International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Performance Perspective Analysis: A Detailed Vision on Denial of Service and Distributed Denial of Service on Cloud Computing

M. Mayuranathan, M. Murugan, V. Dhanakoti

Abstract*: In recent days cloud computing and cloud-based service, provisions play a vital and significant role in Internet-based information computing. It interrelates various applications like sales, purchase, banking, customer service, etc. and it behaves entirely as a service-oriented platform or environment. The primary objective of the cloud computing is sharing the resources within increased efficiency regarding time and cost for all kind of customers who needs a cloud service badly and immediately. Though the energy is high, it cannot assure that the cloud computing, service providing, and customer maintenance are highly secured. Service providers in the cloud are not strictly public; it may be private, community and hybrid. Malicious activities can be created or occurred in the middle of the communication and it is difficult to predict a particular person in the middle becomes a malicious user, from where and how. Secured data transmission and discussion in cloud computing considered as the main problem, and various earlier research works focused on tightening the security. The primary objective of this paper is to discuss different security mechanisms applied to multiple malicious threats in the cloud to understand the various issues and challenges faced in earlier research works. It provides a summary of the risks, appropriate method and the limitations and it helps to understand the primary and main problems related to security.

***Keywords* : Malicious Activities, DoS/DDoS Attacks, Detection, and Prevention Mechanisms, Cloud Computing, Cloud Security.**

I. INTRODUCTION

One of the information technology paradigms is cloud computing where it enables ubiquitous access for sharing different and numerous resources and services. Cloud computing provides better management on the internet. Cloud computing offers an enriched platform for sharing and accessing various resources under SaaS, PaaS, and IaaS [1-2] to reduce the economic consumption for the public. All IT companies are not ready to spend more money on computer resources to install and maintain. Hence the cloud service providers are paying attention to provide rental or agreement-based resources utilization strategies for various sizes of enterprises.

Cloud users are ready to access the resources with reduced maintenance and less cost with increased speed, improved manageability. All the service providing strategies follows "Pay-and-Use" model, which reduces the total cost of the installation, maintenance, and operation. One of the most critical facilities and advancement of the cloud computing is anybody can share/access any resources at anytime from anywhere. It also a significant drawback of cloud computing paradigm such a way that any malicious threats enter into the cloud. Hence denying or identifying the malicious users in the cloud computing is too tricky and it is an essential need nowadays. Each cloud service provider encapsulates the technical description of their services but provides the services based on the user requirement, where the user can only access the services. The number of services and services providers are uncountable in the cloud, whereas the user can choose the service and the service provider based on their policies, strategies and do the deployment. Since the service providers and users can access the data at anytime from anywhere, and then it leads to alter the cloud data without knowing by the owner of the data. The privacy policies and regulations are necessary for data accessing and offering data for a process which is stored in the cloud environment to avoid malicious activities.

It is essential to provide security for the cloud computing environment to escape from malicious activities. In earlier researches cloud security is provided in the form of policies, methods, techniques and related setup for data protection. Some of the activities related to cloud security are privacy preservation and data-confidentiality. There are several attacks occur in the cloud like a sinkhole, Sybil, wormhole, etc., and it all comes under DoS and DDoS attacks. By understanding the dynamic and static behavior of DoS and DDoS activities it can design a methodology against the attacks. Hence this study presents a detailed description of the various methods provided for detecting and preventing the data from DoS and DDoS attacks, to understand the multiple issues and challenges faced by earlier researches.

1.1 Background Study on Various Attacks

There are various kinds of attacks which have been presented already and newly created for hacking the data or information in networking as well as in web are discussed here.

Manuscript published on 30 September 2019
* Correspondence Author
M. Mayuranathan*, Asst.Prof/CSE, SRM Valliammai Engineering College, Chennai, India. Email :manimayur@gmail.com
Dr. M. Murugan, Professor/ECE & Vice-Principal, SRM Valliammai Engineering College, Chennai, India. Email: dr.murugan.m@gmail.com
Dr.V.Dhanakoti, Assoc.Prof/CSE, SRM Valliammai Engineering College, Chennai, India. Email: koti555@gmail.com

In this paper there are three different categories of attacks are discussed such as Browser level, Application level and Accessibility level.

1.1.1 Browser Level Attacks:

i. Cache Poisoning

One of the popular attacks affect network is DNS cache positioning attack where it corrupt internet server's DNS by changing the internet address using a rogue address. Whenever the user is looking of the website using the rogue address it will redirect the browser to different page not to the correct page. Mean time different attacks like spyware, worming, hijacking and other attacks can download the web content form the rogue position.

ii. Hidden Field Manipulation

Some of the web applications have the hidden fields within their web pages and it is possible to hack the hidden information between the browser and the web server. If it has poor coding then the hidden confidential information can be hacked easily stored in the database. The users using the web page or web application cannot see the hidden fields directly. But the attackers may able to find the hidden fields using the following steps as:

- By viewing the source of the web page
- By changing the data in the hidden fields
- Altering the page and reposting back to the server

iii. SQL Injection Attacks

An attacker can directly or indirectly control the database server of the particular web application or web page by using SQL injection attacks. SQL injection is a process of injecting a malicious SQL statement in to the database server. It causes vulnerability to the web application and it cannot be prevent and it is very dangerous. An attacker may by-pass the web applications' authentication mechanism and can retrieve the entire database information and even can delete the information in the database.

iv. Man in the Middle Attack (MIM attack)

During data transmission from any source node to destination node, or from one node to other node in a route, a node presence between the two end nodes can forward the data packets in the wrong route, or hold the data packet and not forwarding, or it alter the data packets and forward is called as man in the middle attack. Sinkhole, Sybil and wormhole attacks are some of the examples of MIM attack.

v. Cloud Malware Injection Attack

Cloud malware injection attack is one of the popular attacks in the cloud environment, in which the attacker insects a malicious service or creating a malicious VM in the cloud like an eavesdropping. The attacker successfully listen the information from the existing service provider to the consumer. Positively it can take charge of the full functionality of the cloud service and also it can do block the other services in the cloud. SQL injection and cross site scripting are the two kinds of cloud malware attacks affecting the entire cloud environment.

1.1.2 Application Level Attacks:

i. Backdoor and Debug Options

This attack is one of the popular attacks, in which a back-door user can login without providing an authentication credentials and can use a special URL for direct accessing of the particular web application. This type of application particularly available in the web and the developers can make the backdoors and turn the debugging to provide troubleshooting in applications. It is because of lack of policies and procedures when taking a system live.

ii. Captcha Breaking

The images that contain the text have to be typed before accessing the website is called captcha. This is a design for preventing an attack by automatically filling up the forms if it is not a real person. So that an attacker curious to break the captcha to crack the information. The developer split this captcha breaking into different phases as:

- Convert the color image into grayscale image.
- Then taking the captcha from the grayscale image.
- The pattern of the converted captcha is verified as a text or image.

iii. Google Hacking

By using advanced google searching methods, it searches the queries used to discover the security, vulnerabilities in the web pages and collects the information of the individual targets. And it can discover an error messages which has sensitive information and find the files having credentials of the data or information. Google hacking is also called as Google Dorking. The attacker searches the string such as DOTPWD, DOT SQL using advanced research methodologies and can get the specific list of sites containing all the information about the site.

iv. Cross Site Scripting Attack

It is an attack whereas an attacker injects malicious scripts to the authenticated web site or any web applications. It causes vulnerabilities in the web application which make unvalidated user input in the output will be generated. In this type of attack the attacker doesn't mean to attack the victim directly but instead it exploits the particular web application that the victim often visits that necessary web application using that vulnerable website as a vehicle to generate a malicious script to that victims' browser.

v. Hypervisor Attack

An intruder exploits the program and takes advantages of vulnerabilities that used to permit various operation systems by sharing a single hardware processor as known as Hypervisor attacks. The attacker uses the hypervisor services like create, delete, clone and migrate to perform and extent a threat. Root kit also another hypervisor attack but it is less common method. The hypervisor permits the hacker to attack the VM which is available in the virtual host. It causes denial of service in the host and also in the group of hosts. If there are various virtual servers involved in this hypervisor attack, then the problem leads to very worst condition.

vi. Dictionary Attacks

It is a technique or method used to crack the password in the protected system or server. The main purpose of this type of attack is to break the authentication system by entering systematically each word in a dictionary as a password.
Otherwise discover the decryption key in order to find the original message from an encrypted message or document. It is often getting successful because so many people in the business use the simple and easy password which can be find out in an English dictionary.

