and PSH. This is represented by Fig. 4.

TCP SYN flood: In this type of attack, the attacker approached the server in a way that server believes that they are requesting to SYN for legal connections with the help of a sequence of TCP requests with TCP flags set which is in fact appearing from spoofed IP addresses. The victim server opens threads and assigns corresponding

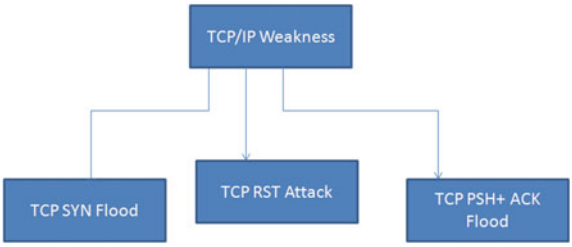

Fig. 4 Types of TCP/IP weakness [7]

buffers so that it can arrange for a connection for handling the each of the SYN requests.

TCP RST attack: In this type of attack, the attacker inhibits amid an active TCP joining among two end points by supposing the present-day system number and forging a TCP RST packet to utilize the IP of client's source which is formerly directed to the server. A botnet is classically utilized to direct thousands of such packets to the server with dissimilar series numbers, which makes it equally tranquil to estimate the exact one. As soon as this happens, the server recognizes the RST packet directed by the attacker, dismissing its association to the client positioned at the forged IP address.

TCP PSH + ACK flood: If a TCP transmitter transmits a packet whose PUSH flag is set to 1, then the outcome pressures the getting server to unoccupied its TCP stack buffer and to refer a byline when this act is comprehensive. The attacker typically uses a botnet to overflow an aimed server with various such requests. This act terminates the TCP stack buffer on the aimed server which causes the server not able to course the legal request or even acknowledge them which eventually roots the denial-of-service condition.

SSL-based attacks: As common services are moving to secure socket layer (SSL) for taming security and address privacy concerns, DDoS events on SSL are also on upswing. SSL is a technique of encryption which is used by many network communication protocols. It is used to offer safeguard to users interconnecting above former protocols by encrypting their interconnections and verifying interconnecting parties. DoS attacks based on SSL can occur in various methods such as harming definite tasks associated to the negotiation process of SSL encryption key, aiming handshake mechanism of the SSL or directing trash data to the SSL server. SSL-based DoS attacks can also be introduced above SSL-encrypted traffic which make it enormously hard to identify. SSL attacks are getting famous because every SSL handshake session utilizes 15 times more server-side resources than the user side. Hence, such attacks are uneven as it takes extensively additional resources of the server to compact with the attack than it does to introduce it.

HTTP flood: An HTTP flood is the DDoS attack which targets the application resources. Attacker exploits the seemingly legal HTTP GET or POST request for attacking the application or Web server. HTTP flood attacks are volumetric attacks

and they often use botnet for attack like attack is launched from multiple computers that constantly and repetitively request to download the site pages of the target (HTTP GET flood) which exhaust the resources of application and hence causing a denial-of-service state. They are difficult to detect as it requires less bandwidth to bring down the server than any other attacks.

DNS Flood: The Domain Name System (DNS) floods are symmetrical DDoS attack in which attacker targets one or more than one DNS server. These attacks try to exhaust server-side entity such as memory or CPU with a flood of UDP requests, generated by scripts running on several compromised botnet machines. It is based on the similar impression as former flooding attacks; a DNS flood aims the DNS application procedure by directing a large volume of DNS requests, the DNS server weighed down and incapable to respond to all of its incoming requests, therefore ultimately crashes. The DNS is the procedure utilized to resolve domain names into IP addresses and its fundamental procedure is UDP which takes the benefit of quick request and response intervals without the overhead of having to create connections.

"Low and Slow" attacks: This "low and slow" attack is more related to particularly application resources. These "low and slow" attacks can be launched from a single computer with no other bots as they are not volumetric in nature. They can target specific design flaws or vulnerabilities on a target server with a relatively small amount of malicious traffic, eventually causing it to crash. Additionally, these attacks happen on the layer of application, a TCP handshake is established by this time, effectively making the malevolent traffic appear like regular traffic traveling above a valid connection.

