Journal of Theoretical and Applied Information Technology
28th February 2022. Vol.100. No 4
2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DISTRIBUTED DENIAL OF SERVICES ATTACKS AND THEIR PREVENTION IN CLOUD SERVICES

[1]SARAH NAIEM, [1]MOHAMED MARIE , [2]AYMAN E. KHEDR, [2]AMIRA M. IDREES

[1]Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt

[2]Faculty of Computers and Information Technology, Future University in Egypt, Cairo, Egypt

Email: SarahNaiem@fci.helwan.edu.eg, dr.mmariem@fci.helwan.edu.eg, ayman.khedr@fue.edu.eg, amira.mohamed@fue.edu.eg

ABSTRACT

Distributed Denial of services (DDOS) attacks are one of the most famous attacks that affect the availability of a service making it a serious problem especially when it comes to cloud computing as it is becoming a bigger part of our lives. Throughout this paper, we first discussed the DDOS types, categories, and approaches in terms of the targeted area of the cloud or the intensity of the attacks whether it's the normal DDOS, the Low-rate DDOS, or Economic-DOS (EDOS). We then presented a comparative analysis between the recent studies discussing the DDOS attacks in cloud. Prevention of DDOS in cloud computing is the first step in the defense mechanism followed by detection and mitigation. The prevention of the DDOS attacks is the foremost important step in protecting the cloud from DDOS which is achieved through challenge-response, hidden servers, and restrictive access approaches. We also provided a summary of the recent studies discussing the different prevention techniques, approaches, and frameworks. The main purpose of this paper is to provide a road map of the current situation of DDOS attacks and how they take place, why they take place and its prevention techniques in cloud computing environment focusing on the true protective prevention stage.

Keywords: *Cloud Computing, Security, DDOS attacks, Low rate DDOS, DDOS prevention*

1. INTRODUCTION

Cloud computing has been widely used over the past decade as it offers lots of services including education [1,2,3], recommendations [4,5], networking, storage, security, flexibility, self-services, elasticity and migration flexibility. The cloud is based on the concept of distribution on virtual machines (VM) dynamically tailored to meet the needs of an organization based on the service level agreement between the cloud and the organization. [4][5]

Alongside to the advantages and services provided by any cloud model comes a lot of security issues as the user's information is exposed. The user of the cloud will be trusting the cloud Service Provider (CSP) in terms of security and privacy of their data and information. The CSP should offer its users the utter most trust they can for them to use their services. Whereas a user can only give this trust if all the security and risk areas is assured including data security, VM security, and other areas. Confidentiality, integrity, and availability, computational security, secure virtualization and threats in service delivery are the concerns for the cloud user. Data confidentiality results from inadequate data deletion by the CSP as the undeleted data will be exposed, unauthorized access to data, and the failure to encrypt the confidential data of the user. While Data integrity is affected by SQL injection, cross scripting metadata spoofing, wrapping attack, virtual machine. Availability of data on cloud is one of the most important factors when it comes to data cloud security. Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks are two of the main threats affecting the availability of data. [6]Where DDOS is an attack where the attacker creates many bots to attack the server instead of using one machine to attack and deny the service of the target from it's users. [6][7]

Even though the focus of this survey is to study the different types of DDOS in cloud computing and

how to prevent them we need to understand how this attack takes place in a cloud environment, the different impacts it cause as a result, and study the different types and classifications of DDOS in cloud. A very important step in our study is to under stand the motive behind these attacks in order to understand what are we fighting against. Several authors discussed this matter and highlighted that this act of felony could be for a criminal benefit, the attacker could be targeting money as extortion, taking revenge, a competitor is trying to destroy the other party, or basically just because the attackers is trying to get a sense of achievement or trying new tools. Regardless of the actual reason behind the attack it still causes a huge amount of damage for the parties being involved and the magnitude of the damage could be highly destructive [8][9].

Throughout the paper the impact of DDOS in cloud computing is first discussed, following that we discussed the different techniques and approach of DDOS and their prevention. The following flowchart shows how the rest of the paper is constructed.