II. ABOUT DOS/DDOS ATTACKS

There are various kinds of DoS/DDoS attacks and different techniques to prevent these attacks illustratedhere. The detailed literature review about DoS and DDoS carried out with a specific type of attacks and technologies to prevent those attacks. Some of the works focused on similar methods to detect and prevent data from DoS and DDoS attacks. Hence some of the unique techniques are described in detail here, and it dealt with specific kinds of attacks. Also, the purpose of recitation of diverse types of attacks is to define several approaches and disparities of DoS attacks to provide complete repossession trials and best practice in networking to thwart high influence tragedy in contradiction of such attacks byways of technology and legal framework. Preventing DoS attacks is not possible in an inaccessible approach. Preventing various DoS and DDoS attacks used for applying CISCO ACLs when forgoing configurations and patches on the application hosts.

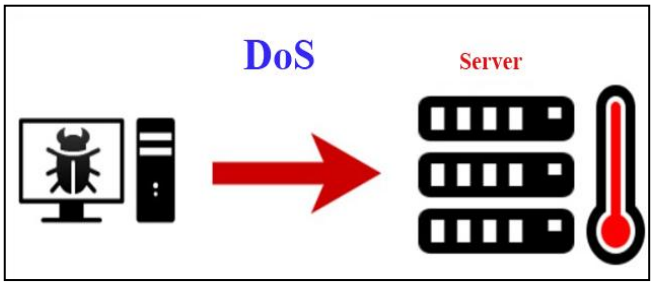

Fig-1: Denial of Service

(A DoS attack made from a single machine to a victim.)
The virus spread by Robert Morris Jr. on Nov. 3, 1988, harmed hundreds of computers in the USA, in research institutions stopped their regular process and also Yahoo entirely up to 3 hours on Feb.6, 2000. At the same time BUYX, E-Bay, Amazon, CNN, EGRP, and mayhem also got infected by the same. On Feb.12, 2000, the Business Week Online reported that DoS attack was detected first time in 1988. After a decade, various alarming attacks are identified by DoS attack. These kinds of interruptions create a high financial loss across multiple e-commerce sites. Hence hosting service provider is challenging for security beef-up. In the initial stage, the DoS attack did not affect the data, and there was no high risk but is producing large audit logs and becomes an irritation. Whereas in recent days DoS and DDoS attacks profoundly affect the information or data and treated as a severe threat, need to be alleviated competently. One of the main classes under malicious attacks which exploited on internet protocol originated by any individual or groups to repudiate other users from excellent access to system and information called as DoS attacks. In the earlier stages, DoS attacks associated with SMURF attacks are the target of routers. When the attacks stop data forwarding on the router will make hosts disconnected from the router. In recent days DoS attacks are focused on web and mail servers and other services. A perfect description of DoS attacks given in the book Incident Response: Investigating Computer Crimes [3] categorized mainly and it is given in Table-1. All the networks are having minor bandwidth suffer due to high bandwidth consumption immediately when it becomes a target. The response rate of the routers is depending on the support of the service providers.

Table-1: Main Categories of DoS attacks

Categories	Description
Destructive	Attacks which destroy the ability of the device to function, such as deleting or changing configuration information or power interruptions
Resource Consumption	Attacks which degrade the ability of the device to function. Such as opening much simultaneous connection to the single device.
Bandwidth Consumption	Attacks which attempt to overwhelm the bandwidth capacity of the network device.

DDoS attacks are a combination of DoS attack staged in recital from several hosts to reprimand the target from further serving its function. From the name DDoS itself says that it is not functioning on a single source (See Figure-1) but in multiple sources (See Figure-2). DDoS cannot be filtered out from a unique IP address, because it was thrown from numerous points installed with agents. Some of the known DDoS tools are Trinoo, Mstream, TFN2K (Tribe Flood Network), Stacheldraht and Shaft. It also considered as a bandwidth attack.

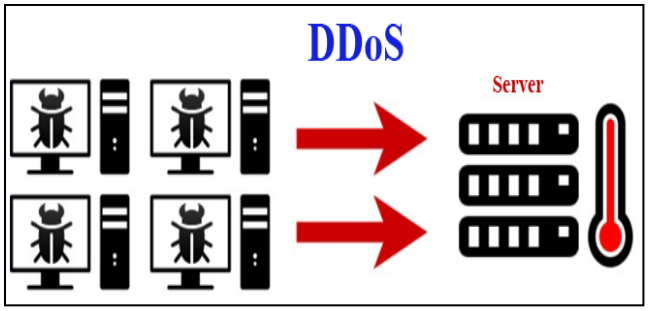

Fig-2: Distributed Denial of Service

(In a DDoS, the attack generation is instead distributed across multiple computers)

This paper used as a reference paper for analyzing the complete information about DoS-DDoS attacks. Also, it concludes DoS-DDoS attack is not a resolved one using single or holistic methods. Hence still there is a high demand for an effective way used for detecting and preventing DoS and DDoS attacks in computing, cloud computing, and networking.

Based on the vulnerabilities DDoS attacks are, and some of the categories of DDoS attacks are given in Table-2[4].

Table-2: Categories of DDoS Attacks

Attacks	Description
Smurf Attack	Forged ICMP packets are sent to the destination server which responds with ICMP reply packets thereby flooding the server with fake requests and denying service to real users.
TCP/SYN Flood	The target server is sent TCP packets with unreachable addresses. The server wastes all its time and resources in determining the right destination causing denial of service to others.
UDP Flood Attack	This happens when the attacker sends a forged UDP packet to a port which responds with a destination unreachable ICMP response. This floods the system if several UDP packets are sent.
Ping of Death	In this case, the destination server is sent an ICMP packet much larger than its expected size. The victim server is unable to reassemble the packet and crashes as a result.
Land Attack	This happens when an attacker sends a packet with identical source and destination addresses. This confuses the target server resulting in a crash.
Ping Flood	This is the most common of the DDOS attacks. Here the attacker sends repeated ping commands to a server resulting in flooding.
Nuke attack	The destination server is flooded with counterfeit ICMP packets that exploit the vulnerabilities of operating systems causing the system to halt.

