# An Overview of DDOS Attacks Detection and Prevention in the Cloud

**Article** · December 2016

DOI: 10.5120/ijais2016451628



**1 author:**

Khalid A. Fakieh
King Abdulaziz University
**54** PUBLICATIONS **49** CITATIONS

*International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868*
*Foundation of Computer Science FCS, New York, USA*
*Volume 11 – No. 7, December 2016 – www.ijais.org*

# An Overview of DDOS Attacks Detection and Prevention in the Cloud

Khalid A. Fakeeh, PhD
King Abdullaziz University
Jeddah, Saudi Arabia

## ABSTRACT
Security is an illusion unless you are hacked. Attacks in the Cloud have more catastrophic and destructive impact on the organizations than the user might expect. As attacks are constantly evolving and making it difficult to defend. Most of the organization will try to check their devices in the cloud to protect against viruses with traditional security measures like antiviruses, or firewall thinking it secures across different attacks, but with a wide range of change in attack pattern organizations have exposed to significant operational and business consequences, not to mention public embarrassment. In this paper, we conducted the survey on DDOS (*Distributed Denial of Service*) attacks research work and analyzed prevention and detection methods used for DDOS attacks in the cloud. We found that there is a good amount of research scope in detecting and preventing slow client application layer attacks in the cloud.

## Keywords
DDOS, Attacks, Security, Threats, SAAS, IAAS.

## 1. INTRODUCTION
As initially designed, the Internet was envisioned to expedite honest data transfers amid different interconnected workstations and systems. It was not planned to optimize data security. Nevertheless, the computerized equivalents of infections, pathogens, and other comparable jeopardies have been perceived since the origins of the Internet. In 1988, when the Internet's forerunner, ARPANET, was comprised of approximately 60,000 interconnected machines, a self-replicating PC system, the Morris Worm, inadvertently disabled nearly 10% of these machines. There are many famous and infamous security incidents on the Internet, and there is no comprehensive database available for all these incidents as many go unreported due to various reasons. After the worm incident, CERT was established in the USA by DARPA to correlate and document the security incidents after that. The formal classification of attack and an incident was

then formulated. An attack can be termed as single or multiple unauthorized attempts to gain access to the system irrespective of whether it's success or failure. An incident is a term coined for multiple attacks which are mostly structured and distinctive in nature. They have their peculiarities in timing, techniques, and modus operandi. The infamous "I Love You" worm released in early 2000 is one of the greatest threat that has affected millions of PCs throughout the world. The "Conficker" virus appears to be the second in the list of Top 10 Web Threats in the history of Internet released by Symantec. There are many other threats like Melissa, Slammer Nimda, Blaster Worm, Storm, etc. which has hit millions of users worldwide. Apart from the virus and worm attacks, there were many other security incidents which resulted in major data breaches and service disruptions. Hackers have altered the websites of major US Departments like Department of Justice (1996), US Air Force (1997). In 2003 a hacktivist group called "Anonymous" was formed and still they continue to be one of the most dreadful unethical hackers in the Internet world.

## 2. TYPES OF ATTACKS/THREATS:
Many forms of attacks evolved namely Data Destruction attacks, Denial of Service, Data Theft, Trojans and Rootkit injections, Phishing and Identity Theft Attacks, Worms and Viruses and advanced persistent threats. Despite constant warnings, many organizations still fail to protect legitimately for cloud resources. With a current user base more than 1 billion clients, the Internet has evolved into the preferred method for organizations and individuals to reliably and which can manage financial institution's products, access online classes, perform hotel and airline reservations, and numerous other tasks. Additionally, the rapid ascent of online social networking has greatly increased the Internet's significance as a marketing platform, which has enhanced targeted marketing opportunities and created critical income source [1]. The growth of e-commerce has tremendously increased various online transactions. In the initial days, online retailers were more focused on the growth and penetration of their service but did not invest in securing the platform. This, in turn, resulted in many security incidents in the e-commerce sector. Payment data sector continues to be the most affected sector. More than 50% of the attacks that took place in 2013 to 2014 have targeted the ecommerce systems. Apart from the Point of Sale (PoS) terminals, the hackers have got access to the Data centers, and almost 10% of the attacks come in the same category.

### 2.1. Major Security Provisions or Requirements
Several high priority breaches have caused organizations to be utmost cautious about implementing electronic commerce systems. The customers are at great risk since they lose their private data and money even when they are unaware of the security aspect of the transaction that they are doing online [2]. Any Computer or Internet-based system must adhere to the fundamental security requirements so as to comply with various standards. Authentication is the method if verifying one's identity or a prerequisite to allowing access to a particular system. The System may challenge the identity of the user, and the user must be guided how to prove the claimed identity. Access Control consists of authentication, authorization, and audit. Data Confidentiality means keeping all the data and transaction information strictly obscured from the view of the unintended audience. Confidentiality and privacy are major issues of utmost concern, and almost 60% of the total internet populations are affected.

## 3. CLOUD COMPUTING OVERVIEW
Cloud computing architecture enables the efficient use of computing resources, which are provided as a service over a

network. The name is based on the cloud symbol; It is the base of the complex infrastructure of the system. Cloud computing services are entrusted with remote user data, software, and computation [3]. Depending on the resources of the cloud, cloud computing has been developed and divided into three layers. The provisional computational resources are utilized on demand as per the need of the application. The user does not need to possess the necessary hardware or software which is usually needed to run the application. On-demand resource allocation and pooling is the major aspect of a cloud computing environment. The users have the option for self-service which facilitates the user to avail computing resources as and when required. On-demand scalability and elasticity of the cloud environment allow rapid provisioning and expansion as per the requirement of the computational resources [3]. IaaS – Infrastructure as a service – This layer provides hardware computing resources as a service. For, e.g., Users will have a virtualized server depending on their infrastructure requirement of the application. The users will not have control over the orchestration layer but will have control over the Operating system, the application deployed as well as storage [4].