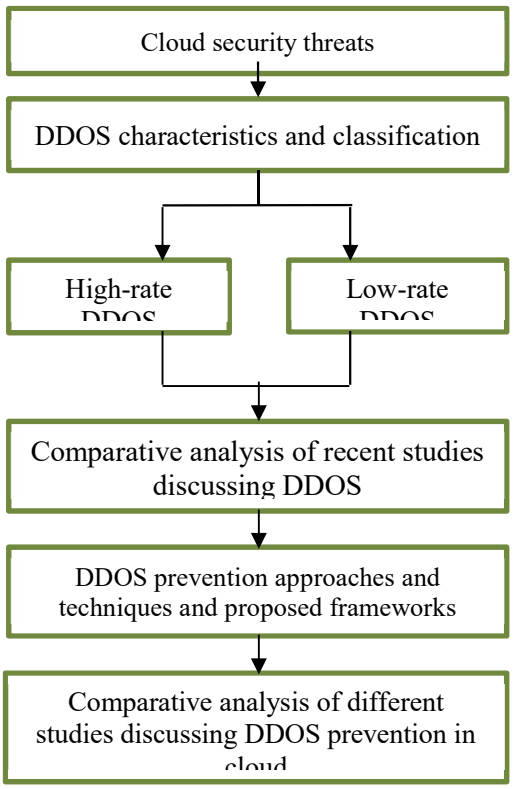

Figure 1 research methodology

2. BACKGROUND

There are three types of service models that are offered by the cloud including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS offers the user access to application services tailored to their needs, PaaS offers a podium for the user to develop, run and administer their own applications on cloud without worrying about the storage or groundwork. As for the IaaS the cloud provides the user with computing facilities like storage, network, servers, data backups, and security and processing power to run their own systems. [10] The cloud offers its services in deployment methods including private, public, hybrid and community.

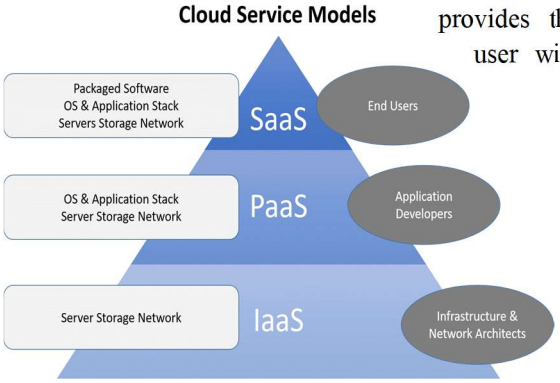

Figure 2 Cloud services models [10]

Security issues must be handled to assure secure authentication, assigned authorization, and key management for encoded data and the client must be aware of all the security threats they might be facing. According to Yadav and Sharma [10]the real security threat is that the data gets subjected to changes intentionally or not, or can get lost during the backing up and updates. There were two solutions for this issue, Provable Data Possession (PDP) and Proof or Retrieve-ability (POR). The PDP is a model for remotely inspecting the data integrity using a hash value and a key while POR works on restraining the capacity in the client serve side. As for data confidentiality the most important thing is to encrypt the data in order to handle and protect delicate data before sending them to the cloud. They concluded their work by stating that security issues must be handled to assure secure authentication, assigned authorization, and key management for encoded data and the client must be aware of all the

security threats that they might be facing. [10]

Each part of the cloud infrastructure executes different processes and provides different services leading to several security issues The security concerns in cloud include data transmission, virtual machine security, network security, data privacy, data integrity, data availability, and security policy and compliances. The Service level agreements (SLA's), cloud data management and security, interoperability, and platform management are some of the most challenging issues when in cloud computing. Managing cloud data security issues is very important given the massive size of unstructured data. The cloud providers need to depend on the infrastructure provided in order to accomplish full data security as they don't have access to the physical security systems, and it's important to create a trust mechanism at all the layers of the cloud. [11]

*S*ecurity threats in cloud might also include compromised credential where threats like Data breaches and permanent data loss vary in their complication and effect according to the the sensitivity of the data being breached or lost due to deletion or failure in appropriate backing up and data retrieval. DOS affect the data availability and the best way to handle this attack is to have prevention and detection plans as it results in huge cost and effect on the future of a business with the client [12]. Other different attacks in cloud computing including Denial of service (DOS), side channel, authentication and man in the middle cryptographic attacks also affect the cloud environment and it might actually be helpless against them as the cloud is used by many different users [13].

3. DISTRIBUTED DOS REVIEW: CHARACTERISTICS AND CLASSIFICATIONS

3.1. DDOS Types and characteristics

DDOS attacks has many different forms and strategies that have been studied in several researches but its categorized generally into Semantic and brute- force attacks [14]. Semantic attacks target the limitations in the cloud serves by creating low spiteful traffic targeting the victim's protocol or service which is also known as low-rate DDOS attacks. The traffic used by attackers in this type is very similar to the normal traffic making it difficult to identify and it includes shrew, reduction of quality, economic denial of sustainability, and low rate DDOS attacks against application server affecting the quality of the service being provided. On the other hand, the traffic of the requests sent by the attacker in brute-force attacks is significantly large with the purpose of overwhelming the victim with requests, it's also known as flooding or high-rate DDOS attacks[15][16]. The high rate DDOS attacks works by interrupting the cloud service through exhausting either the network's or resource's bandwidth capacity and is divided into either application level flood attack or network level flood attack [14].