To understand the various issues and challenges faced and discussed in earlier research works are presented here based on the categories. Initially an introduction point of view, Deepak Lal et al. (2014)[5] said that cloud computing is one of the Internet-based setting; it allows the human at any time and any place being to make use of software and hardware device. M. P. Boss et al. (2007), B. Whyman et al. (2008), & J. Heiser et al. (2009)[6-8]described that the cloud computing as ‘‘a stylish of computing where immensely accessible IT-enabled proficiencies are disseminated ‘as a service' to exterior clients all the way through Internet skills. One of the top most popular technologies used by various companies and organizations is cloud computing [9]. S. Subashini et al. (2011)[10] reported that 24% of the software companies had moved to cloud computing and the amount paid is increased to 95$ billion. Some of the physical resources can be shared as some services through virtualization in IaaS cloud [11].
For example, Amazon EC2, GoGrid, and RackSpace cloud are IaaS in cloud computing. PaaS provides operating systems, server applications like web servers [12] are the services. For example, Google App Engine, Azure platform of Microsoft Windows services under PaaS. CRM, Google Docs, and Salesforce.com are some of the SaaS services in the cloud [13]. Some of the critical issues often occur in cloud computing is security and privacy, it is happening because of sensitive data stored in the cloud [14-15]. Opponents of cloud computing stated that it doesn't have enough security. This paper reports a detailed survey of cloud security focusing on the security challenges and the solutions for the same. Comparing with all the attacks, DoS, DDoS and EDoS attacks are still not prevented or detected completely in the IT environment. Hence this paper focuses on discussing DoS, DDoS and EDos attacks briefly.

III. A Survey of Cloud and Data Security

Almorsy et al. (2016)[16] discussed in detail about the factors associated with the security of the cloud and investigated about the challenges involved in the cloud framework with the view of cloud service providers and the users. The author proposed a security solution to the cloud security challenge and the key features about them. The issues related to cloud infrastructure, service providing issues, policy-related issues and service provider related issues are discussed in detail here. The security challenges in the cloud network and each challenge's origin and causes addressed. Hence the current researchers can understand the existing problems involved with the service providers and vendors in various extents. The author motivated to discuss the detailed study of preventing a malicious attack in the current cloud environment. Also explained the technologies involved in security challenges, multi-tenancy challenge, managing the security control, providing a cloud model for better security. Also suggested the cloud model overcome the above-said difficulties with different layers of protection and to offer better protection.
Singh et al. (2012)[17]described the services provided by cloud and the security concerning the sharing of the services and how the malware activity happens in the cloud and the details of the cloud attacks discussed. The types of cloud attacker classified and how the attacker had taken control of the cloud to spoil the service instance in the cloud elaborated here. Due to the essential need of cloud service in the recent days, it pushed more attention to the malicious users to make the security attacks and to decay the process. In this, the author analyzed the type of vulnerable activities and explained the scenarios of the incident of attack and also proved the attack taxonomy’s applicability and appropriateness. Chouhan et al. (2015)[18]described the software vendors is not ready to pay more expense on deployment and maintenance, due to the modern technologies in the high-speed internet and software development. The software admires all the providers and users as a service (SaaS) for utilizing the features. But the security issues regarding the SaaS paradigm is more unwilling to move on. Thus, for the SaaS environment, security providing is the most significant task for preventing potential security threats. Also describes SaaS architecture with their usage and applications in various fields such as cloud computing, mobile cloud computing, software-defined network and Internet of things and the security threats which affect the multiple layers of the architecture of SaaS. Also thoroughly explained the security issues related to the SaaS framework which encapsulated by the various technologies.

Scalability, incorporation lower costs, reduces time to market; simple upgrades and use to perform proof of concepts in the SaaS framework promised. There is a lot of issues regarding all types of security must be resolved to attain this aim. Singh et al. (2014)[19] discussed cyber-attacks and mitigation. To mitigate the cyber attacks, initially, the service model is identified and highlights the potential threats applicable to the services. The proposed model checks the service model and the appropriate risks including data integrity. An Encryption process is applied to the data to avoid data loss. The proposed approach is immune from various attacks like replay, MITM, reflection and worm attacks. This method outperforms regarding cost, but it is not considering the data uploading and downloading process when comparing with the other bio-metric based security methods. Jitendra Singh et al. (2014)[20]believed that the sensitive data in the cloud damaged by cybercrimes and proposed a Comprehensive Five Phased (CFP) model for mitigating the cyber-crime. CFP model is implemented based on cognizance to improve the cloud security. CFP verifies and audits the country, cloud provider, connection and physical as well as logical resources in the cloud. CFP model also inspects various cloud paradigms to check the security like location, software and service provider for enhancing the safety and other necessary user information during communication. Hence the CFP model identifies and detects cybercrime attacks by proper auditing process. CFP functions at the client side during data transmission don't bother about server-side cloud storage. Hence, it needs to extend to server-side security and data security. While mitigating the cyber-attacks CFP makes data loss. Khan et al. (2016)[21] discussed the details of the services provided by the cloud at less cost and with enhanced performance. Even though more advantages in the cloud computing, it is not able to deal with security issues which may, in turn, aggravate the quality of service as well as the privacy of customers' data. A survey of the security issues and remedial measures to avoid those challenges in the cloud paradigm also discussed. The different malicious attacks in the cloud and the prevention mechanisms also compared. Cloud security-related challenges, processing mechanisms of preventing system, and its scalability are analyzed. The trusted cloud computing and examined a vast number of usual Acts and regulations essential for compliance by the cloud service providers also discussed. Lim et al. (2017)[22] described discovering the unstructured Sybil attack in the cloud with the use of unstructured Sybil attack detection algorithm in cloud computing environments. One-to-one communication primitives used rather than broadcast primitives and, therefore, the message complexity can decrease. In the design of the algorithm consists of the detection of the malicious nodes identified by the regular nodes with the fail-stop signature scheme. In spite of the number of attacker nodes, this Sybil attack detection algorithm can attain compromise. In this algorithm design, it does not rely on broadcast primitives and, therefore, the message complexity decreased from O(n2) to O(n), where n is the number of nodes in the system. The randomized approach used here for local view by sampling random nodes in them, and it is used to eliminate the malicious nodes information in the local view. It entirely based on the fail-stop signature scheme, and it can identify the malicious nodes efficiently in active environments.

IV. A SURVEY OF DOS ATTACKS

Darwish et al. (2017)[23]proposed an authentication protocol for identifying and detecting DoS attacks, which considered as the most significant threats in the cloud computing. Since the cloud architecture is unique, the methods used for detecting and preventing DoS attacks are different than the other traditional methods. DoS attackers mainly focused on the authentication protocol, due to, it is well-thought-out as the gateway for retrieving the cloud resources and hence proposed a cloud-based authentication protocol which concentrates on verifying and authenticating cloud users. The authentication protocol can also do prevention against DoS attacks. Arjunan et al. (2017)[24]discussed the vulnerabilities in existing implementations of virtualization because it is the primary enabler of Cloud computing and also the security issues regarding the cloud computing. Then the framework to identify intrusions at the virtual network layer of Cloud is discussed. Different signature and anomaly-based methods used to discover possible attacks, naïve-Bayes, decision tree, random forest, other trees and linear discriminate analysis for efficient and effective detection of intrusions and used Dempster-Shafer theory (DST) for final decision making, evaluated the feasibility of the classifiers for malicious identification in Cloud through offline simulation using different intrusion datasets. D. Zissis et al. (2012)[25]stated that DoS attackers usually target the service providers, acting like authenticated user which is noticeable by everyone. By giving enormous request to the server, dumping the service queue, and making a traffic jam in the service providing a route, DoS creating harm to server one who is responsible for service providing. The main aim of the DoS attack is to attack the central server. Some of the DoS attack's categories are bandwidth attacks, limitation exploitation attacks, connectivity attacks, data corruption attacks, resource exhaustion attacks, process disruption, and physical disruption. The following Table-3 shows the list of DoS attacks happening in the layer and the protocols.

Table-3: DoS Attacks, Layer, and Protocol .

