© 2015 IJSRSET | Volume 1 | Issue 5 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Network Denial of Service Threat Security on Cloud Computing A Survey

Elmustafa Sayed Ali Ahmed, Rasha E. A. Elatif
Department of Electrical and Electronics Engineering, Red Sea University, Port Sudan, Sudan, Saudi Arabia

ABSTRACT

Cloud computing is one of the most important communication model nowadays since it's provides a sets of resources and multiple types of services offered through the internet. The services and resources provided by cloud computing are cheaper because of no maintenance cost required in the core of clouds, since all services were offered to the clients based on services availability by providers only and clients are free to manage and maintains the resources machines. People use the cloud computing only when they need it, for this reasons cloud computing may be called a services over internet on demand. Companies also use the clouds to reduce their operation costs by resting virtual machines for digital services from cloud providers. With the growth of data every day which require a more services and resources in cloud computing, a security issues are creates a new demands and opportunities for security models that because cloud computing facing many types of attack threats with increasing of clouds . Network Denial of services is one of the most famous attack threats that make sense in a cloud computing context and may be divided into network distributed denial of services and DNS denial of services knows as availability threats. This paper reviews the types of network denial of services attacks also classify the methods of security defences and then compare between all of them.

Keywords: Cloud computing, Denial of Service, DNS DoS, Network Distributed DoS, availability threats, Security.

I. INTRODUCTION

Cloud computing as a model enables on demand access to servers, networks, and applications provide an options for people to use the major benefits of clouds computing of flexible and scalable infrastructures, reduced implementation and maintenance costs [1]. The cloud computing data center is usually composed of thousands of commercial computers, and these computers are connected by network with computing programming model to help user to use cloud resources without concerning the details of implementation [2]. Cloud computing enables clients to access resources online through the internet, from anywhere at any time without worrying about technical management and maintenance issues of the original resources [3]. The security issues related to cloud computing are very important that because of the increasing of clouds of services and resources accessed by clients [4]. Denial of service attack has become an increasingly prevalent security threat, people realize that protecting systems against DoS attack is also one of the key security issues. Network Distributed Denial of Service (DDoS) attacks are one of the biggest concerns for security professionals in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. Other type of denial of services is a DNS denial of services known as Domain Name System (DNS) denial of service, it's a Domain Name System (DNS) flooding attack aims to consumption of critical system resources in order to paralyze the provided services and make them unavailable to its legitimate users [5].

This study is focusing over the security methods that used to ensure security cloud computing against the two types of network attack threats based on denial of services threats; they are distributed and DNS denial of services tacking all considerations related to the solutions of denial of services security. The rest of the paper organized as follows; Section 2 presents the concepts of the denial of services, then reviews the

threats that related to availability of cloud computing, explains the two types of threats network denial of services. Section 3 focuses on networks distributed denial of service attack methods and DNS attacks on cloud computing. Section 4 illustrates the modern defense methods against denial of services attacks.

The list of possible defenses against the two types of availability threats denial of services, and discussion in more depth of the security models related to those threats will be reviewed in section 5. Section 6 briefly review the comparison between the model of security taken as a defense technique for Network Denial of Service Threat in cloud computing. Finally section 7 concludes the paper and provides some future ideas for security in cloud computing.

II. METHODS AND MATERIAL

A. Denial of Service

Denial of service (DOS) has become an increasingly prevalent security threat, users realize that protecting systems against DoS attack is also one of the key security issues. Although DoS attack is becoming a fast growing concern. A Denial of Service attack is a method of blocking service from its intended users. The severity of this attack varies with the magnitude of loss and the duration of attack. DoS attacks could be extended to Distributed Denial of Service (DDoS) attacks which does damage in a massive scale. DoS attacks on DNS wherein attackers flood the name servers of a cloud area to disrupt resolution of resource records belonging to the area and consequently, any of its sub areas [5].

(i). Distributed Denial of Service

A distributed denial of service (D-DoS) is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. A hacker begins by exploiting vulnerability in one computer system and making it the D-DoS master .It is from the master system that the intruder identifies and communicates with other systems by loading cracking tools available on the Internet on multiple compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The flood of packets to the target causes a denial of service [5].