In another study DDOS attacks has been categorized into attacks targeting the network resource, server resource, and application resource. The attackers aim when targeting the network resource is fighting for the whole bandwidth of the network through applying huge amount of false traffic using different types of flooding attacks including User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and Internet Group Message Protocol (IGMP). As for the server's resources the aim is breaking down the server's availability leading to unavailability of services through SSL based attacks, where the attacker obstructs an active TCP and forges a similar packet, sends it to the serve to exploit its weaknesses. As for the attacks targeting the application resources the aim of the assaulter is to attack the protocols used like HTTP, Simple Mail Transfer Protocol (SMTP), HTTPS, FirePower Threat Defense (FTD), Domain Name system (DNS) and these types of attacks include HTTP flooding attacks, Low and Slow attacks, and DNS floods. [17].

Classification of DDOS in cloud has been also studied by Kesavamoorthy et al. [18] where they focused on its impact on cloud, solutions, prevention and detection methods and highlighted that the availability of a service or application is one of the key factors of its reliability and DDOS attacks prevents this from happening. They classified DDOS based on its impact either through bandwidth or resource depletion, flow whether constant or varying bit rate, mode being either direct or indirect attack, and finally deployment method either flooding or

non-flooding. They focused on flooding attacks where it has been further classified into three different levels including Network/transport level, Application level, or based on Botnets. The flooding attacks against the Network/transport level include normal flooding, protocol exploitation flooding, amplification based flooding, and reflection based flooding. While the flooding attacks against the application layer included HTTP flooding. Last but not least are the flooding based on botnets attack including Internet Relay Chat (IRC) and web based botnets [18].

Bhardway et, al. [19] studied the impact of DDOS on cloud, solutions, prevention and detection methods. They Categorized the DDOS attacks on cloud into three categories including the attacks on the infrastructure of the cloud, on the services of the cloud, and on the customer using the cloud service. They discussed the different attacks which we illustrated and summarized in figure 3 and how they work [19].

Dong et al. [20]surveyed DDOS and its impact on cloud computing and software defined networked where they further classified it into flooding attacks, amplification attacks, Local area network denial (Land) attacks, Transfer Control Protocol Synchronize (TCP SYN attacks), Common Gateway Interface(CGI) request attacks, and authentication server attacks. The flooding attacks includes User Diagram Protocol (UDP), HTTP, ICMP, and SIP/Message Tampering attacks. Flooding attacks are defined as the type of attacks that overloads the target resulting in huge traffic on the IP. While amplification attacks uses a broadcast IP address to transfer messages which forces all the nodes of the network to handle the attack without knowing that its being a victim and it includes smurf, fraggle, and Simple Network Management Protocol (SNMP) attacks. While the Land attacks uses high traffic to sends corrupt pockets to the target terminating the legal functions resulting in denial of the original serves. However, the TCP SYN attacks is overloading the target by exploiting their TCP/IP through SYN requests, and the CGI request attack is resulting in failure at the victim's side to take requests resulting from the large amount of CGI request that consumes the CPU of the victim. Last but not least is the Authentication server attacks the attacker sends a fake signatures that results in a large amount of the resources of the attacked party being consume Highlight that prevention shouldn't be a middle phase d in identifying these fake signatures[20].

Shaar et al. [21] in their study discussed DDOS attacks, its taxonomy, and different cloud components that could be targeted by the attacker including attacks on VM, cloud scheduler, hypervisor, the web server, the cloud consumer, IaaS, and SaaS. DDOS on VM like Cloud Internal DOS attacks (CIDos), VM mitigation, neighbor, VM escape, VM sprawing attacks are very dangerous as the attacker might abuse the features of the VM as using the migration qualities and affecting the service provider's performance. Attacks on the hypervisor like Mimicking DDOS attacks work by tricking the cloud user into using a VM that has been infected by a malicious OS. While attacks on the Cloud's customer results in economic losses where the attacker over loads the service provider with requests leading the provider to use the scalability feature and add resources to fulfill the need. Attacks on the IaaS are energy oriented DOS exhausting the infrastructure of the cloud while the attacks on the SAAS are application based DOS working by rejecting the requests of the victim to use the applications provided. Finally, are the DDOS attacks on the web services and through their study they stated almost 17 type of DDOS that can take place when it comes to the attacks on services of the cloud. The aspect being targeted is the Extensible Markup Language XML that is used to encrypt the data being transmitted between the devices using the service. These types of DDOS attacks include Coercive parsing attacks, XML element and/or attribute count attack, Simple Object Access Protocol (SOAP) array attacks , Hash collision attacks which is also known as hash DOS, Business Process Execution Language (BPEL) state deviation attacks, Attack obfuscation, metadata spoofing attacks, Web service Description Language (WSDL) attacks, oversized cryptography attacks, XML external entity attacks, XML entity expansion attacks, HX-DOS attacks, Middleware hijacking attacks, XML-based DOS attacks, address spoofing attacks, Indirect flooding attacks, and Instantiation flooding attacks. [21].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Low-rate Distributed Denial of services

Low-rate DDOS (LDDOS) has been proven to be harder to detect than traditional flooding DDOS, where the attackers changes the dynamics of the attack to a small amount of traffic not higher that 20% of the network's original traffic making it even harder to identify [22].