Attacks	Layer	Protocols
Volume/Bandwidth based attacks	Network	UDP,ICMP
Protocol Attacks	Network	All Routing Protocols
Application Layer Attack	Application	HTTP,TCP/IP

Tan et al. (2011)[26]said, when the number of DoS attacks increased then it degrades the network reliability and accessibility. Hence, it is essential to design and implement an efficient technique for DoS attacks. One of the global attack reports presented a status of the DoS attack[27]isincreased up to 47% in 2014 compared with 2013. From the comparison results, it concluded that the DoS attack is directly affected 13% in application level and 87% in infrastructure level.

Table-4 shows some of the tools that can be used to perform DoS attacks.

Table-4: Tools Used for DoS Attacks

Tools	Layer	Protocols
Namesy	Windows	TCP
Land and Latierra	Network	TCP-IP
Blast	Transport	UDP
Panther	Transport & Network	UDP
Botnets	Network	UDP, TCP-IP

Jain et al. (2011)[28] classified the DoS attack based on the weakness of vulnerability and flood attack. Some of the attacks like Neptune, LAND, death, and ping are vulnerability attacks, whereas spoofing and SYN Flag attacks are flood attacks. From the analyzation of all the attacks, it concluded that all the packets have the information about source and destination and the victim machine assumes it is sending the packets by itself and crash the computer.

Chonka et al. (2011)[29] described various types of HTTP and XML attacks in the cloud computing environment. These types of attack are easy to deploy, but it is too difficult to stop. In other words, it is tedious to provide security in the cloud against these types of attack. The XML attacks and the solution for this attack called cloud-trace-back (CTB) is developed. Aback propagation neural network called cloud protector to discover the cause of these attacks which is used to identify and eliminate this type of traffic attacks. From the experimental results, and also described about the source of the attack within a lesser time interval. Lo et al. (2010)[30] illustrated about DoS/DDoS in the cloud environment and the security issues regarding these attacks. Also, it described as a framework of cooperative intrusion detection system used to decrease the effect of DoS/DDoS attacks. In this system, the cloud computing area, exchange their messages with one another, there is a cooperative agent in the method utilized for determining whether the messages sent from the IDS system or not. Thus, this IDS system eliminated this type of DoS/DDoS attacks. The experimental results show that it easily rejects the DoS attack and needs to reduce computational complexity. Cheng et al. (2002)[31] proposed a method as a spectral analysis for identifying the TCP traffic called Defense against denial of service (DAD) attack. Thus, the approach decreases the false positives of the malicious detection and also reduces the related unwanted slowdown the process or blocking of authenticated traffic. In DAD method the packet flow rate is assigned as a constant based on the time interval and considered as a signal for spectral analysis. If the signal density reduced, then there will be a lack off and decreased the periodic range. Later the attack is identified, and the signal strength is revealed by itself with the help of spectral analysis. Hence it is clear that DAD used for traffic analysis-based DoS attack detection.

V. A SURVEY OF DDOS ATTACKS

Somani et al. (2017)[32]discussed the issues with different vendors in a cloud environment. To provide a strong safety and reliability DDoS attacks to be diminished since it is one of the essential and most substantial attacks faced by more number of cloud users. DDoS attacks aim at the resources as the target, and it degrades the performance and ability of the cloud infrastructure. Methods used to prevent DDoS attacks are merely different than the traditional network approaches. Some of the challenges which affect the expenses of cloud, managing the resource, and quality of service explained here. One of the severe attack concerning in the cloud is the Distributed Denial of Service (DDoS) attack. Also proposed the solution for escaping from the DDoS attack in the cloud and given a survey illustrating the description, avoidance, discovery, and improvement mechanisms of these attacks. Ideal automatic analyzing decisions, multilevel enhancement, and protection using deep resources in the cloud are a few of the significant necessities of the ideal solutions proposed here. The suitable solutions for the development of preventing the DDoS attack with effective resource management discussed. The detailed explanation about the DDoS attacks and the answers to avoid and different metrics to evaluate for the performance analysis by concerning the traditional IT environment explained in detail. It is shown that EDoS attack is the prior form of DDoS attacks in the cloud. Some of the contributions of the solution to the DDoS attack in particular feature such as resource allotment, on-demand resources, cloud discovery, and network reconfiguration using SDNs and offered a thorough instruction for efficient plan. It provides an absolute analysis of explanation gap and parameters to support upcoming defense mechanisms. Darwish et al. (2013)[33] presented a detailed analysis report on DDoS security solutions in a cloud environment. The DDoS detection mechanisms mainly used learning algorithms. Most of the research works focused on introducing protection algorithms for cloud infrastructure and anomaly detection on the public as well as the private cloud. The proposed DDoS attack generation system has three different main components such as designing the scenario, identifying the attack is software based or hardware based and the strength of the offense by analyzing the attack parameters. Some of the important metrics used in performance computation are a memory, CPU, packet loss, latency, and throughput and link usage. From the implementation output, it concluded that the proposed DDoS security solution model applies to private or public clouds.Devi et al. (2016)[34] illustrated the merits and demerits of the cloud computing environment. Various kinds of attacks in the cloud in a specific type of cloud architecture discussed here. In the three layers of service in the cloud are IaaS, PaaS, SaaS, in that if IaaS initially affected means, then the other layers cannot be secured. Like image sharing attack in virtualization in the IaaS layer and all the other attacks and its solutions also discussed elaborately.In this, the author proposed the virtualization method to protect the cloud from a malicious attack by providing the digital signatures and the public, private keys for all VMs. Hence each message passed by hypervisor will be digitally signed so that no alterations can be done and will also have a message digest. Encryption is used to secure data so that even if malicious VM takes data, it can't decrypt by another VM.

Regarding security in the cloud on VMs virtualization attacks like VM isolation violation, VM migration, VM escape, etc. in the cloud computing environment and the prevent based supervised learning system analyzed.

Shamsolmoali et al. (2014)[35] described the DDoS attack creates the harm the resources and access the resources without authentication. But providing a protective system for the cloud environment is the complicated process because of the enormous storage. A statistical method to sense and filter DDOS attacks which need little storage and ability of quick finding proposed. In this method, the high Detection accuracy achieved with less Time consumption. This method is called as Cloud Confidence DDoS Filtering which is easy to set up and needs less storage.

In this approach, used two levels of filtering to identify the attackers –initially the header file is taken from the incoming packets, second, it matches up to the value of TTL with the stored value in the IP2HC table. If it is not equivalent, the packet spoofed, and the system drops it. The result shows that the overall performance of this algorithm in detection accuracy and time consumption is superior to existing models.

Regarding DDoS attacks, various detection strategies such as detection [36-45], mitigation [46-54] and Defence techniques [55-66] proposed for the cloud, and the performance compared. The comparative analysis based on the above said categories are given in Table-5, Table-6, and Table-7.

Table-5: Tools Used for DDoS

Tools Used for DDoS	Protocol	Layer
Trinoo	UDP	Transport
Tribe Flood	UDP, TCP SYN	Network & Transport
Mstream	TCP ACK	Transport
Trinity	TCP RST, TCP Fragment	Transport
Knight	UDP, SYN	Transport
Low Orbit Ion Cannon	TCP, UDP, HTTP	Transport& Application
High Orbit Ion Cannon	HTTP	Application

Table-6: DDoS Detection Methods

Technique	Layer	Tools	Dataset
Forensic Method	Network	NA	CNSMS
Filtering	Network	Attack tools	MA WI Traffic Archive
Intrusion Detection	Network	NA	NA
Multistage Anomaly Detection	Network	NA	NA
DIDS	Network	NA	NA
Securing Cloud Servers	Network	Ns2	Simulation

Table-7: DDoS Mitigation Methods

Technique	Layer	Tools	Dataset
Cloud Enabled DDoS Defence	Application	JavaScript	Real time from planet lab
Mitigating DDoS attacks	Application	Curl Loader	Simulation
Hybrid Cloud Based Firewalling	Network	NA	Virtual
Enhanced Economical Denial of Sustainability	Network	NA	Virtual
EDoS	Application & Network	NA	Virtual
EDoS – Shield	Application	Discrete Simulation	Virtual

From the above tables, it understands that the dataset is also collected from various data sources and pre-processed before feed into the learning model. The learning model learns data initially and analyzes the data using multiple prediction methods to obtain regular or malicious with lesser % of false alarm to improve the accuracy of the prediction pattern matching and filtering methods used.

