



Theoretical Framework of TCP SYN Flood DDoS attack Detection Mechanism using Spoofed IP in Cloud Environment

Dr. Durairaj.M¹, Manimaran.A²

School of Computer Science Engineering and Applications,
Bharathidasan University, Trichirappalli, Tamilnadu, INDIA.

Abstract: Virtualization is a key characteristic of cloud computing to access multiple operating systems in a single physical machine which exploits based on the concept of multi-tenancy. Virtualized Cloud Computing infrastructure network is vulnerable to distributed denial of service (DDoS) attack which makes the resources unavailable for its intended users. As insignificant of DDoS attack, validated users are denied from accessing the cloud services by spoofing authorized client identity (IP Address). Cloud Computing gives importance to protect cloud servers from flooding attacks generated as a result of cloud elastic resource management. When flooding attack occurs in the cloud environment, resource request amplifies drastically and the guest operating system on each virtual machine starts to distribute additional workload. Hence, large numbers of cloud resources are stopped from providing service to the legal users. This paper discusses the virtualization approaches in cloud computing and proposes novel secure cloud framework for detecting DDoS attack by identifying spoofed IP.

Keywords: Cloud Security, DDoS Attack, TCP SYN Flood Attack, IP Spoofing

I. Introduction

Cloud Computing is a category of network based computing that depends on sharing resources on top of a network instead of having local servers to manage applications. Distributed Denial of Service attack occurs in a cloud environment, when multiple systems are flooding the victim server resources [1] [2]. DDoS attacker's objective is to degrade the cloud server's resource capacity and deny the resource to the legal cloud users. Data availability issue is the greatest challenge in distributed cloud environment and the root cause for the data availability issue is DDoS attack [3]. This paper completely discusses the maintenance of data availability in cloud computing environment against DDoS attack.

The most popular method of DDoS attack is TCP SYN flood attack, which makes the victim server resources unavailable to the intended users with the help of large number of forged source IP addresses [4]. TCP protocol establishes the connection between source and destination for the period of TCP three way handshake methods. Attacker sends sequence of SYN request to the victim server to block the server resources. Power of the cloud computing is resource sharing in a distributed environment across the virtual machines [5]. In security aspects, this problem demonstrates the weaknesses of the cloud system due to DDoS attacks [6]. In a private cloud, if one virtual machine is overloaded by flooding attack, then all other virtual machines are affected in a shared environment. TCP SYN flood attacks handle enormous number of data packets by means of fake IP source address in packet header. As a result, victim system gets response from the server even when victim system does not make request to the server, which created numerous half-open connections to consume cloud server resources illegitimately [7]. Cloud war is the extremely dangerous flooding attack scheme under DDoS attack category in which attacker sends request to the victim server successively from multiple source IP address until the entire server resources are utilized [8]. There are three main interfaces involved in these attack criteria; they are Cloud user, Cloud Provider, and Cloud server. Combination of these three interface make six possible ways, such as client to service, service to client, cloud to service, service to cloud, client to cloud, and cloud to client. Numerous tools are available to generate fake IP addresses which make difficult to avoid sending forged IP address as source IP address [9]. It is essential to employ a strong detection mechanism in the cloud server side to find the forged IP addresses and block them [10]. Proposed work primarily concentrates on detecting spoofed IP address and includes it into the blocked list for further IP address comparison. Prior to get request from the valid client or attacker by the virtual cloud server, the proposed detection algorithm identifies the incoming packets whether they are legitimate or spoofed and the legitimate packets are allowed to traverse in the network whereas spoofed packets are dropped.

The rest of the paper is organized as follows. Section II describes the virtualization technologies and its approaches. Section III explains the DDoS attack types and its hierarchical view. Section IV and V discuss the TCP based DDoS attack and DDoS attack detection methods. Section VI present proposed framework design for secure cloud against TCP SYN flood DDoS attack and proposed methodology diagram named as Secure Cloud Authentication System (SCAS). Section VII provides pseudo code for SCAS. Finally the conclusion presented with future work in Section VIII.

II. Virtualization

A. Virtualization Technologies

Virtualization technologies utilize same physical part of the hardware to execute multiple operating system instances or Virtual Machines (VMs) [11]. Each virtual machine functions on its own physical resource with a dedicated operating system called guest operating system. Hypervisor enables hardware resource sharing among virtual machines [12]. Virtualization approaches are classified as Application based virtualization, Operating system based virtualization, and Hypervisor based virtualization.