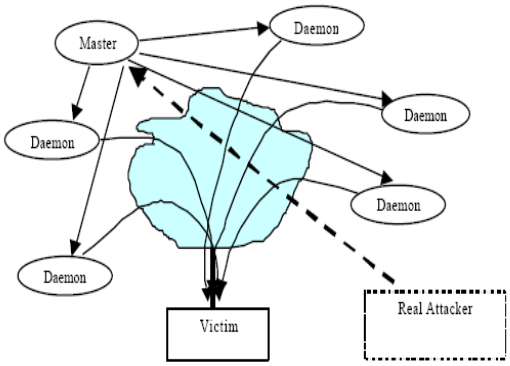

Figure 1: Distributed Denial of Service Attack Components

(ii). DNS Denial of Service

The domain name system (DNS) is a hierarchical distributed system providing the necessary mapping or binding between human comprehensible domain names and the corresponding numerical IP addresses. This mapping procedure is also known as address resolution service. In the root of this hierarchy tree is located the mapping of top level domains, like ".gr", ".com", ".org" etc, to the IP addresses of the corresponding authoritative DNS server. Each of these domains and the subsequent sub-domains form a specific zone.

The leaf of each zone in this hierarchy stores the mapping of a specific domain name to its IP address; this information is kept in the corresponding DNS Resource Record (RR). The main goal of any flooding attack is the consumption of critical system resources in order to paralyze the provided services and make them unavailable to its legitimate users.

Flooding attacks against DNS are similar to other well documented Internet services flooding attacks and could be launched in two distinct ways. In the first one the attacker sends a large number of bogus DNS requests either from a single or multiple sources, depending on the flooding architecture utilized for example of multiple sources flooding architecture attack against a DNS is depicted in Figure 2.

According to this scenario, the attacker orchestrates usually innocent hosts, called zombies, to

simultaneously generate fake DNS requests aiming at disrupting the normal DNS operation by consuming its resources; mainly memory and CPU [6].

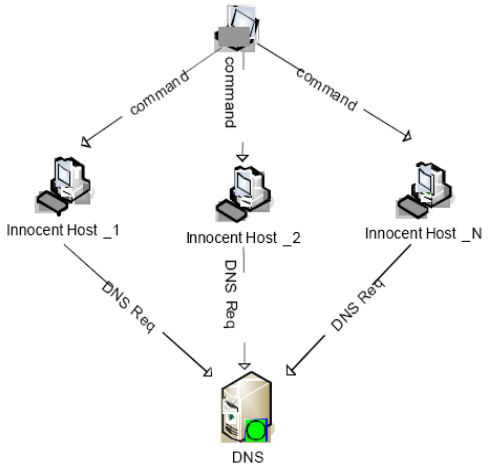

Figure 2: DNS flooding attack architecture

B. Network Denial of Service Attacks

Network denial of service attack might divide into categories; distributed denial of services and DNS denial of services knows as availability threats. Distributed Denial of service has the cohesive strength of many compromised systems working towards a single cause. The first stage of this attack is to build its platform with many host systems that can work under remote commands. The attacker group would first scan networks to hunt for vulnerable systems that are weak in security features. According to researchers there are millions of host machines that are vulnerable without secure patches and proper updates that often fall victims to these attackers. Once the scanning procedure is completed, attackers would bring these hosts into control using software exploitations like buffer overflow, dangling pointers, code injection [7].

i Distributed DOS Attacks

The distributed denial of services D.DOS attack attempt to exhaust the victim's resources such as network bandwidth .There are two types of DDoS attacks; a network centric attack which overloads a service by using up bandwidth and an application layer attack which overloads a service or database with application calls. In network centric attack type the attack will take place through traffic or bandwidth. The traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation. Bandwidth attacks overload the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service [7]. In application layer attack, the application layer data messages can deplete resources in the application layer, leaving the target's system services unavailable. The application layer attacks are the most deadly kind of attacks as they can be very effective with as few as one attacking machine generating a low traffic rate, this makes these attacks very difficult to pro-actively detect and mitigate. These attacks have come to prevalence over the past three or four years and simple application layer flood attacks using HTTP flood have been one of the most common DDoS attacks seen in the wild [7].

ii Domain Name System DOS attacks

In the denial of services against domain name system (DNS), a TCP/IP stack of the DNS server machines attacked to cause them to drop incoming DNS queries, or exhaust the resources of DNS servers One may be able to force name servers to drop DNS queries by attacking the TCP/IP stack of name server machines, for example, by exploiting IP fragmentation reassembly vulnerabilities to exhaust memory or CPU resources. Another approach is to exhaust the CPU and memory resources of a DNS server, for example, by bombarding name servers with a lot of DNS queries so that they do not have enough resources to process all the DNS queries they receive [7].