Zhijun et al. [22]categorized DDOS into high-rate, low-rate attacks, and shrew attacks which are based on low rate attacks and highlighted that the success rate of the LDOS over traditional flooding DDOS is distinguishingly higher and has caused lots of damage to popular websites like CNN, eBay, Yahoo!, Dell, and more. LDDOS main characteristics include Reduce of quality (RoQ), Concealment, and pulsing which are the main reason for the difficulties faced detecting them. RoQ results due to the utilization of the fluctuation mechanism of the TCP/IP protocol, the concealment is camouflaging the original traffic making it seem legit and hard to detect, and pulsing where the attacks are simple from a singular source with a very low rate. The authors classified the LRDOS into three main types including attacks against the security vulnerabilities, organization, and scenarioThe attacks agains the security are vulnerabilities either on the transmission layer, network layer, and/or application layer while the attacks against the orginazitation include single attack source, distributed aggregation attack, and synchronous and asynchronous attack and lastly the actual scenario attacks happens at the networkareas including terminal system, network node or border routers [22].

According to Agrawal and Tapaswi [16] LDDOS is categorized into shrew, RoQ, "Low-rate DDOS against application" (LORDAS), and "Economic Denial of Sustainability" (EDOS) attacks where each has a different approach based on the attack's period of time, rate, and length. Shrew attack's aim is to stop the rightful flow in the TCP of the cloud using low rate traffic interrupting the cloud services based on the periodically scheduling of the sent attacks against the TCP [21]. While the ROQ attacks are still based on the time parameter of the attack's flow it targets the weakness in the TCP to disturb the quality of service received by the rightful users. As for the LORDAS attack it targets the application server by sending harmful request to jam the queue of the server preventing the rightful request from working. The last type of the low rate attacks they discussed is the EDOS which plays on affecting the financial aspect in the cloud's provider. Since the cloud services usually are automatically dynamically scaled up or down based on the user's needs the attacker creates the need for adding VM's that the cloud server provider doesn't need and would cost him a lot of money resulting in unmaintainable services [24][25][16].

After we studied the current situation of DDOS attacks in cloud we provided a comparative analysis in TABLE 1 showing how DDOS is discussed and categorized in terms of attacked area in cloud including cloud's services, resources, and applications and its types including high-rate, low-rate, and EDOS.

4. PREVENTION OF DDOS IN CLOUD COMPUTING

DDOS in cloud computing is a huge problem that needs to be handled and managed through specific prevention, detection, and mitigation approaches. This section of the paper will discuss and clarify the recent prevention approaches. Where the prevention of the occurrence of an attack is the first step and is considered a protection act to stop them from happening or even reducing them[9][16].

Prevention of DDOS in cloud according to Agrawal and Tapaswi [16]is considered precaution from the attack before it takes place where they categorized the prevention of high-rate DDOS into resilient scheduling, network traffic management and hidden servers. Resilient scheduling works by assigning an unceasing value to every session that is then exploited through the resilient scheduler to choose which sessions will get scheduled and when; unfortunately, the performance is disturbed when used on huge scale cloud system. Network Traffic management is based on allocating the bandwidth to different clusters using traffic shaping techniques which affects the auto-scalability feature of cloud. Hidden servers works by balancing the capacity of the traffic on the cloud and monitoring it through adding a node that acts like a forwarding authority protecting the cloud but scalability, shuffling, and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

problems arising from the introduction of more than one proxy are issues that need to be handled [16].

In another study[9], the authors mentioned that prevention is an upbeat approach to stop not handling the consequences. The approaches discussed included Moving Target Defense (MTD), Completely Automated Public Turing test (CAPTCHA), EDOS-Shield Mitigation, Resource quota, and self-verifying Proof of Work (sPOW). MTD works by introducing a dynamic surface for the attack through proxies with changing locations making it harder for the attacker. While the CAPTCHA is based on challenge response technique for the authentication of user identifying whether the user is legit or a bot, the idea is creating a CAPTCHA that is hard enough to prevent bots but not hard for legit users. However, EDOS-Shield mitigation works by creating a blacklist including IPs of unknown sources through turing tests but unfortunately legit users might affected and denied access to the cloud. The sPow uses the same concept of blacklisting the unknown IPs and denying them access and resource quota approach handles EDOS attacks by limiting the quota of the resources yet it might lead the cloud services to slowdown or even stop [9].