1.4 Economic Denial of Sustainability Attack

The general design of an EDoS attack is to make use of cloud resources without paying for it or to halt the economic drivers of using services of cloud computing. The goal of EDoS attack is to make the cloud cost model unsustainable and therefore making a company no longer capable to affordability use or pay for their cloud-based infrastructure. This is also called cloud-based denial-of-service attacks [8]. The general idea of prevention of EDoS attack is represented by Fig. 5.

Cloud computing follows the model of service where clients are charged on the basis of the practice of cloud's resources. The pricing model has altered the problem of DDoS attack in the cloud to an economic one identified as EDoS attack. The objective of an EDoS attack is to divest the consistent cloud users of their long-term financial capability. An EDoS attack becomes successful when it puts economic liability on the cloud user. For instance, attackers who pretend to be authorized users constantly make requests to a Web site hosting in cloud servers with a motive to consume bandwidth, and the burden of the bill falls on the cloud user who is the owner of the Web site. It appears to the Web server that this traffic does not extent

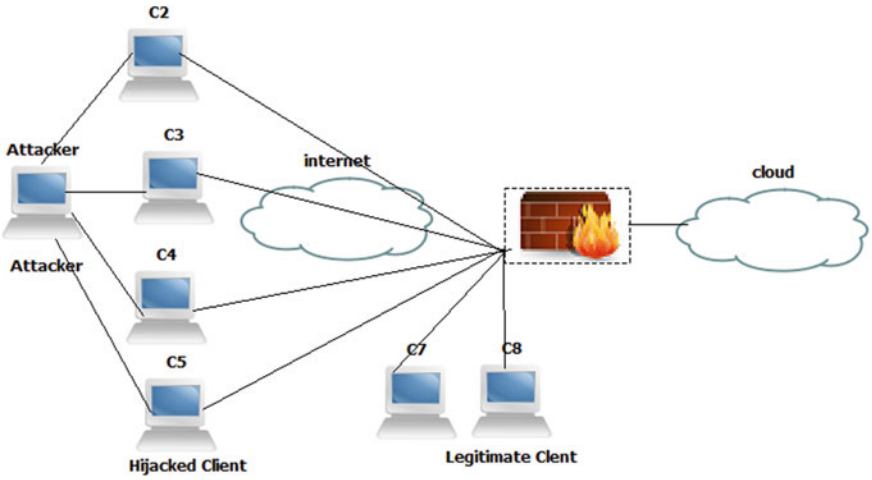

Fig. 5 Prevention of EDoS attack

the service denial level, and it is not easy to differentiate between EDoS attack traffic and legitimate traffic.

If client cloud-based service is intended to upgrade mechanically (such as Amazon EC2), now an attacker can cause financial grief by making large number of automatic requests that seem to be valid externally, however are forged in reality. Client charges will increase as you expand, consuming additional and/or bigger servers (mechanically) to respond to those forged requests. Eventually you will get to a point where your charges go beyond your capability to make payment, i.e., a point where your financial sustainability becomes uncertain.

Many organizations choose cloud infrastructure because of the following reasons:

- Business performance resourcing (compute services)
- Improve employee and partner productivity (Collaboration, QoS)
- Self service and on-demand IT service deliver
- Business Agility (adaptability, simplicity)
- Reduce/optimize cost
- Unlimited capacity (storage).

Service-level agreement (SLA) in cloud works among user and source of the service. When customer instigates request to cloud, then SLA delivers the service conferring to the anticipation of user, i.e., offers the guarantees, service duties, and warranties, and likewise lays down the accessibility and enactment of the service. Client can outspread services that he gains, at whatever stage in cloud structure because of the capability of elasticity.

The cloud service provider's quality and performance can be measured by SLAs in several ways. Certain factors that SLAs could define consist of [9]:

- Accessibility and uptime—the proportion of the time amenities will be accessible

- The amount of synchronized customers that can be assisted
- Specific standards of performance to periodically compare the actual performance
- Response time of application
- The program for notification of network changes in advance that could affect clients
- Response time of help desk for several modules of problems
- The usage statistics that will be offered.

1.5 Difference between DDoS and EDoS.

The difference between EDoS and DDoS attacks are [4].