C. Defense Methods against Denial of services attacks

The challenge in preventing DDoS attacks lies in the nature of the traffic and the nature of the attack. Because most often the traffic is legitimate as defined by protocol. To identify the attacks the difference between volumetric and application-level attack traffic must also be understood clearly. Application level attacks exploit specific applications or services on the targeted system. They typically bombard a protocol and port a specific service uses to render the service useless and the attack take place by HTTP or DNS. Volumetric attacks use an increased attack footprint that seeks to overwhelm the target. This traffic can be application specific, but it is most often simply random traffic sent at a high intensity

to over utilize the target's available resources using DNS or SYN floods. There are many types of defense methods those used against denial of services attacks, these methods like Route Filtering, Unicast Reverse Path Forwarding, Geographic Dispersion, Tightening Connection Limits and Timeouts, Reputation Based Blocking, and control accessing method [8].

i. Route Filtering Techniques

A Remotely triggered black hole (RTBH) filtering can drop undesirable traffic before it enters a protected network by what is called black holes. When an attack has been detected, black holing can be used to drop all attack traffic at the network edge based on either destination or source IP address, and regarding RTBH filtering for further information [9].

ii. Unicast Reverse Path Forwarding

Network administrators can use Unicast Reverse Path Forwarding (uRPF) to help limit malicious traffic flows occurring on a network, as is often the case with DDoS attacks. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. It can limit the appearance of spoofed addresses on a network, by discarding packets if the source IP address is not valid [9].

iii. Geographic Dispersion

To mitigating DDoS attacks, distributing the footprint of DDoS attacks is used in clouds which make the targets not individually saturated by the volume of attack traffic. This solution uses a routing concept known as Any cast to allows traffic from a source to be routed to various nodes via the nearest hop node in a group of potential transit points and its provide geographic dispersion [10].

iv. Tightening Connection Limits and Timeouts

Anti-spoofing used to limiting connections and enforcing timeouts in a network environment seek to ensure that DDoS attacks are not launched or spread from inside the network.

v. Reputation Based Blocking

Reputation based blocking is an essential component to web filtering provides URL analysis and establishes a reputation for each URL to limits the impact of untrustworthy URLs. Its uses to defense against malware, botnet activity, and other web-based threats attack [10].

vi. Control Accessing

Access Control Lists provide a flexible option to a variety of security threats and exploits, including DDoS, which provide a reactive mitigation for DDoS attacks by ordered set of rules and rule specifies a set of conditions that a packet must satisfy to match the rule plays as traffic filter. Firewalls, routers, and even switches support, and when of each these devices determine that an ACL applies to a packet, it tests the packet against the conditions of all rules and determine whether the packet is permitted or denied, and continues processing packets that are permitted and drops packets that are denied [10].

D. Network Denial of Service Threat Security Methods

Many studies have proposed to defenses against a network denial of service attack, in both types distributed network and domain name system denial of services attacks. In the following sections we present a review of different security methods against distributed network denial of services attacks. These different studies were collected from several researches based on the mechanisms and the security type used in the proposed research.

i. Artificial Intelligent and Prediction Based Models

Suriadi, S et al [11], describe a mechanism for integrating a hash based puzzle into web services frameworks available and analyze the effectiveness of the countermeasure using different scenarios on a network test bed. This study presents techniques to defense the clouds against flooding attacks using client puzzles which they can also mitigate certain types of semantic based attacks.

Joshi, B. et al [12], propose a mechanism to test the efficiency of a cloud trace back model in dealing with DDoS attacks using back propagation neural network to predicts safe models which finds that the model is useful in tackling distributed denial of service attacks.

T. Siva, E.S. Phalguna Krishna [13], provide security to cloud resources by denial of service (DoS) attacks and their related sub domains also to security of application denial of service (ADoS) attacks which comes under DDOS attacks concentrate on SaaS in cloud computing. The research present different types of cloud based DDOS attacks and their solutions, also give most dangerous application DoS attacks scenario and their remedy mechanisms, by introducing new port hopping scheme as true random number generation (TRNG) based port hopping in cloud computing environment. This hopping scheme by using pseudo random number Generation (PRNG) over comes the disadvantage of prediction of the port hopping sequence and is periodic in nature.