Even though the accuracy is improved using the knowledge base analysis, from the Table-5 to 8, it is evident that DDoS attack in the cloud can be mitigated using various kinds of methods such as detection, mitigation, and Defense methods. Also, it is evident that in recent days most of the ways are focusing on providing a prevention technique for DoS and DDoS attacks.

Table-8: DDoS Defense Methods

Technique	Layer	Tools	Dataset
Simulation Study	Network	OMNet, Zoness and SNMP	Simulated
TorWard	Network & Transport	Opensource IDS Suricata, Barnyard2, BASE, ETPro, ETOpen	Real time from Planetlab
Securing Cloud	Network	Snort, VMware, honeypot	Virtual
Securing Cloud Computing	Network	NA	DARPA
Comber Approach	Application	NA	Virtual
Cloud Security Defence	Application	Tshark, tcpdump, VB.Net	Virtual

VI. A SURVEY OF EDOS ATTACKS

One of the sub domains from DDoS is Economic DoS (EDoS) attack which should be identified and detected in the cloud, said by Somani et al. (2017)[67].The schematic diagram of the EDoS attack is illustrated in Figure-3.

The author presented a detailed survey about the classification, anticipation, detection and extenuation mechanisms of these attacks. Taxonomy is provided to make the reader understand various classes of methods used for different contributions. From the conclusion, it stated that, a high need of solutions to be designed to keep the utility computing models in mind. Some of the developed solutions in earlier days are true auto-scaling, a defense based profound resources and multi-layer-based mitigation, considered as desired solutions. Finally, the author provided a specific protocol for building a practical solution with the detailed requirements for designing defense methods. Al-Haidari et al. (2015)[68]said that EDoS is considered as one of single class service and presented the impacts of EDoS attacks in cloud computing. Then designed an analytical model based on the queuing model to capture the cloud services and the performance metrics such as E-2-E response time, resource utilization, cost, and throughput. Also these results verified using a simulation-based experiment.

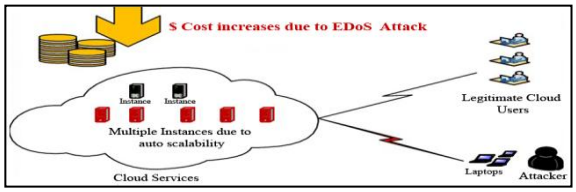

Fig-3: EDoS Attack Scenario

Sood et al. (2016)[69] discussed various computing layers with the architecture and the security issues. Cloud computing is defined based on the remote servers, data to be processed, store and manage, and the local server of the network. During data transmission in the cloud, various hazardous attacks created on the cloud, and it mainly affects the data or resources. One of the standard attacks is Packet Flooding attach, and it leads economic degrades. EDoS is a kind of packet flood attack changes the resource and does high damage. Singh et al. (2014)[70] discussed EDoS attacks in the cloud. The resources are dynamically scaled and check the setup of the resources into the server to prevent the EDoS. Also, the author provided a review of different EDoS mitigation methods proposed in recent earlier researches.

Though, there are large numbers of methods/techniques and tools has been proposed by the lot of researchers in the cloud environment for eliminating and controlling the DoS/DDoS attacks, most of the methods described only theoretically. Few of them were experimentally proved their efficiency and explained below.

VII. EXPERIMENTAL RESULTS BASED COMPARISON (DOS/DDOS)

Some of the methods proposed in earlier research works experimentally investigated, and their performance evaluated regarding Memory Usage, CPU utilization, Accuracy, and Execution time. The following tables 9 & 10 show that the experimental results obtained from [26, 30-31, 71] for analyzing and detecting DoS attacks. It describes the comparative analysis of various IDS methods and their performance on DoS attack.

Each method and the mechanism used for core function and their performance regarding memory usage and CPU usage are given in the table. From the Table - 9 it is understood that the memory and CPU utilization is increased after the attack than the before the attack. From the Table – 10, it is to realize that Netwag tool provided the best accuracy in detecting the malicious attack when compared to others, but the execution time is more.

NIDS method offered the accuracy and execution time moderately for the various datasets with three test cases. Dou et al. (2013)[37], Chonka et al. (2011)[29] offered the accuracy nearly 98% and above. These methods had given the better accuracy but the execution time is little more when compared to others. By considering both accuracy and execution time, Netwag tool with RF classifier provided the 98.9% accuracy in 0.4 ms execution time. Hence, this method is very suitable for detecting the attacks with the highest accuracy with lesser execution time.

Table-9: Performance Comparison regarding Memory and CPU Utilization

Systems	Detection Mechanism	Before Malicious Act		After Malicious Act		After Prevention	
		Memory Usage in MB	CPU Usage in %	Memory Usage in MB	CPU Usage in %	Memory Usage in MB	CPU Usage in %
Cooperative IDS [30]	Signature	671	9	673	10	665	7
DoS Detection [26]	Anomaly	689	10	692	10	676	6
Hybrid IDS [71]	DM and ML	721	7	724	8	701	8
Two Stage Hybrid IDS [72]	Signature and Anomaly	709	10	721	12	698	8
Authentication Protocol [23]	User ID Verification	693	11	705	15	680	8

Cloud Trace Back[29]	Identity Verification	743	13	750	18	731	10

Table-10: Performance Comparison regarding Accuracy and Execution time

Method	Training Dataset	Testing Dataset	Accuracy (%)			Execution Time (Sec)		
			Case - 1	Case – 2	Case - 3	Case - 1	Case - 2	Case - 3
NIDS[24]	KDD99(10%) training dataset	KDD99(10%) test dataset	92.55	92.63	94.75	1.246	2.14	3.539
	NSLKDD training dataset	NSLKDD test dataset	74.51	75.96	82.83	0.231	0.329	0.7366
	Booter 1 training dataset	Booter 1 test dataset	90.73	95.51	99.97	0.093	0.167	0.171
	Botnet training dataset	Botnet test dataset	89.95	91.46	94.47	0.0244	0.274	0.0303
			Accuracy (%)			Execution Time (Sec)		
NETWAG Tool[45]	-	-	Ripper	RF	PART	Ripper	RF	PART
	-	-	99.2	98.9	97.8	4.61	0.4	0.34
			Accuracy (%)			Execution Time (Sec)		
Devi et al.[34]	-	-	98			4.1		
Dou et al.[37]	-	-	98.7			4.6		
Chonka et al. [29]	-	-	99			6.1		

VIII. SUMMARY AND CONCLUSION

The primary objective of this work is to learn and understand various methods, techniques and tools used for detecting and preventing DoS, DDoS and EDoS attacks in cloud computing environment. One of the objectives is to know the issues and challenges faced by the earlier research works based on the tools and the attack, whereas it helps to determine the problem statement of the research work and able to design a novel method for identifying, detecting and preventing various malicious attacks in cloud computing. The DDoS attack considered as the primary category of the DoS attack and it plays a fundamental role while taking into consideration the cloud computing model. The cloud computing is a loosely coupled system and it can be easily affected by any malicious attacks. In this a detailed survey presented, and it discussed various DoS, DDoS and EDoS attacks and their impacts including multiple methodologies to detect or to identify those attacks. It analyzed that the essential information about numerous types of attacks, effects, various kinds of attackers and their origin. A broad, comprehensive study provided for DoS, DDoS and EDoS with Defense solutions in the cloud computing environment. It will be beneficial for upcoming researchers by providing guidance about the attacks and the various Defense mechanisms and directions to avoid the above-said attacks.