PaaS- Platform as a Service – These are often referred to as middleware as a service also. This level is a secure and provisioned layer over the infrastructure layer which provides users support for programming language platforms such as.NET, J2EE, etc. Various middleware services are Google App Engine (GAE) or Microsoft Windows Azure [4].

SaaS – Software as a Service – This is the topmost layer of a cloud computing environment and can be essentially denoted to as application hosting. An application like CRM, ERP, etc. is hosted in the cloud and licensed to users on a usage basis or monthly/yearly basis [4]. Security in Cloud Computing Environment – There are few major security issues in cloud computing and out of that seven issues are important to be considered [5].

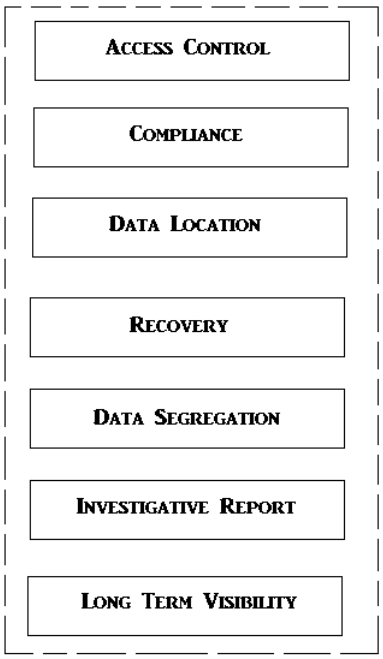


**Figure.1. Security issues in cloud computing**

1. Access control issues are about Data ownership issues of the transmitted information from the client
2. Compliance issues are about The security of the application deployed by the clients are their responsibility and Proper audit to be done by the clients to make their application secure and free from OWASP top 10 vulnerabilities
3. Data location issues include The clients may not be knowing in which country or jurisdiction their data resides
4. Recovery issues are about Thee should be adequate disaster recovery mechanisms
5. Data segregation issues are about the information from multiple companies will be available in the cloud. Adequate controls must be deployed to segregate and compartmentalize the data [5].
6. Investigative reports include, fault activity information which is gained from legal ways will not have access for clients [5].
7. Long term visibility is if the ownership of the provider is transferred, then the client should have the ability to retract a contract [5].

To mitigate the above issues or risks, the essential security service which is deployed in a cloud should cater the following attributes

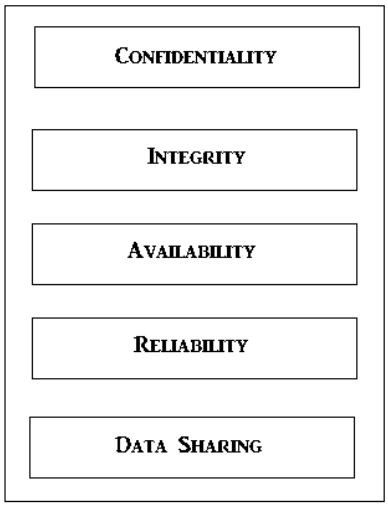


**Figure.2. Security Attributes in the Cloud**

1. *Confidentiality:* All the data submitted or hosted by the client should be secure. Adequate controls and measures must be deployed so that the access to the data is available only to the client and the cloud service provider
2. *Integrity:* The data submitted by the client must never be tampered or altered by the service provider of the cloud or by any other unauthorized user
3. *Availability:* The data hosted by the client must be available 24x7 without any disruptions through authentic means
4. *Reliability:* The client data must be protected and should have high availability. Adequate disaster recovery mechanisms must be deployed

5. *Data Sharing:* The clients must be able to share the data between their trusted parties without any hindrances.

## 3.1 Types of Attacks in Cloud

The disadvantage of this capability and convenience of a connected world is that it's vulnerable to intentional disturbances. Malevolent users frequently attempt to obtain sensitive data or disable typical workstation functions. Malevolent Intentions frequently involve the theft of personal or financial data. A digital attack by a pernicious gathering mechanism, intended to disturb a site on the Internet (or any mechanism joined with it), is termed an availability based attack. These attacks utilize a broad range of distinctive attack vectors, including TCP surges, (HTTP) Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure (HTTPS) surges, low-rate attacks, Secure Sockets Layer (SSL) attacks, and others. As a result, availability based strikes are among the most significant security dangers affecting Internet sites [6]. These attacks are referred to as denial-of-service (DoS) attacks. If the attack is executed by multiple machines, it is referred to as a distributed denial-of-service (DDoS) attack. Both DoS and DDoS attacks are widely reported in the news media, with articles describing how malignant hackers were able to cause critical downtime or rupture security for a well-known and trusted site [7]. In DDoS attack, a legion of malevolent hosts usually referred to as "zombies" harmonize to aggregate and send massive data to a target server. The network nodes in the edge are likely to develop resource crunches and will progressively become vulnerable. The resource overruns are likely to be inversely proportional to the distance from the edge. Two reasons are identified for such an impact. The node which is near to the server mostly has less service capability as its closer to the network edge. The closer nodes mostly have less capacity as so handles fewer users. Secondly, such type of nodes will have to suffer more aggregated attacks which compound inside the network. Under extreme overload situations, the entire server system itself becomes vulnerable and prone to disruption. Till now DDoS is one of the major and most destructive type of attack on the Internet over the past decades [8].