Upma Goyal et al [14], propose a defense mechanism against the DDoS attacks which is known as cloud specific intrusion detection system. This defense mechanism will be able to detect the attack before the DDoS attack succeeds. The mechanism includes two methods of intrusion detection they are; behavior based method which compares the recent user actions to the usual behavior and the knowledge based method which detects known attacks. The behavior deviation is analyzed using artificial intelligence. With all the responses, the IDS detect the attack and alert the other nodes. The cloud Intrusion detection model will be detecting the attack traffic with the help of Entropy and The Anomaly based detection system.

N. Ch. S. N. Iyengar et al [15] propose a fuzzy logic based defense mechanism that can be set with predefined rules by which it can detect the malicious packets and takes proper counter measures to mitigate the DDoS attack. The predefined traffic parameters used are vary significantly between a normal traffic pattern and attack traffic pattern .However for any particular data center, from DDoS traffic pattern, the parameters can be changed based upon specific requirements.

ii. Filtering Based Models

J. RAMESHBABU et al [16] study focus on the impact of DDoS attacks in cloud and the NEIF technique available to overcome the attacks of distributed denial of service DDoS on the clouds. NEIF installed at the ISPs' edge routers plays as a dual role in shielding DDoS attacks using ingress filtering to discover and prevent the DDoS attacks from its customer, and also been extensively deploying to avoid source IP spoofing. The mechanism discarding packets which have a source address which is not allocated to customers. It can ensure an SP's network do not participate in flooding DDoS attacks.

Priyanka Negi et al [17], proposed a modification to the confidence based filtering method (CBF) which is investigated for cloud computing environment based on correlation pattern to mitigate DDoS attacks on Cloud. The modification introduces nominal additional bandwidth and tries to increase the processing speed of the victim initiated server. In the enhanced confidence based filtering method legitimate packet is the one whose confidence based filtering value is above the discarding threshold. Those packets with scores lower than the discarding threshold are regarded as attack ones.

iii. Monitoring and Identifying Based Models

Chu-Hsing Lin et al [18], analyze native modules of the PHP dynamic pages and find the amount of system resources consumed by parts of the native modules. The study propose a method based on semantic concept to formulate rules to identify and monitoring malicious browsing behaviors in order to improve performance of web services and to slice the cost.

Ashley chonka et al [19], study some of the current attacks that attackers may initiate as HTTP and XML. the proposed research offer a solution to trace back through cloud trace back (CTB) to find the source of these attacks, and introduce the mechanism, called cloud protector, to detect and such attack traffic. The results show that proposed idea able to detect most of the attack messages and were able to identify the source of the attack within a short period of time.

A.M. Lonea et al [20], provide a combination between the evidences obtained from intrusion detection systems (IDSs) deployed in the virtual machines (VMs) of the cloud systems and a data fusion methodology in the front end. Specifically. The VM based IDS will yield alerts when the attacks appear, which will be stored into the MySQL database placed within the cloud fusion unit (CFU) of the front end server. the study propose a quantitative solution for analyzing alerts generated by

the IDSs, using the dempster Shafer theory (DST) operations in 3 valued logic and the fault tree analysis (FTA) for the flooding attacks. The solution to identify these attacks is to use the dempsters combination rule to fuse evidence from multiple independent sources. The proposed solution represents the imprecision and efficiently utilizes it in IDS to reduce the false alarm rates by the representation of the ignorance.

A. S. Syed Navaz et al [21], Propose a combination scheme between hereto merge entropy based system with anomaly detection System for providing multilevel distributed denial of service (DDoS). The proposed idea taking two steps; first, users are allowed to pass through router in network site in that it incorporates detection algorithm and detects for legitimate user. then secondly, again it pass through router placed in cloud site in that it incorporates confirmation algorithm and checks for threshold value, if it's beyond the threshold value it considered as legitimate user, else it's an intruder found in environment. This system is represented and maintained by as third party. When attack happens in environment, it sends notification message for client and advisory report to cloud service provider (CSP) to identify the attacks.