There are an enormous number of solutions provided by various earlier researchers targeted to prevent, detect and mitigate. From the survey, it is carried out and analyzed that some of the researchers in this field, obtained the detection of attacks up to 98%, some works obtained 97% of mitigation but the prevention of the attacks yet to be improved much more. Among the various solutions, it analyzed that prevention mechanisms in the cloud security need to develop. The complete view of the different attacks and defense mechanisms with multiple metrics and methods are described here. This detailed survey offers the necessary information about the DoS/DDoS/EDoS attacks and their complete arrangements. From this, there is a chance for researchers to innovate various novel mechanisms to prevent and avoid those attacks with high accuracy. In this survey, differentiated the multiple types of attacks, their source, the impacts, prevention mechanisms and the practical solutions in a more significant level in the cloud environment are discussed.

Security is the biggest concern in the cloud environment; the traditional methods for Dos/DDoS attacks are not suitable for the impact of attackers in recent days. So there is a need for multilevel solutions mainly designed for the cloud security with less cost, high accuracy, less execution time and primarily to prevent. For both service providers and consumers there is a need for security requirements with different levels of map security. "Prevention is better than cure" likewise supervised learning methods are essential to alert the system for any suspicious activity before occurring in the cloud. Secured data management needed necessary in the cloud for improving the efficiency to provide the trusted cloud environment. It is an open challenge to the various researchers to provide better security in the cloud, and there is a need for innovative methods and techniques to prevent the multiple types of attacks in the cloud.

REFERENCES

1. Hassan Takabi, James B.D. Joshi, Gail Joon Ahn, "Cloud Computing Security and Privacy Challenges in Cloud Computing Environments", The IEEE Computer and Reliability Societies, Volume. 8,Issue. 6, pp. 24-31, 2010, doi. 10.1109/MSP.2010.186.
2. Mahesh U. Shankarwar, Ambika V. Pawar, "Security and Privacy in Cloud Computing: A Survey", Advances in Intelligent Systems and Computing - Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications, Volume. 328, Issue. 1, pp. 1-11, 2014, doi.10.1007/978-3-319-12012-6_1.
3. Mandia, Kevin, Prosise. C, "Incident Response: Investigating Computer Crime", Berkeley: Osborne - McGraw-Hill, Volume. 328, Issue. 1, pp. 360-361. 2001, ISBN 10: 0072131829.
4. Deshpande H. A, "Honey Mesh: Preventing Distributed Denial of Service Attacks using Virtualized Honeypots", International Journal of Engineering Research and Technology, Volume. 4, Issue. 8, pp. 263-267, 2015, doi. 10.17577/IJERTV4ISO80325.
5. Deepak Lal. K. B, "Fuzzy Keyword Search Over Encrypted Data in Multicloud", Discovery, Volume. 21,Issue. 67, pp. 71-77, 2014, doi.10.1.1.589.6785.
6. Boss. G, Malladi. P, Quan. D, Legregni. L, Hall. H, "Cloud Computing", IBM White Paper, 2007.
7. Whyman. B, "Cloud Computing", Information Security and Privacy Advisory Board, pp. 11–13, 2008.
8. Heiser. J, "What You Need to Know about Cloud Computing Security and Compliance", Gartner, 2009, Online. Available: http://www.gartner.com/it/page.jspid=G00168345.
9. Keiko. H, David. G R, Eduardo. F.M, Eduardo. B.F, "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, Volume. 4, Issue. 1, pp. 5-18, 2010, doi. 10.1186/1869-0238-4-5.
10. Subashini. S, Kavitha. V, "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Network and Computer Applications, Volume. 34, Issue. 1, pp. 1-11, 2011, doi. 10.1016/j.jnca.2010.07.006.
11. Nidal M. Turab, Anas Abu TalebShadi R. Masadeh, "Cloud Computing Challenges and Solutions", International Journal of Computer Networks & Communications, Volume.5, Issue.5, pp. 209-216, 2013, doi. 10.5121/ijcnc.2013.5515.
12. Australian Government Department of Defense Intelligence and Security, "Cloud Computing Security Considerations", Cyber Security Operations Centre, pp. 1-18, 2012.
13. Harshitha. K. Raj, "A Survey on Cloud Computing ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume. 4, Issue. 7, pp. 352-357, 2014, ISSN. 2277 128X.
14. Mohammed A. AlZain, Ben Soh, Eric Pardede, "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", Journal of Software, Volume. 8, Issue. 5, pp. 1068-1078, 2013, doi. 10.4304/jsw.8.5.
15. Meenu Bhati, Puneet Rani, "Review of Passive Security Measure on Trusted Cloud Computing", International Journal of Scientific Engineering and Applied Science Volume. 1, Issue. 3, pp. 551-556, 2015, ISSN. 2395-3470.
16. Almorsy. M, Grundy. J, Müller. I, "An Analysis of the Cloud Computing Security Problem", Cornell University Library, pp. 1-6, 2016, Cite. 1609.01107.
17. Singh. A, Shrivastava. M, "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology, Volume. 1, Issue. 4, pp. 321-323, 2012, ISSN. 2277-3754.
18. Chouhan. P. K, Yao. F, and Sezers S,"Software as a Service: Understanding Security Issues", Science and Information Conference IEEE, pp. 162-170, 2015, doi. 10.1109/SAI.2015.7237140.
19. Singh. J, "Comprehensive Solution to Mitigate the Cyber-Attacks in Cloud Computing", International Journal of Cyber-Security and Digital Forensics, Volume. 3, Issue. 2, pp. 84-92, 2014,doi. 10.17781/P001294.
20. Jitendra Singh, Ashish Jha, "Cloud Storage, Issues and Solutions", International Journal of Engineering and Computer Science, Volume. 3, Issue. 4, pp. 5499-5506, 2014, ISSN. 2319-7242.
21. Khan. M. A, "A Survey of Security Issues for Cloud Computing", Journal of Network and Computer Applications", Volume.71, Issue.3, pp.11-29, 2016, doi. 10.1016/j.jnca.2016.05.010.
22. Lim. J, Yu. H, Gil. J. M, "Detecting Sybil Attacks in Cloud Computing Environments Based on Fail-Stop Signature", Symmetry, Volume. 9, Issue. 3, pp. 35-47, 2017, doi. 10.3390/sym9030035.
23. Darwish. M, Ouda. A, Capretz. L. F, "Formal Analysis of an Authentication Protocol against External Cloud-Based Denial-of-Service (DoS) Attack",International Journal for Information Security Research, Volume. 3, Issue.1 / 2, pp. 400-407, 2017,Cite. arXiv:1711.09985.
24. Arjunan. K, and Modi. C. N, "An Enhanced Intrusion Detection Framework for Securing Network Layer of Cloud Computing", IEEE ISEA Asia Security and Privacy, pp. 1-10, 2017, doi. 10.1109/ISEASP.2017.7976988.
25. Zissis. D, Lekkas. D, "Addressing Cloud Computing Security Issues", Future Generation Computer System, Volume. 28, Issue. 3, pp. 583-592, 2012, doi.10.1016/j.future.2010.12.006.
26. Tan. Z, Jamdagni. A, He. X, Nanda. P, Liu. R.P, "Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", Neural Information Processing, Springer, pp. 756-765, 2011, doi. 10.1145/2490428.2490450.
27. Acunetix, "Analysis of an Intrusion: DOS Attack", 2014.
28. Jain. P, Jain. J, Gupta. Z, "Mitigation of Denial of Service (DoS) Attack", International Journal of Computational Engineering and Management, Volume. 11, Issue. 1, pp. 38-44, 2011, ISSN. 2230-7893.
29. Chonka. A, Xiang. Y, Zhou. W, Bonti. A, "Cloud Security Defence to Protect Cloud Computing Against HTTP-DoS and XML-DoS Attacks", Journal of Network and Computer Applications, Volume.34, Issue. 4, pp. 1097-1107, 2011, doi. 10.1016/j.jnca.2010.06.004.
30. Lo. C. C, Huang. C. C, Ku. J, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", In Parallel Processing Workshops 39th International Conference on IEEE, Volume. 1, Issue. 1, pp. 280-284, 2010, doi. 10.1109/ICPPW.2010.46.
31. Cheng. C. M, Kung, H. T, Tan. K. S, "Use of Spectral Analysis in Defence against DoS Attacks", In Global Telecommunications Conference IEEE, Volume. 3, Issue.1, pp. 2143-214), 2002, doi. 10.1109/GLOCOM.2002.1189011.
32. Somani. G, Gaur. M. S, Sanghi. D, Conti. M, Buyya. R, "DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", Computer Communications, Volume. 107, Issue. 1, pp. 30-48, 2017, doi. 10.1016/j.comcom.2017.03.010.
33. Darwish. M, Ouda. A, Capretz. L. F, "Cloud-Based DDoS Attacks and Defenses", International Conference on Information Society IEEE, pp. 67-71, 2013, Cited. arXiv:1511.08839.
34. Devi. B. K, Subbulakshmi. T, "A Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment", Indian Journal of Science and Technology, Volume. 9, Issue. 34, pp. 1-7, 2016, doi. 7485/ijst/2016/v9i34/93175.
35. Shamsolmoali. P, Zareapoor. M, "Statistical-Based Filtering System against DDoS Attacks in Cloud Computing", Advances in Computing, Communications and Informatics International Conference on IEEE, pp. 1234-1239, 2014, doi. 10.1109/ICACCI.2014.6968282.
36. Chen. Z, Han. F, Cao. J, Jiang. X, Chen. S, "Cloud Computing Based Forensic Analysis for the Collaborative Network Security Management System", Tsinghua Science and Technology, Volume. 18, Issue. 1, pp. 40-50, 2013, ISSN. 1007-0214.
37. Dou. W, Chen. Q, Chen. J, "A Confidence-Based Filtering Method for DDoS Attack Defense in a Cloud Environment", Future Generation Computer Systems, Volume. 29, Issue. 7, pp. 1838-1850, 2013, doi. 10.1016/j.future.2012.12.011.
38. Wei. W, Chen. F, Xia. Y, Jin.G, "A Rank Correlation-Based Detection against Distributed Reflection DoS Attacks", IEEE Communications Letters, Volume. 17, Issue. 1, pp. 173-175, 2013, doi. 10.1109/LCOMM.2012.121912.122257.
39. Tan. Z, Nagar. U. T, He. X, Nanda. P, Liu. R. P, Wang. S, Hu. J,"Enhancing Big Data Security With Collaborative Intrusion Detection", IEEE Cloud Computing,Volume. 1, Issue. 3, pp.27-33, 2014, doi.: 10.1109/MCC.2014.53.
40. Cha. B, Kim. J, "Study of Multistage Anomaly Detection for Secured Cloud Computing Resources in Future Internet", IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC) USA, Volume. 12, pp. 1046-1050, 2011, doi.10.1109/DASC.2011.171.
41. Li. H, Wu. Q, "A Distributed Intrusion Detection Model Based on Cloud Theory", IEEE 2nd International Conference on Cloud Computing and Intelligent Systems, Volume. 1, Issue. 1, pp. 435-439, 2012, doi.10.1109/CCIS.2012.6664443.
42. Chapade. S.S, Pandey. K.U, Bhade D.S, "Securing Cloud Servers Against Flooding-Based DDoS Attacks", International Conference on Communication Systems and Network Technologies, pp.