# 4. DDOS ATTACK DETECTION & PREVENTION IN CLOUD:

The ways to resist and restrict DoS and DDoS started evolving in the early decades. Since the late 1990s, the idea of intrusion detection systems (IDS) has evolved. IDS refer to hardware and software that detect and record suspicious, anomalous, or inappropriate activities. An intrusion prevention system (IPS) has functions similar to those of IDS but is more sophisticated in that it is capable of taking the necessary measures to prevent or reduce malicious activities. This work combines IDS and IPS in what is called an intrusion detection and prevention system (IDP). Numerous studies have focused on the use of one of the IDS techniques, which include anomaly-based detection (AD), signature-based detection (SD), or a hybrid of both [9]. Intrusion Prevention Systems offers a defensive layer to protect networking systems. IPS can be termed as a proactive network technique combining the firewall techniques and intrusion detection systems. IPS evades or blocks the attacks from affecting the network or precisely intruding into the network by probing various datasets and data records and utilizing attack pattern recognition sensors. On successful identification of an attack, the Intrusion Prevention System blocks the attack and logs the felonious data. The IPS identifies attack patterns using signatures which perform matching of the inbound and outbound data. The IPS also performs host detection of both inbound as well as outbound packets and tries to block the threat activity before any indemnities are caused by the attack. The Host-based approach [10] utilizes the host or the operating system to monitor and prevent the attacks. Host-based is the most prevalent standard for IPS. The host-based IPS is deployed by installing a small resident program/application in the host operating system level. This application is often called as the monitoring agent. The monitoring agents check for any suspicious activity from the host which it is deployed and report it to a central monitoring station. This enables the IPS to prevent the attacks well before it reached the target. The monitoring agents generate some alerts depending on the type of activity and are categorized based on priorities which can be customized. Various levels of monitoring are done by the monitoring agents viz Filesystem Monitoring, Logfile Analysis, Connection Analysis, Kernel-based Intrusion detection, etc. The system also checks whether specific parts of memory is accessed or modified and acts accordingly. The monitoring agents check for system configuration files and scans for insecure setting and other objects which are prone to security violations. The major disadvantage is that if a malevolent intruder is successful in altering the monitoring agent, there is no way to thwart the attack unless the security administrator deploys sufficient controls[11]. Network-based approach: This approach mainly efforts on the network by sniffing, identifying and fingerprinting all the inbound and outbound packets in and out of the network. The Network-based approach requires a combination of other network-based security systems to effectively provide a comprehensive security to the network and the servers. One advantage of the network-based approach is that there is no need of any client or monitoring software to be installed on the host machines. The "Trap" is a new technology in Internet security that enables users to turn the tables on attackers. This technology is intended to be attacked so as to obtain information about the attacker. IDSs are widely deployed in computer networks to face against a large type of attacks. IDSs deployment raises a significant drawback, particularly managing of an oversized variety of triggered alerts. This drawback becomes worse by the very fact that some business IDSs might generate thousands of alerts per day. Characteristic the $64000 alarms from the large volume of alarms may become irritating for the organization. Hence, reducing false alarms may be a crucial issue in IDSs potency and usefulness [12]. The IDS's offers great and in-depth information about the attack vectors and area of intrusion. The major aspect if any IDS or broadly security infrastructure in the prevention of zero-day attacks. Zero-day attacked are classified as those attacks. This class of attack refers to attacks which have never popped up or observed and has no signature logged into the database about them. Pure signature based systems are unable to trace out or prevent zero-day attacks. Anomaly-based Intrusion Detection system Is a devised to have the ability to prevent zero-day attacks in real time. The anomaly-based systems are devised to function by detecting the anomalies or divergences from the normal operating procedure from a predefined operating procedure. This anomaly based detection enables an IDS to prevent zero day attacks by calculating the percentage deviation from the streamlined procedure. The detection of both local and global zero-day attacks are the major challenge for an IDS. While detecting the former is fairly easy for IDS as the streamlined local procedure is almost well defined but identifying the global zero-day attack still seems to be a challenge. But in

reality, this leads to a high Detection rate which in turn causes a large amount of False Alarms. Intrusions are defined as malicious events or behavior that intends to harm a system or to gain unauthorized access to a system. IDS refers to software that inspects inbound and outbound network traffic that is attempting to compromise, attack, or break into a system .IDS has its rules for normal and other-than-normal behavior to detect possible intrusions. These rules vary for different scenarios. IDS acts like a burglar alarm. IDS raise the alarm if an intrusion occurs. An attack could be successful or unsuccessful and in both cases [12]. IDS are responsible for logging the attacking behavior, which could then be analyzed by the administrator to deal with comparable threats in the future. Detection could be signature-based or anomaly-based [13].

## 5. RELATED WORK IN APPLICATION LAYER

Modeled attack Detection Method (MAD) and Periodic attack detection (PAD): IP to hop count method is used to detect spoofed packets and then discard the same in [20]. It's not possible to change the TTL value of the packet as it says some hops the packet has taken to reach its destination. Time to live field of IP header is used to generate hop count information. Here Hop count filtering method is used to build an IP to hop count mapping table by combing all IP addresses based on hop counts. Created mapping table will detect IP packets which are spoofed and will discard the same. Hop count mechanism can be made more accurate using the Fuzzy logic technique to find out packet arrival time. Modeled attack detection method operates on the time series and sample it so that it can detect attacks very soon than periodic attack detection methodology, as PAD technique depends on the near periodic traffic nature [18].

Dynamic Detection Method: The dynamic detection method is described in the paper [19]. This mechanism is deployed on the edge routers which stay near to victim location. Each such routers will be made ti perform attack detection on the egress ports of the routers which are further connected to victim networks. If a low-rate transmission control protocol attack is detected, the router has to verify the input port (s) from that the attack traffic is being received. Detection is then carried out on all the input ports of the affected router. If a low-rate attack is detected at ingress input port, then the affected router can block the detection to any or all the upstream routers connected to the input port. If the affected router cannot discover a low-rate attack at any of its input port, this implies that the low- rate attack is being distributed in an exceedingly distributed manner. Once a low-rate attack is detected, this pushback mechanism is employed to spot the attack as near the attack origin as potential. The pushback mechanism minimizes the amount of affected transmission control protocol flows [19].