B. Virtualization Approaches

In an application based virtualization approach, hardware resources are controlled by host operating system and all the virtualized applications are hosted on top of the host operating system (Figure 1). Each virtual machine runs under dedicated guest operating system and related applications [13]. This type of virtualization approach is not popular due to security risks. In an operating system based virtualization approach, host operating system itself enables the virtualization and single physical server resources are shared by multiple isolated and virtualized guest OS's (Figure 2). All the virtualized OS instances are on the same host operating system kernel with special control over the physical infrastructure [14]. This approach is easy to adopt but it reveals destructive design, such as when an attacker injects malicious code into the host operating system all guest operating systems are affected and attacker gains complete control over the VMs. The third approach is hypervisor based virtualization [15]; in this approach, hypervisor directly interact with the hardware resources and it allocates hardware resource across multiple VMs (Figure 3).

Figure 1: Application Based Virtualization

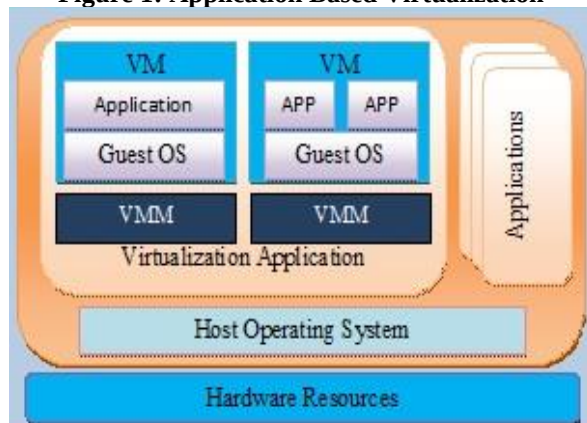


Figure 2: OS based Virtualization

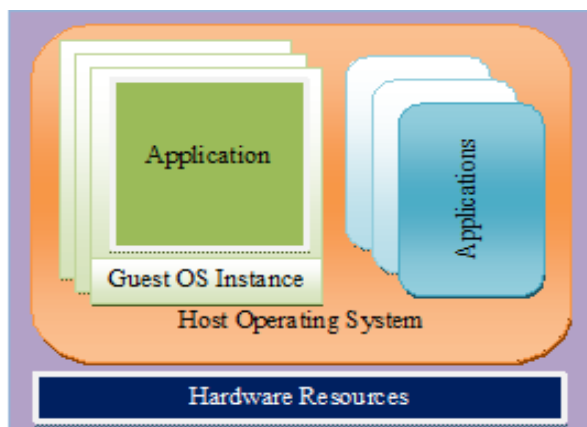
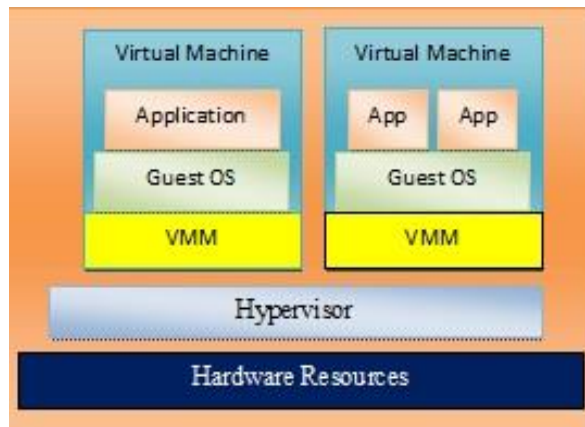


Figure 3: Hypervisor based Virtualization



C. Multi-Tenancy and Virtualization

Multi-Tenancy offers shared space for cloud users with the help of virtualization technology to reduce cost and get optimum use of resources in a shared environment. It permits several operating systems to run on a single machine concurrently. Cloud users are sharing the resources such as storage space, CPU processing, Memory, and Network bandwidth in a multi-tenant environment [16]. In a virtualized cloud environment physical machine can be divided into several virtual machines identified as guest machines and each virtual machine has its individual operating systems and applications but in certainty they are sharing single host machine resources [17].