- The objective of an EDoS is to create cost-effective unsustainability in the cloud resources for the object, while the objective of DDoS attack is to damage or block the facilities of cloud.
- DDoS attacks are capable in a short span of time, and, on the other hand, EDoS attacks are milder and completed in a stretched time span.
- EDoS attack takes place beyond the usual movement edge and beneath the edge of DDoS attack. Thus, it might not be likely to detect it by the help of customary intrusion detection system. Moreover, the approaches employed against application layer and DDoS attacks are not relevant in case of an EDoS attack.

2 DDoS Mitigation Methodology

See Tables 1 and 2.

3 EDoS Mitigation Methodology

See Table 3.

4 Conclusion

Cloud computing allows us to scale our servers up and up in order to provision greater amounts of requests for service. This unlocks a new walk of approach for attackers, known as economic denial of sustainability. DDoS is usually easy to spot given vast upsurges in traffic. EDoS attacks are not essentially easy to detect, because the arrangement and business logic are not present in most applications or masses of applications and infrastructure to provide the connection between requests and

Table 1 Security issues in cloud environment [10–13]

Security issue	Description	Related attack/intrusion/difficulty
Data security	Data stored in cloud database need to be in encrypted format and must not be accessed by other tenants	Data/information breach, unauthorized access to data
Data location	Actual geographical location of storage of data that belongs to cloud client is unknown to the cloud client	Different locations may have different laws and rules, and confliction occurs while determining ownership of the malicious data
Data segregation	Data separation needs to be maintained in host machines that are shared by various clients	Unauthorized access to data of co-resident client
Data integrity	Refers to accurate and consistent database in cloud since the access to the data can be from any device at any time	Inconsistent database
Data confidentiality	Stored data should be compliance with security and privacy policies and terms	Data/information breach
Availability	Services from cloud provider should be available to the client all the time without any downtime	Denial-of-service attacks, flood attacks
Authentication and authorization	Database of user credentials should be kept secure and user access levels must be defined and followed accurately	Insider attack, user to root attack
Privileged user access	Different levels of users require different level of access	Unauthorized user access
Regulatory compliance	To avoid legal issues, cloud user and provider should comply with terms and conditions	Difficulties in legal matters and crime investigations
Recovery and backup	Lost data must be recoverable, and backup is taken for sensitive data	Permanent data loss due to natural disaster or successful attack
Network security	Traffic flowing through network layer should be encrypted with techniques such as TLS or SSL	Packet sniffing
Web application security	Application provided by cloud must not be vulnerable to any security flaw	Service injection attack
Virtualization vulnerabilities	Multi-tenancy may cause troubles since properties of the virtual machines, like isolation, inspection, and interposition may not be followed properly	Blue Pill rootkit, SubVirt, direct kernel structure manipulation (DKSM)

(continued)

Table 1 (continued)

Security issue	Description	Related attack/intrusion/difficulty
Injection vulnerabilities	Design/architectural flaws in the application provided by cloud service may lead to injection attacks	SQL injection, OS injection, LDAP injection
Vulnerabilities in browser APIs	Poor security in handling APIs and vulnerable design of browsers may invite attackers to harm services	SSL certificate spoofing, attacks on browser caches, phishing attacks on mail clients
PaaS-related issues	PaaS providers have to take care of program codes and data related to applications that are being developed in cloud environment	Illegal data transfer, extensive black box testing, attacks on visible code or infrastructure
IaaS-related issues	IaaS provides the computing resources, like storage, RAM, processors to the clients, and security issues related with these resources affect IaaS cloud providers	Reliability of the data stored, trust issues with the provider

Table 2 Comparison of various defense mechanisms of DDoS attack [3, 14, 15]