Shrewd Sending Rates and Buffer Size: TCP flow can be protecting from shrew attacks by increasing the buffer storage capacity of the target router. When flow management and queue management is used to get high link utilization, then TCP flow can be protected using shrew attacks as mentioned in [21]. Low DOS attacks go undetected as random early detection schemed will help in avoiding congestion at the router, which will consider longer queue size and high burst rates. The attacker has to transmit at high speeds to fill the longer buffer. Hence these are not low rate attacks and cannot be detected with RED algorithm [21].

Randomising Retransmission Timeout: Most of systems have retransmission timeouts (RTO) of 1 sec. This very standard value is being exploited by low rate DOS attacks. If RTO value is set to any decided value, then it's believed that attacker will not be able to detect the right RTO. Using this parameter rate of attack can be controlled. When flows are monitored properly, and by using RTO randomisation, problems with packets can be detected, and back tracing will help in finding the attacker as explained in the paper [22]. This is not very effective and efficient way to detect the attacks. This will fail to detect low rate DDOS attacks. When attacks look legitimate, this technique will completely fail and will not able to detect or prevent such attacks [22]

Packet percentage and queue caching method: Target router's cache queue is investigated by the method suggested in [23]. The detection method regulates the incoming traffic based on the arriving traffic flow at the router. This provides active queue management [23]. Here, Halting anomaly with weighted choking is used for detecting low DDOS attacks. The proposed HAWK method uses dropping algorithms to detect the Denial of service traffic flow. It achieves fairness among non-adaptive traffic flow and adaptive traffic flow. Attack detection is performed by referring two parameters. First is analyzing the cache queue for a percentage of packets at the target router. It is done by verifying the TCP packet's percentage of attacker flow. The second parameter is the threshold percentage, Using some packets of clients and attackers threshold percentage are calculated. TCP flow will detect low DOS attack using the threshold value [23].

An Extended firecol known as E-Firecol is proposed in [30]. This is made up of intrusion prevention system which will be placed in Internet Service Provider (ISP) level. This Intrusion Prevention System creates a ring of virtual protection around the hosts to defend against Denial of service attacks. It is also collaborated by exchanging the selected traffic information. Experimental results discussed in this papers proves that E-Firecol is very effective when compared with plain firecol [30]. Whereas this paper research doesn't concentrate on application layer DDOS attacks. Protection at ISP level doesn't guarantee that web services will not be attacked. Hence this system is still vulnerable to slow and low application level DDOS attacks. Intrusion Prevention System traditionally had done using a firewall. Genuine users' state information can be preserved by using stateful firewalls. But these are not able to prevent high volume DDOS attacks [30]. These firewalls will work best in the network layer, but they cannot detect low and slow attacks as in the case of application layer attacks.

Multilevel DDOS attack detection is provided by combining existing anomaly based detection system with entropy-based systems. At the first level, users are verified at the network level for legitimate requests by making users request pass through a router which has many detection algorithms. In the second level, another router at cloud environment will detect for attacks and it is passed through thresholds. If the connection is beyond a threshold value, then it's considered as legitimate. Else it is detected as an attack. The third party is used to represent and maintain this system. Whenever an attack is detected then, it will notify the user as discussed in [31]. This approach doesn't qualify for requests as Routers will deal with network connections and application layer attacks will be targeted at the request level. Threshold values don't sufficiently detect if the attack is high flood attack or

low attack, and there is no clear explanation that system doesn't block the legitimate user.

Low rate DDOS attacks are detected by flow level filter [32]. Traffic rate is gradually increased gradually, and network hosts will be attacked by low rate DDOS attacks. DDOS attacks are blocked by flow level filter as discussed in the paper [32]. Cloud computing offers different services on demand. Software puzzle is a technology in which end-user will be provided with a software puzzle which user needs to solve correctly before gaining access. The user will request for access to services in cloud and service provider or server will respond with a puzzle. Successfully solving the puzzle will lead to access. If the user provides incorrect puzzle access will be blocked. A Large number of requests is sent using software or machines for DDOS attacks. Here threshold based request method is used to solve DDOS attacks. Means user will be allowed to provide an only certain number of requests in certain time. Any user who crosses the threshold value will be blocked by the system as discussed in [33].

Neural Networks and Data mining technique is used to detect DDOS attacks. This model needs less memory and claims that they have faster detection. The result shows that most of TCP attacks are detected as discussed in [34]. This system doesn't help in detecting layer 7 (Application Layer) attacks and carry a lot of overhead. TTL value method doesn't help in detecting low and slow attacks. Packet monitoring in the cloud for TTL value said to have greater advantages in detecting DDOS attacks in the cloud, but it slows down the system performance which creates a limitation for cloud service providers [38]. Most of the high flood DDOS attacks can be detected using TTL value monitoring but low and slow attacks remain hidden, and the system tends to be highly vulnerable to such attacks.