Potluri [26]discussed different prevention tactics including machine learning, neural network classifiers, SDN, genetic algorithms, and block-chain. All of these schemes are based on the same concept of monitoring the traffic, diverting and evaluating it using different techniques. The Machine learning is used by applying the C.4.5 algorithm using signature based technique to creates a decision tree working on automatic identification of the false traffic. The Neural network classifier method has a high rate of success with a lowermost rate of false detections based on "Neyman Pearson cost minimization" strategy and "Resilient Back Propagation" on different datasets where the classifier checks whether the traffic is an attack or not and acts accordingly. The SDN tactic is one of the best solutions for the prevention of DDOS as it uses the SDN prevention architecture and traffic analysis techniques where the packets received are analyzed and properly handled. While Genetic Algorithm prevention is based on extraction and feature section methods and SVM is used to classify the packets. Blockchain prevention uses hash values to read and write IP addresses to easily identify the harmful traffic from the legit ones [26].

Srinivasan et, al [27] also discussed prevention of DDOS and mentioned Challenge/Response protocol, hidden servers, and Restrictive source access approach in terms of technique difficulty, disadvantages and limitations. Challenge/Response protocol uses puzzles that can successfully identify bots in the traffic but it requires further storage for the huge amount of generated graphics and puzzles, images might accumulate, and it might face parsing and dictionary attacks. While the Hidden server helps legit clients to access the services provided without any direct connection with the server at the beginning but it requires an extra layer of security for redirection and extra server ports. Restrictive source access offers efficient control over the admission and organizes the process of dropping traffic across different classes but the main challenge of this approach is its effect on the quality of service provided to the legit users but it doesn't work well with large amount of traffic from different bots that might be spoofing the network [27].

Harale and Thakare [28] in their study reviewed five efficient techniques for handling TCP floods which are also known as CS_DDOS attacks in cloud which is the second most occurring type of attacks following information theft in cybercrimes. The techniques they reviewed included CS_DDOS systems, TCP-based DDOS detection systems, Hypervisor-based detection system, Virtualization techniques, and System of System (SoS). The CS_DDOS system is composed of detection and prevention, where the detection system gathers packets in a timely matter and compare them to the blacklisted attackers of the system and accordingly passes or sends it to the prevention system. While the TCP-based DDOS detection system is composed of data collection, sample generation and feature selection, classification, and attack alarm. The Hypervisor-based consists of a "Trust Model" used to help distinguishing the trustworthy resources. However, the Virtualization techniques included Para-virtualization, Hardware VM and container virtualization but the efficiency of these systems is affect by the DDOS attack even if it was a light attack. Finally, the SoS which uses mediators for observing the system and helps in having good QoS.

They proposed a methodology based on the CS_DDOS system which included both detection and prevention and used the Least Squares Support Vector Machine (LS_SVM) in the classification which helped providing more precise attack identification[28].

An innovative framework was proposed by Saravanan et,al. [29] in their study but they first discussed the problems that arise from the use of different prevention techniques then proposed a new concept. The idea of the new concept they introduced is that it is implemented instead of the CAPTCHA or reCAPTCHA method for identifying legit traffic from bots and harmful floods which is categorized as a challenge response prevention technique. The idea of CAPTCHA is based on "Graphical Turing Test" which is considered one of the main techniques used in challenge response including also text puzzles, graphical tests, and Crypto puzzles [33] to prevent machines from acting like humans and gaining unauthorized access. The problem with this approach as mentioned by the authors is that it could lead lead to puzzle building up and might also lead to extra image overhead leading to late response or even failure and blockage of the system. The proposed prevention technique is based on Visual Comprehension "VISUALCOM", Image Completion "IMGCOM", and Image Completion Anomaly detection "AD-IMGCOM". The first approach which is Visual comprehension works through provoking the user to answer questions as a response founded on a displayed image which helps with reduction of the storage space that results from the use of other turing test techniques [30]. The second approach proposed is said to be a little bit more complicated than the first one as it takes one picture and partitions it into several parts and as a challenge for the user he is supposed to drag the image partitions and drop them to create the whole complete image exactly the same concept of the actual puzzles which still uses only one image but is a bit harder for the users which makes it hard for bots. The third proposed approach is similar to the second one but more challenging as it adds some irregularities to the image that the user has to identify and ignore when constructing the image which makes AD-IMGCOM even harder than IMGCOM for bots. The functioning of the proposed methods has been evaluated in terms of performance time and success rate and it was proven that its better than other challenge response techniques increase the success rate and performance. [30]