S. No.	Security mechanism	Benefits	Limitations
1	Filtering of packets (ingress and egress) at edge router of SOURCE	It will perform detection and filtering of packets with spoofed IP addresses at the edge router of source which should be lean on the legal IP address range (used internally in the network)	Spoofed packets might not be discovered if those addresses are covered in the legal IP address range used in the internal network
2	D-WARD	It blocks the attack traffic which is initiated from a network at the boundary of the network's source	More CPU Utilization compared to others
3	MULTOPS	DDOS flooding attacks are detected as well as filtered based on the considerable differentiation between the receiver and transmitter going to and coming from a network node	For observing the packet rates of every IP address, MULTOPS uses a dynamic tree structure which will result in making this a dangerous object of a memory exhaustion attack
4	IP traceback mechanisms	Instead of spoofed IP addresses, it traceback the forged IP packets to their correct sources	These types of mechanisms have heavy computating, network or management overheads. This brings up challenges in the operations and deployments

(continued)

Table 2 (continued)

S. No.	Security mechanism	Benefits	Limitations
5	Packet filtering and marking mechanisms	It marks valid packet at every router alongside with their route to the destination thus the filtering of attack traffic is done by the victim's edge routers	The strength of the attacker is a factor to which this defense mechanism relies on. If the volume grows filters turn out to be ineffective and cannot be installed
6	Increasing backlog	Defends from overflowing a host's backlog of sockets connected	Poor solution for functions, they used linear list traversal. It tries to free the state associated with stale connections
7	SYN Cache	Secret bits in TCP header prevent an attacker from targeting a specific hash value	It is complex in nature
8	Firewalls and proxies	They have policies (inspection) for acting against SYN flooding attacks	attacks can be easily bypassed using advance mechanisms
9	IP-level defense mechanism	It is more devoted to defend SIP servers	Servers are complex to implement and work only at IP level
10	Mitigation on the page access behavior	It is helpful to avoid HTTP-GET flooding attacks	Large False positives

Table 3 Summary of EDoS mitigation techniques [16–18]

Approaches	Methodology	Distributed approach	Learning ability	Limitations
EDoS armor	Packet filtering and authentication	No	Yes	Provide defense only for E-commerce applications
EDoS shield	Virtual firewall and authentication	No	Yes	Does not deal with IP spoofing attacks
Enhanced EDoS shield	Graphical turing test and TTL	No	Yes	–
sPoW	Packet filtering, crypto-puzzle	Yes	Yes	Prevents only network-level EDoS attack

(continued)

Table 3 (continued)

Approaches	Methodology	Distributed approach	Learning ability	Limitations
Cloud traceback	Packet marking and traceback	Yes	Yes	Does not deal with IP spoofing
Cloud watch	Traffic monitoring	Yes	No	Incompetent solution counter to EDoS because user can be still charged for over exploitation of resources
In-cloud scrubber	Authentication through crypto-puzzle	No	Yes	Authentic user is reluctant to resolve such problems; thwarts merely network-level EDoS attacks
DDoS mitigation system	Graphical turing test, crypto-puzzle	No	Yes	Does not covenant with IP packet disintegration, does not covenant with dynamic IP addresses
Digital signatures	Digital signature generation and verification	Yes		Some digital signing processes can be computationally intensive, slowing down business processes and limiting their ability to scale

successful transactions. Current mitigation methodology for DDoS attack and EDoS attack that put forward to address was reviewed in this paper. Machine learning techniques are required for preventing the attack. Therefore, this paper reviews all the aspects of DDoS and EDoS attack [5, 19].

References

1. Sabahi F (2011) Cloud computing security threats and responses. In: 2011 IEEE 3rd international conference on communication software and networks (ICCSN), pp 245–249
2. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gener Comp Syst 28(3):583–592
3. Incapsula Survey, What DDos attacks really cost businesses