524-528, 2013, doi. 10.1109/CSNT.2013.114.
43. Aishwarya. R, Malliga. S, "Intrusion Detection System - An Efficient Way to Thwart Against DoS/DDoS Attack in the Cloud Environment", International Conference on Recent Trends in Information Technology IEEE, Volume. 1, Issue. 1, pp. 1-6, 2014, doi. 10.1109/ICRTIT.2014.6996163.
44. Maqsood.R, Shahabuddin. N, Upadhyay. D, "A Scheme for Detecting Intrusions and Minimizing Data Loss in Virtual Networks", International Conference on Computational Intelligence and Communication Networks IEEE, Volume. 1, Issue. 1, pp. 738-743, 2014, doi. 10.1109/CICN.2014.160.
45. Shamsolmoali. P, Zareapoor. M, "Statistical-Based Filtering System Against DDOS Attacks in Cloud Computing", International Conference on Advances in Computing, Communications, and Informatics IEEE, pp. 1234-1239, 2014, doi. 10.1109/ICACCI.2014.6968282.
46. Jia. Q, Wang. H, Fleck. D, Li. F, Stavrou.A, Powell. W, "Catch Me If You Can: A Cloud-Enabled DDoS Defense", IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 264-275, 2014, doi. 10.1109/DSN.2014.35.
47. Al-Haidari. F, Sqalli. MH, Salah. K, "Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses", IEEE International Conference on Trust, Security, and Privacy in Computing and Communications, pp. 1167-1174, 2012, doi. 10.1109/TrustCom.2012.146.
48. Lua. R, Yow. K.C, "Mitigating DDoS Attacks With Transparent and Intelligent Fast-Flux Swarm Network", IEEE Network, Volume. 25, Issue. 4, pp. 28–33, 2011, doi. 10.1109/MNET.2011.5958005.
49. Yan. Q, Yu. F, "Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing", IEEE Communications Magazine, Volume. 53, Issue. 4, pp. 52-59, 2015, doi. 10.1109/MCOM.2015.7081075.
50. Guenane. F.A, Jaafar. B, Noguciera. M, Pujolle. G, "Autonomous Architecture for Managing Firewalling Cloud-Based Service", International Conference and Workshop on the Network of the Future, pp. 1-5, 2014, doi. 10.1109/NOF.2014.7119774.
51. Kumar. M.N, Sujatha. P, Kalva. V, Nagori. R, Katukojwala. A.K, Kumar. M, "Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing Using In-Cloud Scrubber Service", International Conference on Computational Intelligence and Communication Networks, pp. 535-539, 2012, doi. 10.1109/CICN.2012.149.
52. Guenane. F, Nogueira. M, Pujolle. G, "Reducing DDoS Attacks Impact Using a Hybrid Cloud-Based Firewalling Architecture", Global Information Infrastructure and Networking Symposium, pp. 1-6, 2014, doi. 10.1109/GIIS.2014.6934276.
53. Alosaimi. W, Al-Begain. K, "An Enhanced Economical Denial of Sustainability Mitigation System for the Cloud", International Conference on Next Generation Mobile Apps, Services and Technologies, pp. 19-25, 2013, doi. 10.1109/NGMAST.2013.13.
54. Sqalli. M.H, Al-Haidari. F, Salah. K, "EDoS-Shield-a Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing", IEEE International Conference on Utility and Cloud Computing, pp. 49-56, 2011, doi. 10.1109/UCC.2011.17.
55. Chung. C.J, Khatkar. P, Xing. T, Lee. J, Huang. D, "NICE: Network Intrusion Detection and Counter Measure Selection in Virtual Network Systems", IEEE Transactions on Dependable and Secure Computing, Volume. 10, Issue. 4, pp. 198-211, 2013, doi. 10.1109/TDSC.2013.8.
56. Anwar. Z, Malik. A.W, "Can a DDoS Attack Meltdown My Data Center? A Simulation Study and Defense Strategies", IEEE Communications Letters, Volume. 18, Issue. 7, pp. 1175-1178, 2014, doi. 10.1109/LCOMM.2014.2328587.
57. Ling. Z, Luo. J, Wu. K, Yu. W, Fu. X, "TorWard: Discovery, Blocking, and Traceback of Malicious Traffic Over tor", IEEE Transactions on Information Forensics and Security, Volume. 10, Issue. 12, pp. 2515-2530, 2015, doi. 10.1109/TIFS.2015.2465934.
58. Choi. J, Choi. C, Ko. B, Kim. P, "A Method of DDoS Attack Detection Using HTTP Packet Pattern and Rule Engine in Cloud Computing Environment", Soft Computing - A Fusion of Foundations, Methodologies and Applications, Volume. 18, Issue. 9, pp. 1697-1703, 2014, doi. 10.1007/s00500-014-1250-8.
59. Arshad. J, Townend. P, Xu. J, "A Novel Intrusion Severity Analysis Approach for Clouds", Future Generation Computer Systems, Volume. 29, Issue. 1, pp. 416-428, 2013, doi. 10.1016/j.future.2011.08.009.
60. Bakshi. A, Yogesh. B, "Securing Cloud from DDoS Attacks Using Intrusion Detection System in Virtual Machine", International Conference on Communication Software and Networks, pp. 260-264, 2010, doi. 10.1109/ICCSN.2010.56.
61. Chen. Q, Lin. W, Dou. W, Yu. S, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment", IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 427-434, 2011, doi. 10.1109/DASC.2011.86.
62. Joshi. B, Vijayan. A.S, Joshi. B.K, "Securing Cloud Computing Environment against DDoS Attacks", International Conference on Computer Communication and Informatics, pp. 1-5, 2012, doi. 10.1109/ICCCI.2012.6158817.
63. Karnwal. T, Sivakumar. T, Aghila. G, "A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack", IEEE Students Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012, doi. 10.1109/SCEECS.2012.6184829.
64. Anitha. E, Malliga. S, "A Packet Marking Approach To Protect Cloud Environment Against DDoS Attacks", IEEE International Conference on Information Communication and Embedded Systems, pp. 367-370, 2013, doi. 10.1109/ICICES.2013.6508330.
65. Hong. J.B, Kim. D.S, "Assessing the Effectiveness of Moving Target Defenses Using Security Models", IEEE Transactions on Dependable and Secure Computing, Volume. 13, Issue. 2, pp. 163–177, 2016, doi. 10.1109/TDSC.2015.2443790.
66. Chonka. A, Xiang. Y, Zhou. W, Bonti. A, "Cloud Security Defence to Protect Cloud Computing against HTTP-DoS and XML-DoS Attacks", Journal of Network and Computer Applications, Volume. 34, Issue. 4, pp. 1097-1107, 2011, doi. 10.1016/j.jnca.2010.06.004.
67. Somani. G, Gaur. M. S, Sanghi. D, Conti. M, Buyya. R, "DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", Computer Communications, Volume. 107, pp. 30-48, 2017, doi. 10.1016/j.comcom.2017.03.010.
68. Al-Haidari. F, Sqalli. M, Salah. K, "Evaluation of the Impact of EDoS Attacks Against Cloud Computing Services", Arabian Journal for Science and Engineering, Volume. 40, Issue. 3, pp. 773-785, 2015, doi. 10.1007/s13369-014-1548-y.
69. Sood. R, Garg. S, Palta. P, "A Novel Approach to Data Filtration Against Packet Flooded Attacks in Cloud Service", Journal of Network Communications and Emerging Technologies, Volume. 6, Issue. 5, pp. 37-41, 2016, ISSN: 2395 -5317.
70. Singh. P, Manickam. S, Rehman. S. U, "A Survey of Mitigation Techniques Against Economic Denial of Sustainability (EDoS) Attack on Cloud Computing Architecture", IEEE International Conference on Reliability, Infocom Technologies and Optimization, pp. 1-4, 2014.
71. Malik. A.J, Shahzad. W, Khan. F.A, "Network Intrusion Detection Using Hybrid Binary PSO and Random Forests Algorithm", Security and Communication Networks, Volume. 8, Issue. 16, pp. 2646-2660, 2015, doi. 10.1002/sec.508.
72. Hussain. J, Lalmuanawma. S, Chhakchhuak. L, "A Novel Network Intrusion Detection System Using Two-Stage Hybrid Classification Technique", International Journal of Computer & Communication Engineering Research, Volume. 3, Issue. 2, pp. 16-27, 2015, ISSN. 2321-4198.