In the Figure.3.0 low rate DOS attacks are explained. Attacking duration is mentioned using Ta. Attacking burst width is indicated with Tb. Attacking burst rate is indicated using Rb. TCP throughput will be decreased with LDOS attacks. Retransmission Timeouts will increase during LDOS attacks. An attacker can easily manipulate the flow in such a way that it can lead to increase in RTO ( retransmission timeouts). LDOS attacks will have longer duration flow which will create congestion but less enough to catch within

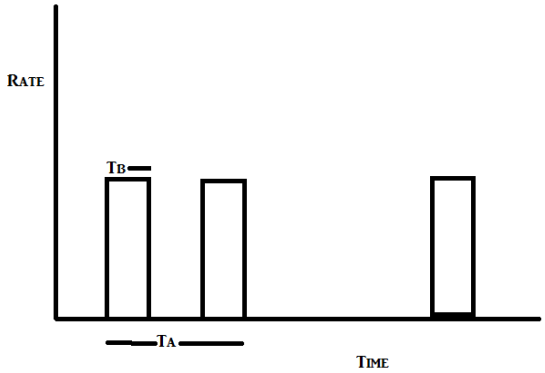


**Figure.3.0 "Low rate DDoS time diagram."**

congestion and large rate to create losses of packets. Resources of designated servers will be consumed by such LDOS attacks and violate server protection schemes [35]. High rate DOS attacks can be detected in the routers or by most of DOS mechanisms. Low rate denial of service attacks is tough to detect. In this paper [36], low rate DDoS detection is tried using a combination of analytical modeling, experiments, and simulations. Low rate DOS attacks exploit TCP's retransmission timeout mechanism. Protocol homogeneity is exploited by such attacks, an attempt of studying random timeout mechanism is made in [36]. DDOS attacks detection techniques are reviewed, and a numerically stable framework development is focussed in this paper [37]. A literature review and different algorithm analysis are done. A study of parameter considered by DDoS detection is carried out here. An algorithm is described here which uses the parameter context value to determine the reliability of the DDOS detection algorithm [39].

**Table.1.0. "Comparison of DDOS Mechanisms"**

| **Mechanisms/Papers** | **Working approaches** | **Benefits** | **Drawbacks** |
|---|---|---|---|
| IP Trace back methods for Flooding attacks on Internet Threat Monitors (ITM ) Using Honeypots [14] | Proxy Servers are used here. Honey pots act as proxy servers and honey pot entries are used to trace the attacks. | Very less overhead and servers will not be damaged directly. . | Honey pots are cost consuming processes, and there is a higher amount of processing delay. |
| Grey Rational Analysis and Decision Tree Methods [15] | Traffic Strength is analyzed by creating decision trees. Upstream Router's traffic flow is analyzed, and the decision tree is created. | Attack strength can be improved by identifying upstream routers. Helps in detecting flood attacks. | This system will face difficulties when network size grows higher and higher. It doesn't detect low and slow HTTP attacks. |
| New information | For each session flow of the network, information | To calculate information distance, computational complexity is very less. | There is no guarantee that Accurate detection is Possible. It's of more |

| | | | |
|---|---|---|---|
| metrics[16] | distances are calculated. | | theoretical than practical results. |
| Enhanced ICMP traceback-Cumulative Path[17] | Victim uses I trace-CP messages to track source and path used. These Itrace-CP messages are generated by intermediate routers. | Entire attack path will be constructed in very short time | It is difficult to adapt to changing topology as changes need to be done on every router and more space is needed to process packets. |
| Dynamic Detection Method [19] | This is deployed near to victim site. Normally on the nearest router of the victim site. It's effective for non-distributed low DoS attacks. | No extra memory is needed if any modification is needed to existing infrastructure. | Processing and memory overhead and Fails against Distributed LDOS Attack |
| Periodic attack detection (PAD) and Modelled attack Detection Method (MAD) [18] | IP to hop count method is used to detect spoofed packets and then discard the same | It depends on the signature database and also on the accuracy of fuzzy controller design. Hence its said to be effective for known signatures. | The monitoring mechanism is needed and has high processing and memory overhead. |
| Halting anomaly with weighted choking [23] | HAWK method uses dropping algorithms to detect the Denial of service traffic flow. It achieves fairness among non-adaptive traffic flow and adaptive traffic flow. | Threshold Value set is used and can be effective with a proper threshold value. | The monitoring mechanism is needed and Processing overhead and not effective for slowloris, RUDY, and other slow attacks. |
| Random Early Detection [21] | TCP flow can be protecting from shrew attacks by increasing the buffer storage capacity of the target router | It depends on known patterns and signature database. | Memory and Processing overhead is seen and will not be able to detect slowloris, RUDY or any new slow attacks. |
| RTO randomization[22] | Most of systems have retransmission timeouts (RTO) of 1 sec. This very standard value is being exploited by low rate DOS attacks. If RTO value is set to any decided value, then it's believed that attacker will not be able to detect the right RTO | The rate of attack can be controlled. | This fails for distributed DDOS attacks in the cloud. This will not be able to detect application layer slow and low rate attacks. |
| Utility- Oriented Federation of Cloud Computing Environments for Scaling of Application Services [25] | Cloud Simulator tool is used to implement this methodology. Various applications are implemented using federated cloud environment. | High-Performance Gain is seen using this methodology. | This doesn't help in detecting slow and low attacks of the application layer. And not practical |

| | | | |
|---|---|---|---|
| A Study on Recent Approaches in Handling DDoS Attacks[26] | DDOS attack detection implementation is discussed. Many approaches are used here. | Various approaches of DDOS attacks are discussed and analyzed in this paper. Methodologies used by all these approaches are highlighted. | There are no good methods to detect slowloris and RUDY attacks discussed here. |
| Cloud-based Security Research Testbed: A DDoS Use Case [27] | This paper discusses solutions for network security managers by analyzing a cloud-based research testbed. | These testbeds enable operators to emulate various network topologies, services, and to analyze attacks threatening these systems. | The framework is not practical and doesn't help in detecting application layer slow and low attacks. |
| Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing[29] | The proposed architecture takes into consideration of different pricing and purchase functions. Service quality differentiation is provided by architecture. This will help in selecting clients based on good behavior and differentiate bad behavior clients. | Here in this paper distributed gateway based architecture is implemented for the dynamic resource pricing of Distributed Denial of Services. | Fewer chances of predicting attacks. |
| Detecting Distributed Denial of Service (DDoS) Attacks through Inductive Learning[28] | The ratio of no of TCP flags to the total no of packets is calculated based on proposed network traffic analysis methods. The presence of DDOS attacks is detected based on TCP flag rates and by using machine learning algorithms. | Machine learning algorithms seem to be effective for layer 4 attacks. | This applies only on the specific flags depending on the rate of such flags in the traffic. This is not proven a method for application layer attacks. |