4. Sukhada Bhingarkar A, Deven Shah B (2015) A survey: securing cloud infrastructure against EDoS attack. In: International conference on grid & cloud computing and applications (GCA'15), pp 16–22
5. Abbasi H, Ezzati-Jivan N, Bellaiche M, Talhi C, Dagenais M (2019) Machine learning-based EDoS attack detection technique using execution trace analysis. J Hardware Syst Secur. https://doi.org/10.1007/s41635-018-0061-2
6. Rajkumar MN (2013) A survey on latest DoS attacks: classification and defense mechanisms. Int J Innov Res Comput Commun Eng 1:1847–1860
7. Egress filtering [online]. Available: www.whatis.techtarget.com/definition/egress-filtering
8. EDoS, https://www.elasticvapor.com/2009/01/cloud-attack-economic-denial-of.html
9. Bianco P, Lewis GA, Merson P (2008) Service level agreements in service—Oriented architecture environments, CMU/SEI-2008-TN-021, September 2008
10. Fernandes, Diogo AB, et al (2014) Security issues in Cloud environment: a survey. Int J Inf Secur 13(2):113–170
11. Gartner: Seven Cloud Computing Security Risks, Networkworld, [online]. Available: https://www.networkworld.com/article/2281535/data-center/gartner-seven-Cloud-computing-security-risks.htnl
12. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of Cloud computing. J Netw Comput Appl 34(1):1–11
13. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M (2013) A survey on security issues and solutions at different layers of Cloud computing. J Supercomput 63(2):561–592
14. Singh PK, Bhargava BK, Paprzycki M, Kaushal NC, Hong WC (2020) Handbook of wireless sensor networks: issues and challenges in current scenario's. In: Advances in intelligent systems and computing, vol 1132. Springer, Cham, Switzerland, pp 155–437
15. Singh PK, Kar AK, Singh Y, Kolekar MH, Tanwar S (2020) Proceedings of ICRIC 2019, Recent innovations in computing, 2020, Lecture Notes in Electrical Engineering, vol 597. Springer, Cham, Switzerland, pp 3–920.
16. Singh P, Manickam S, Rehman SUI (2014) A survey of mitigation techniques against Economic Denial of Sustainability (EDoS) attack on cloud computing architecture. In: Reliability, Infocom technologies and optimization (ICRITO) (trends and future directions), 2014. IEEE, pp 1–4.
17. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing [online]. Available: www.tools.ietf.org/html/rfc282
18. Singh P, Paprzycki M, Bhargava B, Chhabra J, Kaushal N, Kumar Y (2018) Futuristic trends in network and communication technologies. In: FTNCT 2018. Communications in computer and information science, vol 958, pp 3–509
19. Nautiyal S, Wadhwa S (2019) A comparative approach to mitigate economic denial of sustainability (EDoS) in a cloud environment. in: 2019 4th international conference on information systems and computer networks (ISCON), Mathura, India, pp 615–619. https://doi.org/10.1109/ISCON47742.2019.9036257
20. Amita (2015) EDoS-shield—a mitigation technique against EDoS attacks in cloud computing. Int J Eng Res Technol 4(05):795–797
21. Rameshbabu J, Balaji B, Daniel RW, Malathi K (2014) A prevention of DDoS attacks in cloud using NEIF techniques. Int J Sci Res Public 4(4):1–4
22. Yu S, Tian Y, Guo S, Wu DO (2014) Can we beat DDoS attacks in clouds. IEEE Trans Parallel Distrib Syst 25(9):2245–2254
23. Nam SY, Djuraev S (2014) Defending HTTP web servers against DDoS attacks through busy period-based attack flow detection. KSII Trans Internet Inf Syst 8(7):2512–2531
24. Darwish M, Ouda A, Capretz LF (2013) Cloud-based DDOS attacks and defenses. In: IEEE international conference, pp 67–71
25. Vashisht S, Kaur M (2015) Study of cloud computing environment, EDoS attack using CloudSim. Int J Adv Res Comput Sci 6(5):181–184
26. Shangytbayeva GA, Karpinski MP, Akhmetov BS (2015) Mathematical model of system of protection of computer networks against attacks DOS/DDOS. Mod Appl Sci 9(8)

27. Strom S (2015) Global information assurance certification paper. As part of GIAC practical repository, December 2015
28. CloudComputing, https://www.google.co.in/search?q=cloud+computing&biw=1366&bih=613&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwiI1IKsyb7RAhUhDcAKHWTEChAQ_AUIBygC#imgrc=sOyFCX-Gf5M08M%3A. Accessed on 25 July 2016
29. Ingress filtering [online]. Available: www.whatis.techtarget.com/definition/ingress-filtering
30. Poongodi M, Hamdi M, Sharma A, Ma M, Singh PK (2019) DDoS detection mechanism using trust-based evaluation system in VANET. IEEE Access 7:183532–183544. https://doi.org/10.1109/ACCESS.2019.2960367