Saharan and Gupta [31] surveyed the prevention techniques for DDOS and categorized it into three different approaches not technical approaches but conceptual ones. The approaches they discussed included early detection, Reactive techniques and proactive techniques and they highlighted that the prevention of actual instance of an attack is considered a proactive approach. Proactive prevention approach means trying to prevent the attack before it happens and they included in their study two approaches either ideal prevention or true prevention. The ideal prevention is the actual prevention of the broadcast based and signature based DDOS attacks while the True prevention is based on the idea of securing the network itself and making it independent. After that they mentioned some of the techniques being used for prevention which included figure printing, packet authentication, dynamic Path identifiers (DPI), prevention and trace back, and Source Address Validity Enforcement(SAVE). Even though the authors categorized the prevention approaches and discussed the current techniques, unfortunately they didn't relate the studied techniques they covered to the approaches discussed which could have added a huge dimension to their work. [31]

A new DDOS prevention and detection scheme has been introduced by Ali and Osman [32] which consists of 5 stages include Blacklist, Hash Message Authentication Code (HMAC), correlation based sequential backward selection, mutual information with recursive elimination, and last stage is the detection level. The black list and the HMAC stages of the scheme are the preventions part and the second two stages are the stages leading to the final stage which is the detection of the DDOS attack. The blacklist stage is where the packets sent to the cloud are compared to the list IPs saved in the list and if its part of the list then the sender is denied access to the cloud as its considered an attack. The second stage uses HMAC to authenticate the packet through A-256 algorithms and if the packet is successfully authenticated is then passed to the third stage which helps in the detection of the DDOS. Following that the the best classification feature is selected to help classify the packets and then its passed to the final stage of their scheme which is the detection stage where its based on "Fuzzy logic" for the packet classification and Support Vector Machine Neural networks (SVM-NN). The authors did not mention that the success rate of the prevention stage of their scheme even though they tested the detection stage using different techniques for the SVM different kernels and parameters [32].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

After studying the most recent different surveys and techniques for the prevention of DDOS in cloud computing we constructed Table 2 to provide a comparative analysis of the current situation which is displayed at the end of the article. It has been clear enough through our study that most of the conducted researches and studies don't address the prevention of DDOS in terms of the specific techniques associated to prevention which include challenge response, captcha, restrictive access , or hidden server techniques. They focus on prevention of DDOS as part of its detection based on other techniques including machine learning, anomaly, entropy or statistical based techniques. Prevention is a standalone process and yet its still considered part of the detection process but its based on different techniques.

5. CONCLUSION AND FUTURE WORK

DDOS attacks are increasing progressively and affecting the availability of services for legit users in cloud computing which affects it's reliability. Throughout our survey on DDOS and its prevention techniques the different types of DDOS attacks were studied in terms of behavior, flow and targeted area in the cloud.This survey paper only discussed the previous categorizations and only covered the prevention techniques of DDOS attacks , we believe that for a more detailed understanding of the topic the detection and mitigation frameworks should be understood along side with the different mechanisms used for protection against this attack. In addition to that we believe that even though this topic is vigorously discussed in many researches due to its high impact on the cloud's security there should be a clearer and standard way to classify these attacks instead of it being discussed from different aspect. It has been deducted from the previous research that DDOS could be classified into semantic attacks and brute force attacks. Semantic attacks target the limitations in the cloud's protocol or services through low traffic attacks which is also known as Low rate DDOS (LDDOS). While brute-force attacks which are also known as high-rate or flooding attacks are based on over loading the cloud by sending large amount of requests to prevent the rightful users from getting their services through consumption of the bandwidth. After discussing the different techniques, approaches, and classifications of DDOS in cloud we conducted a comparative analysis of different studies in terms of cloud's targeted area and the type of attack. Following that we studied the recent prevention techniques including challenge response , hidden servers, restrictive access that are used as part of the defense mechanism against DDOS in cloud which includes prevention, detection, and mitigation and also a comparative analysis of the current situation was displayed along with different prevention proposed frameworks. According to our findings the behavior of the DDOS whether high-rate or low-rate and the targeted aspect of the cloud should be taken into consideration when defending the cloud environment against them. In addition to that we also found out that there is a misperception between the prevention layer that is the proactive layer before the detection layer and the prevention techniques that are part of the detection layer which are achieved through intrusion prevention

REFERENCES

[1] *Khedr, A. E., & Idrees, A. M. (2017). Adapting Load Balancing Techniques for Improving the Performance of e-Learning Educational Process. Journal of Computers, 12(3), 250-257.*

[2] *Khedr, A. E., & Idrees, A. M. (2017). Enhanced e-Learning System for e-Courses Based on Cloud Computing. Journal of Computers, 12(1).*

[3] *Sultan, N., Khedr, A. E., Idrees, A. M., & Kholeif, S. (2017). Data Mining Approach for Detecting Key Performance Indicators. Journal of Artificial Intelligence, 10(2), 59-65.*