No more an interloper is necessary to attack the entire infrastructure. One can directly target the resource intensive applications that one is executing on the cloud and use simple low ¬band width attacks to make as unavailable to that service. Secure HTTP is one of the good specimens of DOS attacks. The websites or services hosted on high-profile web servers like e-payment gateways, banks, and even domain name servers [40]. The flow of information can be controlled by the attackers by allowing some information available at prescribed times. Many studies have been carried out on the detection mechanism as the extent of damage caused by DDoS attacks has increased. Although, the present or existing security mechanisms have failed in providing an effective defense against DDoS attacks or can only provide defense against specific types of these attacks. Few DDoS attack detection methods are based on trace back, while some others are on feature monitoring of a server [41]. Defense against DDoS Attacks like CLAD (Cloud -Based Attack Defense) run on cloud infrastructures as a network service to protect web servers. The goal is to have an innovative DDoS defense solution, which has enough capacity to extend the firepower of the botnets. CLAD is so transparent that no modifications are needed at clients side and server software. [41]

IDS (Intrusion Detection System): Signature based ID systems are sufficient to tackle the misuse intrusions, but cannot tackle out of the box thinkers who penetrations test, audit, or network attacks, purposely thinking nonlinearly with the expectation of ultimately discovering code, policy, and logic flaws. IDPSes are used for other purposes, such as identifying issues with security policies, documentation existing threats and also put-off individuals from violating policies [41]. Auto Responsive Honey Pot Architecture, Data Mining Approach, KNN, DDoS Detection using Entropy Classifier are discussed [41].

One of the complicacy to have an effective defense against DDoS is to identify the attacked traffic separately than legitimately traffics. Many spoofed IP addresses are used by the attackers to attack the system, thereby making it resource consuming to check each of the data packets. With the help of reverse checking mechanism, edge routers are used to mark the source of the data packet. A Large volume of data comes from certain slots in case of DDoS attack. If the source IP has

been created, the type of the data will be identical in most of the cases. With the help of TTL or hop counts, data packets are categorized as trusted or untrusted. "Hardware-based watermarking technology" can be used to perform this operation [42]

Cloud providers attempt to provide services and performance as if the programs were installed locally on the end user's system. Regardless of volume and magnitude of cloud, the maneuver IT virtualization strategy answers to contradiction to service attack which is dangerous threat capable of collapsing applications that are stored centrally in the cloud. The new form of XML-based and HTTP-based DOS is much simpler in implementing and also in devastating these attacks to web services [43]. DDoS attacks in the application layer attempt to target a specific service with web flood. For example, HTTP flood attacks send high rates of authentic application layer requests to a server in an attempt to impress the server resources. DDoS attacks consume less bandwidth and are far more difficult to recognize because the attacker attacks server through a flood of authenticating requests. [44]

Vulnerability in the protocol is the reason for flood attacks in HTTP. Mitigation method takes into consideration the perspective of the symbol or protocol design ensuring an effective and successful implementation, for the flood attack. The Cloud services level, followed by Network level, Web server level, Web service level, and Web application are the 5 mitigated main levels in the HTTP flood attack, as discussed in [44]. Various requests have been proposed to deal with DDoS attacks, but a way of attacking changes each time, no proposal completely prevents DDoS attacks. Honeypot is one of such approaches. These are similar to monitored decoys, which are employed in a network to study the try outs of hackers and also to alert network administrators of a possible intrusion. We need to defend our operating network with the high probability against known DDoS and future variants, first. And secondly, we can trap the attacker so that recording of the compromise can help in a legal action against the attacker [45]. The technique used in this project is based on average distance estimation in DDoS. We estimate the mean value of the distance in the next time interval by using exponential smoothing estimation technique in this project. This distance based traffic separation DDoS technique uses Minimum Mean Square Error (MMSE) linear predictor to estimate traffic rates from various distances. When the real value is out of the legal scope, the peculiar situation is detected. In the mitigation algorithm, specific detection methods are not involved, but we mainly focus on the resource management aspect of detection. [46]. Filter Tree Approach is used to Protect Cloud Computing against XML DDoS and HTTP DDoS attack, then Sensor Filtering, Hop Count Filter, IP Frequency Divergence, also Double Signature are used to detect HTTPS attacks as discussed in [47]. To separate and protect the web server from huge volumes of DDoS requests when attacked is the main intention behind the proposed system. Particularly, a DDoS defense system for protecting the web services is proposed [48].

## 6. CONCLUSION

In this paper, we discussed different research work conducted in the field of DDOS attacks in Cloud. We listed all possible DDOS attacks and the methods used to detect and prevent the same in the cloud. We found that though there is a lot of research has been conducted in DDOS attacks for the cloud. But, there is not much emphasis given on slow Application layer DDOS attacks. It is highly recommended to prioritize on slow client application layer DDOS attacks on Cloud.

## 7. REFERENCES

[1] Alzahrani, A., Alalwan, N. & Sarrab, M. 2014. Mobile Cloud Computing: Advantage, Disadvantage and Open Challenge. Proceedings of the 7th Euro American Conference on Telematics and Information Systems, hlm. 21.