III. DDoS Attack

The DDoS attacks can be classified into three categories; they are Volume based attacks/Bandwidth based attacks, Protocol attacks and Application layer attacks. Volume based attacks overload the victim system to consume the network bandwidth like UDP (User Datagram Protocol) floods and ICMP (Internet Control Message Protocol) floods [18]. Protocol attacks overload the target system to consume the resources like Ping of

death, Smurf attack, SYN flood attack and fragmented packet attack [19]. Application layer attacks overload the web applications by sending HTTP request like HTTP DDoS attacks and XML DDoS attacks [19]. TCP SYN Flood attack is one kind of DDoS attack, in which one victim machine receives more number of TCP SYN requests than its actual volume, which makes the cloud server to provide inadequate service to other machines. TCP SYN Flood attack is most dangerous DDoS attack in Distributed Cloud Environment due to the nature of VMs resource sharing [20]. The hierarchical view of TCP SYN flood attack belongs to DDoS attack is depicted in Figure 4.

Figure 4: Hierarchical view of TCP SYN Flood Attack



IV. TCP based DDoS attack

Transmission Control Protocol (TCP) based DDoS attack is popular in the Cloud server. Latest Akamai's report says 90% of the existing DDoS attacks are TCP based because of IP Spoofing method [21]. Majority of Cloud based Server side attacks can be initiated in the TCP/IP protocol suite [22]. TCP 3-way handshake method half-open connection establishment is the reason for DDoS attack in the cloud environment. Normal TCP 3-way handshake method reveals the connection establishment for data transfer among cloud user and cloud server. Steps are as follows

1. Cloud user sends a SYN request to the cloud server.
2. Cloud server replies ACK/SYN packet to the cloud user.
3. Cloud user sends ACK back to the cloud server to complete the connection establishment.

IP Spoofing can be categorized into three types, they are random spoofing, subnet spoofing, and fixed spoofing [23]. Attackers generate 32-bit random numbers for forged Packet source address in random spoofing. Subnet spoofing deals with the subnet address, which calculates the range from forged source address (141.83.121.0), for ex. (141.83.121.0 to 141.83.121.255). In fixed spoofing method, source IP address is taken from specified IP address list and attacker achieve this by performing reflector attack. When the cloud server is under DDoS attack using IP spoofing, the TCP connection establishment are as follows, Attacker sends a request (SYN) to the cloud server using spoofed source IP address, and then the server checks the availability of resources and reply to the sender with (SYN+ACK) packet. Server waits for an acknowledgement, but the sender never responds because of spoofed IP address [24]. Dissimilarity of random spoofing and subnet spoofing is ACK/SYN packet return to the sender. In random spoofing method, server returns ACK/SYN packet to other subnet address in most of the time, whereas subnet spoofing method permits server to send ACK/SYN packet to the correct subnet and the third round will be failed [25].

V. DDoS Attack detection methods

Flooding attack detection approaches are broadly divided into three types. They are Trace back based, Rule based, and Attribute based. Cloud Trace Back (CTB) approach is used to find the exact source of DDoS attack. Deterministic Packet Marking (DPM) is the well suited and effective algorithm for CTB [26][27]. DPM works in the IP header to mark the ID field and reserved flags. Whenever the router gets incoming packets, it is marked and the outgoing packets are neglected. The marked packets are unchangeable until the packet negotiates within the network. Cloud Protector is another DDoS attack detection method using CTB, which is a trained Back Propagation Neural Network (BPNN) to discover and sort out the DDoS attack [28]. Working functionality of neural network is, it has three different layers (input, hidden, and output Layers) which are organized and it incorporates a group of interconnected nodes, which has a weight associated with each of the connections. Threshold Logic Unit (TLU) plays significant role in neural network which incorporates input objects within an array of weighted quantities and check the threshold value. Second approach is rule based detection which provides some rules and conditions to sustain normal traffic apart from mistrustful traffic. Third approach is attribute based detection that detect the attack by controlling the Network/Transport layer attributes such as IP, TCP, UDP, and ICMP [29].

Flooding DDoS attack can be divided into two types which are direct attack and reflector attack. In direct attack type, attacker can directly send the request with spoofed IP address to the victim computer or network. Whereas reflector attack type, attacker selects the source address as victim computer IP address and send a sequence of request to the third party. After that based upon the request made by the attacker, third party replies to the victim computer and vast networking protocols are used for reflector DDoS attack [30][31].