[4] *Al Mazroi, A., Khedr, A. E., & Idrees, A. M. (2021). A Proposed Customer Relationship Framework based on Information Retrieval. Expert Systems With Applications, 176.*

[5] *Khedr, A. E., Idrees, A. M., Hegazy, A.-F., & El-Shewy, S. (2017). A proposed configurable approach for recommendation systems via data mining techniques. Enterprise Information Systems.*

[6] *J. Mirkovic, A. Hussain, S. Fahmy, P. Reiher, and R.K. Thomas, "Accurately measuring denial of service in simulation and testbed ex-periments," IEEE Transactions on Dependable and Secure Computing, vol. 6, no. 2, pp. 81-95, April*

[7] *G. Somani, M.S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, vol. 107, pp. 30-48, July 2017.*

[8] *Abusaimeh, H. (2020). Distributed denial of service attacks in cloud computing. International Journal of Advanced Computer Science and Applications, 11(6), 163–168.*

[9] *Bakr, A., Abd El-Aziz, A. A., & Hefny, H. A. (2019). A survey on mitigation techniques against ddos attacks on cloud computing architecture. International Journal of Advanced Science and Technology, 28(12), 187–200.*

[10] *Yadav, R., & Sharma, A. (2018). A Critical Review of Data Security in Cloud Computing Infrastructure. Conference on Cyber Security (ICCS 2018) (p. 6). International Journal of Advanced Studies Of Scientific Research (IJASSR)*

[11] *Ahmed, A. A., & Hussan, T. (2018). Cloud Computing: Study Of Security Issues And Research Challenges. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) , 7 (4), 8*

[12] *Jathanna, R., Jagli, D.(2017).* ***Cloud Computing and Security Issues,*** *International Journal of Engineering Research and Applications 07(06), 31-38.*

[13] *Saxena, N. (january 2018). Enhanced Cloud Security Novel Technique to Detect and Isolate Zombie Attacks in Cloud Enviroment. Jour of Adv Research in Dynamical & Control Systems, 10.*

[14] *N. Agrawal and S. Tapaswi. "A Lightweight Approach to Detect the Low/High Rate IP Spoofed Cloud DDoS Attacks," in Proc. 7th IEEE International Symposium on Cloud and Service Computing (SC2), Kanazawa, Japan, 22-25 Nov. 2017, pp. 118-123.*

[15] *A. Praseed and P.S. Thilagam, "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 661-685, First Quarter 2019.*

[16] *Agrawal, N., & Tapaswi, S. (2019). Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. IEEE Communications Surveys and Tutorials, 21(4), 3769–3795.*

[17] *Wadhwa, S., & Mandhar, V. (2021). Survey on DDoS and EDoS Attack in Cloud Environment. In P. K. Singh, M. H. Kolekar, R. K. Bhatnagar, A. Noor, S. Tanwar, S. Khanna, & S. N. Ltd. (Ed.), Springer Nature Singapore Pte Ltd.Advances in Intelligent Systems and Computing Proceedings of Intelligent System Design: INDIA 2019. In Advances in Intelligent Systems and Computing: Vol. 194 AISC (Issue 1171)*

[18] *Kesavamoorthy, R., Alaguvathana, P., Suganya, R., & Vigneshwaran, P. (2020). Classification of DDoS attacks – A survey. Test Engineering and Management, 83(May), 12926–12932.*

[19] *Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review, 39.*

[20] *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.*

[21] *Shaar, F., & Efe, A. (2018). DDoS Attacks and Impacts on Various Cloud Computing Components. 7(1).*

[22] *Zhijun, W., Wenjing, L., Liang, L., & Meng, Y. (2020). Low-Rate DoS Attacks, Detection, Defense, and Challenges: A Survey. IEEE Access, 8, 43920–43943. https://doi.org/10.1109/ACCESS.2020.2976609*

[23] *J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for Low-Rate Shrew DDoS," IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1069-1083, July 2014.*

[24] *M.Guirguis,"Reduction-of-qualityattacksonadaptationmechanisms," Boston University, 2007.*

[25] *Z.A. Baig, S.M. Sait, and F. Binbeshr, "Controlled access to cloud resources for mitigating Economic Denial of Sustainability (EDoS) attacks," Computer Networks, vol. 97, pp. 31-47, March 2016*

[26] *Potluri, S. (2020). Detection and Prevention Mechanisms for DDoS Attack in Cloud Computing Environment. 1–6.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[27] *Srinivasan, K., & Mubarakali, A. (2020). A Survey on the Impact of DDoS Attacks in Cloud Computing : Prevention , Detection and Mitigation Techniques (Vol. 2). Springer International Publishing.*

[28] *Harale, A., & Thakare, V. (2019). Critical Analysis of various techniques of DDOS attack and formation to efficient techniques. International Journal of Management, Technology And Engineering , IX (I), 35-40.*