[2] Curtis, G. and Cobham, D. (2005). Business Information Systems: Analysis, Design and Practice , 6thed, FT Prentice Hall, Harlow

[3] Zaigham Mahmood ."Cloud Computing: Characteristics and Deployment Approaches",2011 11th IEEE International Conference on Computer and Information Technology.

[4] Mr. P. R Ubhale & Prof. A. M. Sahu,"Securing Cloud Computing Environment using Intrusion Detection and Prevention System (IDPS),"International Journal of Computer Science and Management Research Vol 2 Issue 5 May 2013.

[5] Kazi Zunnurhain and Susan V. Vrbsky,"Security Attacks and Solutions in Clouds" in Proceedings of the 1st international conference on cloud computing, pp. 145–156, Citeseer, 2010.

[6] King, N. J. & Raja, V. 2013. What Do They Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data. American Business Law Journal 50(2): 413-482

[7] Bakshi, A. & Yogesh, B. 2010. Securing Cloud from DDoS Attacks Using Intrusion Detection System in Virtual Machine. Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, him. 260-264

[8] David K. Y. Yau, John C. S. Lui, Feng Liang, and Yeung Yam,"Defending Against Distributed Denial-of-Service Attacks With Max-Min Fair Server-Centric Router Throttles," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 13, NO. 1, FEBRUARY 2005

[9] Alqahtani, S. M., Balushi, M. A. & John, R. 2014. An Intelligent Intrusion Detection System for Cloud Computing (Sidscc). Computational Science and Computational Intelligence (CSCI), 2014 International Conference on, him. 135-141.

[10] Ahmed, Martuza, et al. "PIDS: A packet-based approach to network intrusion detection and prevention." Information Management and Engineering, 2009. ICIME'09. International Conference on. IEEE, 2009

[11] Pieter de Boer & Martin Pels, "Host-based Intrusion Detection Systems."

[12] Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L. L. 2009. On Technical Security Issues in Cloud Computing. Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, him. 109-116

[13] Babaie, T., Chawla, S. & Ardon, S. 2014. Network Traffic Decomposition for Anomaly Detection. arXiv preprint arXiv:1403.0157

[14] K Munivara Prasad, Dr. A Rama Mohan Reddy, IP Traceback for Flooding attacks on Internet Threat Monitors (ITM ) Using Honeypots, International Journal of Network Security & Its Applications (IJNSA), ISSN: 0974 - 9330, Vol.4, pp 13-27, No.1, Jan 2012.

[15] Y. C Wu,., Tseng, H. R., Yang, W., and Jan, R. H.,"DDoS "detection and traceback with a decision tree and grey relational analysis.,", International Journal of Ad Hoc and Ubiquitous Computing, Vol-7, 121–136.2011.

[16] Y. Xiang, Li, K., and Zhou, W., ''Low-rate DDoS attacks detection and traceback by using new information metrics,'' IEEE T Inf. Foren. Sec., 6:426–437 (2011).

[17] H.F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues," CERT Coordination Center, Special Report: CMU/SEI-2002-SR-009 (2002).

[18] K. Subhashini, and G. Subbalakshmi, ''Tracing sources of DDoS attacks in IP networks using machine learning automatic defense system,''International. Journal. Electron. Commun. Comput. Eng., 3: 164–169 (2012).

[19] Gautam Thatte, Urbashi Mitra and John Heidemann,"Detection of Low-Rate Attacks in Computer Networks,"University of Southern California IEEE (2005)

[20] C.Jin, H.Wang, and K.Shin: "Hop-Count Filtering An Effective Defense against Spoofed DoS Traffic," ACM CCS (2003)

[21] Sandeep Sarat and Andreas Terz, "On the Effect of Router Buffer Sizes on Low-Rate Denial of Service Attacks," IEEE Computer Society (2005)

[22] G.Yang, M.Gerla, and M.Y.Sanadidi, "Defense against low rate tcp-targeted denial- of-service attacks," ISCC '04 Proceedings of the Ninth International Symposium on Computers and Communications 2004 Volume 2 (ISCC"04), pages 345–350, Washington, DC, USA. IEEEComputer Society (2004)

[23] Y.K. Kwok, R .Tripathi, Y.Chen and H.K.HAWK,"Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks," Proc.of the 3rd Int'l Conf. on Networking and Mobile Computing (ICCNMC 2005). New York: Springer-Verlag, pp: 423-432 (2005)

[24] J.C.C.Rodriguez, A.P. Briones and J.A.Nolazco, "Dynamic DDoS Mitigation based on TTL field using Fuzzy logic," CONIELECOMP '07, Mexico (2007)

[25] Rajkumar Buyya, Rajiv Ranjan, and Rodrigo N. Calheiros," InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services," Springer 2010.

[26] Debajyoti Mukhopadhyay, Byung-Jun Oh, Sang-Heon Shim, Young-Chon Kim, " A Study on Recent Approaches in Handling DDoS Attacks," Cornell University Library,2010.

[27] Toma´s Jirsk, Martin Husak, Pavel Celeda, Zdenek Eichler, "Cloud-based Security Research Testbed: A DDoS Use Case,"IEEE, 2014.

[28] Sanguk Noh et al.," Detecting Distributed Denial of Service (DDoS) Attacks through Inductive Learning,"LNCS 2690, pp. 286–295, 2003.

[29] David Mankins, Rajesh Krishnan, Ceilyn Boyd, John Zao, Michael Frantz, "Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing," IEEE 2001.