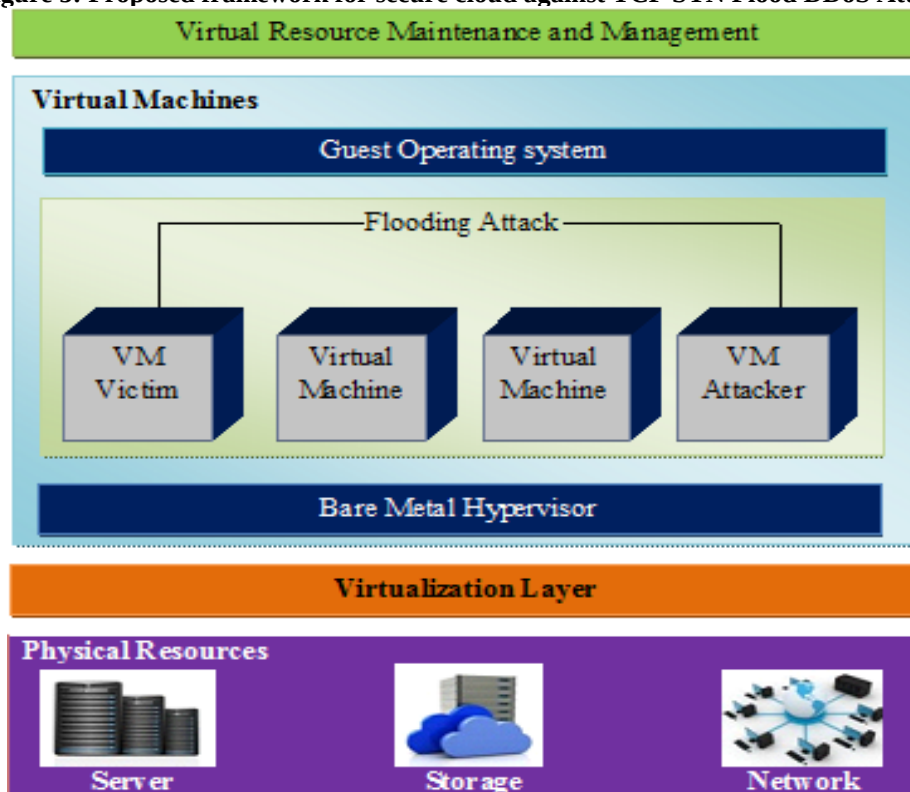
TCP SYN flood DDoS attack detection and prevention mechanisms are suitable for connection oriented network. In the case of cloud computing, this type of DDoS attack detection technique is essential to protect cloud server resources. Cloud Computing services are connectionless and completely internet based which provide resources to the cloud users at maximum level due to its scalability nature and load balancing features, However limit should be maintained for all kind of services even if it is virtualized data management. The proposed methodology introduces a token counter to limit the number of incoming requests and compare it along with a threshold value. Proposed algorithm contributes 4 check points to detect the illegal requests and block those IP addresses using SCAS (Secure Cloud Authentication System).

VI. Proposed Mechanism for TCP SYN Flood DDoS Attack in Cloud Environment

A. Framework

Proposed framework explains the nature of distributed cloud environment in the IaaS (Infrastructure as a service) level. Features of cloud computing provides virtualized hardware and software, elastic resource sharing nature to maintain data availability and reliability. Security issues are major hurdles for adopting cloud based services in industries as well as academic institutions. The most important cause for data availability and reliability issues are DDoS attacks. This proposed framework diagram (shown in Figure 5) delivers comprehensible design to protect against flooding based DDoS attack on virtual machines. Framework diagram considers two layers; they are physical layer and virtualization layer. Physical layer consists of bare metals of the data centre and it acts as a host machine. Physical resources are server, storage and network to manage all kind of requests. Virtualization layers are contributing more in cloud services to provide limitless data by scaling up and scaling down the resources. Hence the security level issues are also affected more in this layer. Server handles more number of virtual machines and virtual machines work under unique guest operating systems (OS image) to manage source requests. Type 1 hypervisor used here to communicate directly with the bare metal for secure communication, whereas type 2 hypervisor used in host operating system as intermediate system to communicate with the bare metal, unexpectedly if operating system gets crash then all the virtual machines are running under host operating system will also be crashed. Virtual resource maintenance and management layers are used to handle resources and maintain the data availability and reliability. The proposed methodology is explained in detail on how the flooding attack scenario handled and blocks the intruders in the next section.