AUTHORS PROFILE

M. Mayuranathan has Completed B.E Computer science from Periyar University in the year 2002. M.Tech in Computer Science and Engineering from SRM University, Chennai in the year 2005. Currently working as a Assistant Professor (Senior Grade) in Department of CSE at Valliammai Engineering College, Chennai. His research interests are Image Processing, Security etc.. He is Life member of ISTE, ISC. He is having 14 years of teaching experience.

Dr. M. Murugan was born on 21st April 1968, graduated in Electronics & Communication Engineering from the University of Madras in April 1989, received his Masters in Electronics & Telecom Engineering (Spl.:Microwave) and Ph.D. from the University of Pune in May 2001 and July 2010 respectively. He has over 29 years of experience in teaching the Under Graduate and Post Graduate Students in the specialized fields of Microwave, Antennas, Optical Communication Satellite Communication and EMI&C. He is a Fellow of IETE and Member of ISTE, IEI, ISOI, SEMCEI, SSI, CSI and ISCA. In his credit, he has over One Hundred papers published in National/ International repute Conferences /Journals. He was the Convener of two National Conferences, Co-Convener of one National Conference and one National Level Seminar & Chief Coordinator of two AICTE-ISTE approved Short Term Training Programs.

Professor M. Murugan Authored Four text books entitled "Mobile Communication System", "Communication Systems", "Optical & Microwave Communication" and 'Wave Theory & Antenna' for Diploma & Degree level students. He is an approved P.G./ Ph. D. Supervisor of the Anna University, Chennai and Sathyabhama University, Chennai.
Currently he is guiding eight research candidates and has reviewed Ph.D Thesis of many Universities, in addition to reviewing papers for Conferences. Currently, he is serving as Editor in Chief of i-manager's Journal of Wireless Communication and Networks. He has also delivered Several Expert Lectures on various topics for the Students and Staffs. He has also served as Session Chair of few Conferences held in India.

Dr.V.Dhanakoti has Completed Masters in Computer Application from the University of Madras in the year 1999 and Completed M.E in CSE from Sathyabhama University in the year 2005. He successfully completed his research from Anna University, Chennai in the year 2013. He is life member of ISTE, CSI, IAENG, IACSIT and Senior Member of UACEE, SDWC. He has published around 13 International Journals and 10 International Conferences.