[30] Ravi Chandra & Madhavi Gudavalli,"E-FireCol to Detect Multiple DDOS Attacks,"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 12, December 2013

[31] A.S.Syed Navaz et al.," Entropy-based Anomaly Detection System to Prevent DDoS Attacks in Cloud,"International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013

[32] Markku Antikainen, Tuomas Aura, and Mikko Särelä," Denial-of-Service Attacks in Bloom-Filter-BasedForwarding," IEEE/ACM Transactions On Networking, Vol. 22, No. 5, October 2014.

[33] Subramaniam.T.K and Deepa.B, "PREVENTING DISTRIBUTED DENIAL OF SERVICE ATTACKS IN CLOUD ENVIRONMENTS,"International Journal of Information Technology, Control and Automation (IJITCA) Vol. 6, No.2, April 2016.

[34] Pourya Shamsolmoali et al.," C2DF: High Rate DDOS filtering method in Cloud Computing", I.J. Computer Network and Information Security, 2014, 9, 43-50.

[35] H. V. Shashidhara & Dr. S. Balaji,"Low Rate Denial of Service (LDoS) attack – A Survey,"International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 6, June 2014

[36] Aleksandar Kuzmanovic and Edward W. Knightly,"Low-Rate TCP-Targeted Denial of Service Attacks and Counter-Strategies."

[37] Baldev Singh and S.N. Panda,"An Adaptive Approach to Mitigate DDoS Attacks in Cloud,"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 10, 2015

[38] Iqra Sattar et al.,"A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment,"International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 8, April 2015

[39] Aleksandar Kuzmanovic and Edward W. Knightly,"LowRate TCPTargeted Denial of Service Attacks," SIGCOMM'03, August 25–29,2003, Karlsruhe, Germany.

[40] T.Gunasekhar, K.Thirupathi Rao, P.Saikiran, P.V.S Lakshmi, "A Survey on Denial of Service Attacks," (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2373-2376.

[40] T.Gunasekhar, K.Thirupathi Rao, P.Saikiran, P.V.S Lakshmi, "A Survey on Denial of Service Attacks," (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2373-2376.

[41] Amit Khajuria, & Roshan Srivastava, "Analysis of the DDoS Defence Strategies in Cloud Computing " INTERNATIONAL JOURNAL OF ENHANCED

RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS.

[42] Masudur Rahman & Wah Man Cheung, "A Novel Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack,"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 6, 2014

[43] Santhi et al.,"A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks," International Journal of Advanced Research in Computer Science and Software Engineering 3(5), May - 2013, pp. 416-420

[44] FuiFui Wong and Cheng Xiang Tan,"A SURVEY OF TRENDS IN MASSIVE DDOS ATTACKS AND CLOUD-BASED MITIGATIONS," International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014.

[45] Kumar Shridhar & Nikhil Gautam, "A Prevention of DDoS Attacks in Cloud Using Honeypot," International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[46] Dr. S.SaravanaKumar, R.SenthilKumar et al.," Detecting and Preventing DDoS Attacks in Cloud,"International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2015.

[47] Kirtesh Agrawal and Nikita Bhatt et al., "Survey on DDoS Attack in Cloud Environment," International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 3, 2015.

[48] V.Priyadharshini & Dr.K.Kuppusamy,"Prevention of DDOS Attacks using New Cracking Algorithm," International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622.

[49] Iqra Sattar et al.,"A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment," International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 8, April 2015.

[50] Upma Goyal, Gayatri Bhatti and Sandeep Mehmi,"A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model," International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013.

[51] J.J.Shah and Dr. L.G.Malik, "Impact of DDOS Attacks on Cloud Environment," International Journal of Research in Computer and Communication Technology, Vol 2, Issue 7, July-2013

[52] Mohd Nazri Ismail et al., "New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment," International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (4)

[53] A.M. Lonea, D.E. Popescu, H. Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment," INT J COMPUT COMMUN, ISSN 1841-9836 8(1):70-78, February 2013.

[54] Krishna Modi and Prof. Abdul Quadir Md, "Detection and Prevention of DDoS Attacks on the Cloud using Double-TCP Mechanism and HMM-based Architecture," International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol. 3, No. 2, April 2014, pp. 113 – 120

[55] Esraa Alomari et al., Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications (0975 – 8887) Volume 49– No.7, July 2012

[56] Muhammad Morshed Alam et al.," Study on Auto Detecting Defence Mechanisms against Application Layer DDoS Attacks in SIP Server," JOURNAL OF NETWORKS, VOL. 10, NO. 6, JUNE 2015

[57] Muhammad Yeasir Arafat et al.,"A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server,"International Journal of Computer Applications (0975 – 8887) Volume 131 – No.1, December 2015

[58] Phenomon institute, "Efficacy of Emerging Network Security Technologies" February 2013.

[59]http://www.securityfocus.com/archive/1/456339/30/0/threaded

[60]http://www.cnet.com/news/paypal-suffers-from-e-commerce-outage/

[61] John Kindervag, "Develop a two-phased DDoS Mitigation Strategy," Forrester Research, Inc., May 17, 2013. CyberFactors, a wholly owned subsidiary of CyberRiskPartners and sister company of CloudInsure.com

[62] https://www.maxmind.com/en/geoip2-databases

[63]http://www.forbes.com/sites/jonmatonis/2012/04/02/watch-bitcoin-robbery-in-slow-motion/#66190b922bb9

[64] C. Zhang, Z. Cai, W. Chen, Luo, X., and Yin, J. "Flow level detection and filtering of low-rate DDoS. Computer Networks," 56, pages:3417–3431. (2012)

[65] Y. C Wu, Tseng, H. R., Yang, W., and Jan, R. H "DoS detection and traceback with decision tree and grey relational analysis.", International Journal of Ad Hoc and Ubiquitous Computing, 7, 121–136. .(2011)