[29] *A.Saravanan, S. SathyaBama, S. Kadry, L. R. Ramasamy (2019) Journal, I., & Engineering, C. (n.d.). A new framework to alleviate DDoS vulnerabilities in cloud computing.*

[30] *C. S. Dule and Girijamma H. A., "Content an Insight to Security Paradigm for BigData on Cloud: Current Trend and Research," International Journal of Electrical and Computer Engineering (IJECE), vol/issue: 7(5), pp. 2873-2882, 2017.*

[31] *Saharan, S., & Gupta, V. (2021). DDoS Prevention: Review and Issues. Springer NAture Singapore , 567-574.*

[32] *A Ali, A. A., & Aldeen Osman, S. F. (2018). International Journal of Computer Science and Mobile Computing Efficient DDoS Attack Detection and Prevention Framework Using Two-Level Classification in Cloud Environment. International Journal of Computer Science and Mobile Computing, 7(8), 1–7. www.ijcsmc.com*

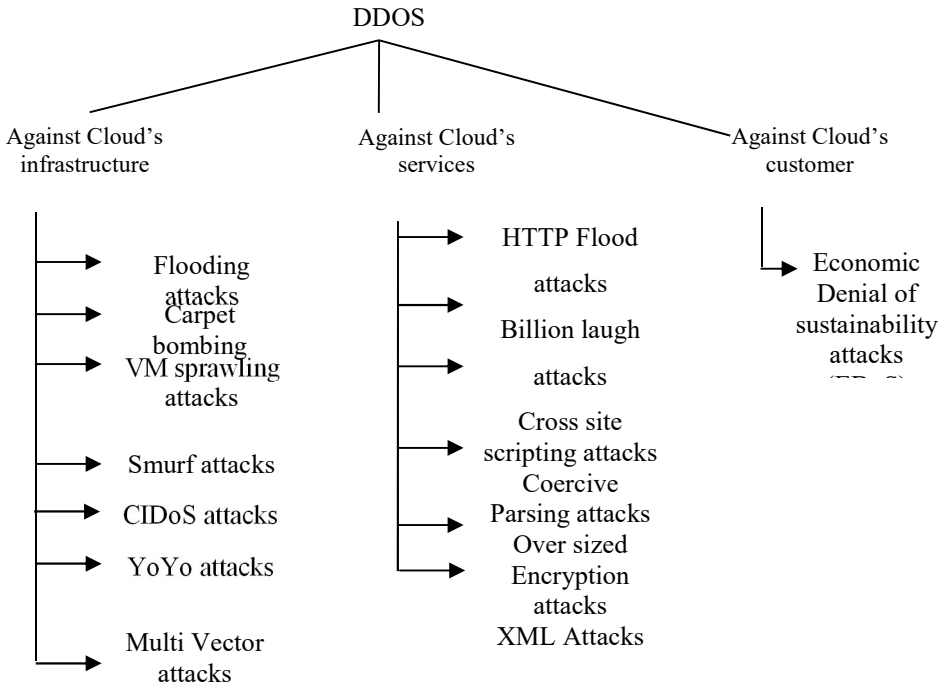

Figure 3 DDOS types categorized against Cloud aspects according to Bhardway et, al. [19]

Table 1 Comparative analysis of DDOS categorization according to recent research

Authors	Year	DDOS Categorization	Attack type covered		
			High rate	Low rate	E-DOS
[16]	2019	Brute force and semantic	√	√	√
[17]	2021	Attacks against network, server, and application resources	√		
[18]	2020	Bandwidth and resource depletion, direct and indirect, flooding and non-flooding , and attacks against network, servers, and application resources	√		
[19]	2021	Attacks against Cloud's infrastructure, services, and consumer	√		√
[20]	2019	Authors discussed the different types of highrate DDOS	√		
[21]	2018	Attacks against the cloud's components,	√	√	√
[22]	2020	High rate, low rate, and shrew attacks		√	√

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2 comparative analysis of DDOS prevention techniques

Authors	Approaches	Techniques	New Techniques Proposed	Comments
Agrawal & Tapaswi (2019)[16]	√	√		Discussed resilient scheduling, network traffic management, hidden servers approaches
Bakr et al (2019) [9]		√		
Potluri, 2020 [26]		√		
Srinivasan et, al (2020) [27]	√	√		Discussed challenge response, hidden servers, &restrictive access
Harale &Thakare (2019) [28]		√	√	Only focused on the prevention of TCP flooding attacks
Saravanan et,al. (2019) [29]		√	√	The techniques weren't implemented
Saharan &Gupta (2021) [31]	√	√		Ideal and True prevention are conceptual not technical aproaches
Ali & Osman 2018 [32]			√	Performance of the prevention in their framework was not examined as the detection was