Figure 5: Proposed framework for secure cloud against TCP SYN Flood DDoS Attack



B. Methodology

Proposed algorithm comprises of a Secure Cloud Authentication System (SCAS) (see Figure 6) for flooding attack which authenticates the connections among the SYN requester and the cloud service provider. Requests can be reached to cloud service provider through cloud instance, here the proposed algorithm works in cloud instance. SCAS detects and blocks the forged packets before it reaches to the cloud server to ensure the incoming packets are legitimate. Flood_Check () receives the incoming request from the source and counts the incoming packets called Packet Counter (PC) with particular time interval, if packet count is less than threshold value then packets forward to server otherwise call Packet_Check (). Packet_Check () extracts the flooding detected packet information and store the packet details in Active Connection Table (ACT) for comparison. ACT contains source IP address, destination IP address, and source MAC address as shown in Table I. Hence the ACT packet details are updated concurrently. One more table called Spoofed Address Table (SAT) used to check with the incoming packets to find and block the illegal user's request which contains spoofed IP address and equivalent MAC address as shown in Table II. Packet_Check () checks whether the source MAC address is same as SAT MAC address. If both the MAC addresses are same then it will be treated as illegal request using Spoofed IP, therefore packets will be dropped. If not, packets will be forwarded to IP_Check (). Finally compares packet information's with the updated ACT and check the MAC address and corresponding IP addresses. If similar MAC addresses have different IP addresses, then store those packet information's in the Spoofed Address Table (SAT) and drop the packets for connection termination else packets forward to destination server as legitimate SYN request.

Figure 6: Secure Cloud Authentication System

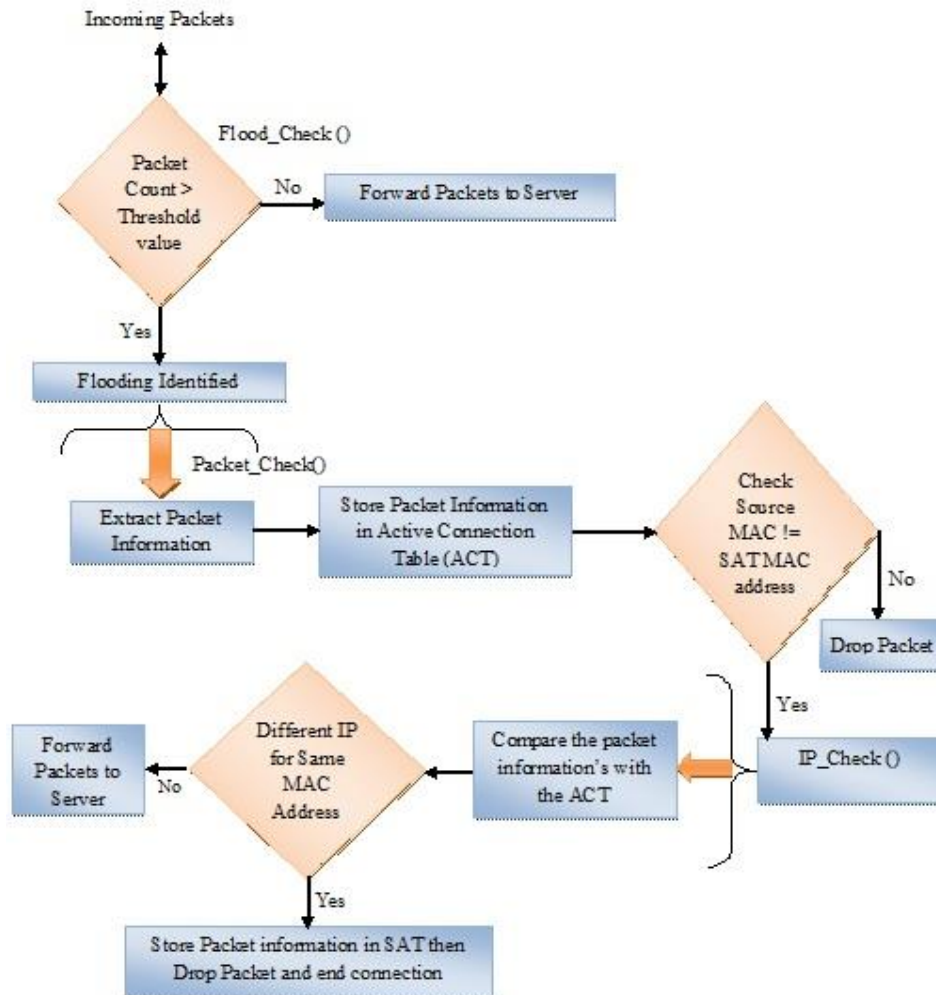


Table I: Active Connection Table

Source IP Address	Source MAC Address	Destination IP Address
192.37.66.75	00-00-35-00-59-27	192.49.23.58
192.45.82.76	00-00-35-00-59-27	192.49.23.58
192.77.56.23	00-00-35-00-59-27	192.49.23.58
192.35.67.45	00-00-45-00-00-25	192.49.23.58
192.35.67.45	00-00-45-00-00-25	192.49.23.58

Table II: Spoofed Address Table

IP Address	MAC Address
192.27.63.51	00-00-29-00-00-47
192.27.63.51	00-00-29-00-00-47
192.41.36.85	00-00-59-00-97-25
192.61.49.37	00-00-59-00-97-25
192.57.15.89	00-00-59-00-97-25

VII. Pseudo Code for Secure Cloud Authentication System (SCAS)

The following pseudo code describes the Secure Cloud Authentication System functionalities and its efficiency. There are three procedures and two tables are used to achieve better efficiency. Each procedure gives detailed conditional statements to process the functionalities of spoofed IP packets blocking.

Pseudo Code:

```

Flood_check()
    If Packet Count > Threshold value within Time_limit → flooding identified
        Buffer all packets and do Packet_check();
    Else do Echo_Check();
Packet_check()
    Packets in Buffer
        Extract packet informations → store the packet informations in ACT;
        if source_packet_MAC address! in SAT → Do IP_check();
    Else Drop Packet;
IP_Check()
    While (packet IP & MAC != Packets IP & MAC in ACT) do
        If source_packet_MAC is same for different IP →
            store source_packet_MAC in SAT and drop packet
    Else Forward Packet;

```

flood_check() procedure checks the number of incoming packets, packet_check() procedure stores packet information and compares source MAC address, spoofed address table (SAT) MAC address, finally ip_check() procedure checks source MAC address and its corresponding IP address to detect and block spoofed packets.

VIII. Conclusion and Future Work

DDoS attack security threats plays prominent role in cloud computing to affect cloud server data. A variety of DDoS attack detection methods are discussed using virtualization techniques. TCP SYN flood based DDoS attack methods and working principles are discussed with precise illustration. Various DDoS attack detection methods and their merits, demerits are taken into consideration in the proposed work. DDoS attack detection and prevention techniques are essential for cloud computing to protect cloud server resources due to its virtualized resource sharing nature. Proposed methodology detects flooding of attack request from attacker and prevents them prior to get into cloud service provider to reduce illegal resource utilization. Future work focuses on introducing new algorithm for this DDoS attack detection methodology and simulates the results in cloud scenario.

IX. References

- [1] Manavi, Sina, et al. "Secure model for virtualization layer in cloud infrastructure." International Journal of Cyber-Security and Digital Forensics (IJCSDf) 1.1 (2012): 32-40.
- [2] M.Durairaj, A.Manimaran, "A Study on Securing Cloud Environment from DDOS Attack to Preserve Data Availability" International Journal of Scientific & Technology Research, Volume 3, Issue 2, February 2015.
- [3] Mittal, Akash, Ajit Kumar Shrivastava, and Manish Manoria. "A Review of DDOS Attack and its Countermeasures in TCP Based Networks." International Journal of Computer Science & Engineering Survey 2 (2011): 177-87.
- [4] Chen, Wei, and Dit-Yan Yeung. "Defending against TCP SYN flooding attacks under different types of IP spoofing." Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on. IEEE, 2006.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
- [5] Durairaj, M., and A. Manimaran. "A Study on Security Issues in Cloud Based E-Learning." Indian Journal of Science and Technology 8.8 (2015): 757-765.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
- [6] Katkamwar, Niraj Suresh, Atharva Girish Puranik, and Purva Deshpande. "Securing Cloud Servers against Flooding Based DDoS Attacks." International Journal of Application or Innovation in Engineering and Management (IJAIEEM) 1.3 (2012): 50-55.
- [7] Lonea, Alina Madalina, Daniela Elena Popescu, and Huaglority Tianfield. "Detecting ddos attacks in cloud computing environment." International Journal of Computers Communications & Control 8.1 (2012): 70-78.

- [8] Bhandari, Nisha H. "Survey on DDoS Attacks and its Detection & Defence Approaches." *International Journal of Science and Modern Engineering (IJISME)* ISSN: 2319-6386 (2013).
- [9] Ismail, Mohd Nazri, et al. "New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment." *International Journal of Computer Science and Security (IJCSS)* 6.4 (2012): 226.
- [10] Udendhran, R. "New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment." *Asian Journal of Computer Science and Information Technology* 4.12 (2014): 87-91.
- [11] S. Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34.1 (2011): 1-11.
- [12] BHADARIA, Rohit, et al. "SECURITY ISSUES IN CLOUD COMPUTING." *Acta Technica Corvinensis-Bulletin of Engineering* 7.4 (2014).
- [13] Carroll, Mariana, Paula Kotzé, and Alta Van der Merwe. "Secure virtualization: benefits, risks and constraints." (2011).
- [14] Mishra, Neha. "A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues." *RIET-IJSET: International Journal of Science, Engineering and Technology* 2.1 (2015): 59-68.
- [15] Grover, Jitender, and Mohit Sharma. "Cloud computing and its security issues—A review." *Computing, Communication and Networking Technologies (ICCCNT)*, 2014 International Conference on. IEEE, 2014.
- [16] Lombardi, Flavio, and Roberto Di Pietro. "Secure virtualization for cloud computing." *Journal of Network and Computer Applications* 34.4 (2011): 1113-1122.
- [17] Fernandes, Diogo AB, et al. "Security issues in cloud environments: a survey." *International Journal of Information Security* 13.2 (2014): 113-170.
- [18] Haris, S. H. C., R. B. Ahmad, and M. A. H. A. Ghani. "Detecting TCP SYN flood attack based on anomaly detection." *Network Applications Protocols and Services (NETAPPS)*, 2010 Second International Conference on. IEEE, 2010.
- [19] Wei, Lifei, et al. "Security and privacy for storage and computation in cloud computing." *Information Sciences* 258 (2014): 371-386.
- [20] Singh, Navdeep, et al. "A Review on Security Issues in Cloud Computing." *International Journal of Innovation and Applied Studies* 8.3 (2014): 1090-1093.
- [21] Mezzour, Ghita, Kathleen M. Carley, and L. Richard Carley. "An empirical study of global malware encounters." *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*. ACM, 2015.
- [22] Chapade, S. S., K. U. Pandey, and D. S. Bhade. "Securing cloud servers against flooding based ddos attacks." *Communication Systems and Network Technologies (CSNT)*, 2013 International Conference on. IEEE, 2013.
- [23] Eddy, Wesley M. "Defenses against TCP SYN flooding attacks." *The Internet Protocol Journal* 9.4 (2006): 2-16.
- [24] Haris, S. H. C., R. B. Ahmad, and M. A. H. A. Ghani. "Detecting TCP SYN flood attack based on anomaly detection." *Network Applications Protocols and Services (NETAPPS)*, 2010 Second International Conference on. IEEE, 2010.
- [25] Aich, Asish, Alo Sen, and Satya Ranjan Dash. "A Survey on Cloud Environment Security Risk and Remedy." *Computational Intelligence and Networks (CINE)*, 2015 International Conference on. IEEE, 2015.
- [26] Joshi, Bansidhar, A. Santhana Vijayan, and Bineet Kumar Joshi. "Securing cloud computing environment against DDoS attacks." *Computer Communication and Informatics (ICCCI)*, 2012 International Conference on. IEEE, 2012.
- [27] Chen, Chin-Ling, and Hsin-Chiao Chen. "A Rule-based Detection Mechanism against Distributed Denial of Service Attacks." *The Third International Conference on Digital Enterprise and Information Systems (DEIS2015)*. 2015.
- [28] Li, Jin, Yong Liu, and Lin Gu. "DDoS attack detection based on neural network." *Aware Computing (ISAC)*, 2010 2nd International Symposium on. IEEE, 2010.
- [29] Nazir, Mohsin, et al. "Cloud Computing: Current Research Challenges." *Book Chapter of Cloud Computing: Reviews, Surveys, Tools, Techniques and Applications-An Open-Access eBook published by HCTL Open* (2015).
- [30] Xiao, Ziqian, and Jingyou Chen. "Cloud Computing Security Issues and Countermeasures." *Proceedings of the 4th International Conference on Computer Engineering and Networks*. Springer International Publishing, 2015.
- [31] Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." *Information Sciences* 305 (2015): 357-383.