Mettildha Mary et al [22], propose a novel solution, named DDoS and EDoS Shield, to avoid the denial of service and economic denial of sustainability (EDoS) attack in the cloud computing systems. The main idea of the proposed scheme is to verify whether the requests coming from the users are from a legitimate person or generated by bots. This work will test the efficiency of a cloud trace back model using a new data set based upon deterministic packet marking (DPM) algorithm. This scheme will check the cloud trace back model using flexible deterministic packet marking, which provides a defense system with the ability to find out and identify the real sources of attacking packets that traverse through the network.

Bing Wang et al [23], propose a graphic model based attack detection system that can deal with the dataset shift problem. The core of the attack detection system is a graph model. It stores known traffic patterns as a relational graph between patterns and their labels (malicious or normal). When new network traffic arrives, the system uses this graph to determine whether it is malicious. The mechanism of DDoS attack mitigation architecture integrates a highly programmable network monitoring to enable attack detection and a flexible control structure to allow fast and specific attack reaction. The proposed architecture can effectively and efficiently address the security challenges brought by the new network paradigm.

iv. Networking and Data Based Models

N. Jeyanthi et al [24], proposed spoofing detection algorithm to detect DDoS attacks is used to detect address spoofing for each request to a service. The proposed algorithm consists of a cloud authentication system (CAS) that will authenticate the connections between the DC requester and the cloud service provider, and which will ensure that the incoming request packet is legitimate. CAS will be embedded in the cloud service provider, and receive all the incoming packets from the requester, who may be legitimate, attacker or a combination of bot before it is allowed to reach the service.

Sanchika Gupta et al [25], identifies vulnerabilities responsible for well-known network based attacks on cloud and does a critical analysis on the security measures available in cloud environment. The proposed study focuses on a nonconventional technique for securing cloud network from malicious insiders and outsiders with the use of network profiling. The profile is created for each virtual machine (VM) in cloud that describes network behavior of each cloud user .The behavior gathered is then used for determination and detection of network attacks on cloud. The novelty of the approach lies in the early detection of network attacks with robustness and minimum complexity. The proposed technique can be deployed with minimal changes to existing cloud environment.

Namrata and Prof. D. S. Datar [26], design a cloud computing based collaborative network security management system using botnet which balances the load in the network and check for each and every file transferring in the cloud for the bot. If the file contains the bot then the folder in which that file is saved, will be deleted from that client. The proposed system is to protect the cloud from botnet and prevent the cloud from botnet attack. During the systems operation, the collaborative mechanism runs as expected to balance the load in the network, and to check the file transferring in

the network as instructed by the security center or the server machine.

Danveer Singh et al [27], describe how to detect DDoS violence, in view of that cloud providers will alert to assign resources to users even in denial of service violent behavior in in the distance ahead. The paper proposes types of detections like network traffic analysis based DDoS detection, and data analysis based DDoS detection.

Osanaiye [28], discusses different methods for detecting spoofed IP packet in cloud computing and proposes host based operating system fingerprinting that uses both passive and active method to match the operating system and applications of incoming packet from its database.

III. RESULTS AND DISCUSSION

Security Models Comparison

The proposed models which they are mentioned in the above sections were gathered from many researches based on four issues they are, artificial intelligent and prediction, filtering, monitoring and identifying, networking and data. The following table shows the comparison between all the discussed security models based on investigation area, proposes, and mechanism.

Table 1: Security Models Comparison

Proposed Models by Authors	***Investigation Area***	***Investigation Propose***	***Mechanism Used***
Suriadi, S et al [11]	Web Services clouds	Defense against flooding attacks	client puzzles to mitigate certain types of semantic based attacks
Joshi, B. et al [12]	cloud trace back dealing with DDoS attacks	test the efficiency of a cloud trace back model	back propagation neural network production
T.Siva, E.S. Phalguna Krishna [13]	SaaS in cloud computing	security to cloud resources by (DoS) attacks application DOS attacks	true random number generation (TRNG) based port hopping scheme
Upma Goyal et al [14]	Behavior of user actions	detect the attack and alert the other nodes	Artificial intelligent, Entropy and Anomaly based detection system.
N.Ch.S.N. Iyengar et al [15]	malicious packets attack	predefined traffic parameters to detect the malicious packets	fuzzy logic based defense
J.RAMESHBABU et al [16]	IP spoofing and unauthorized customer address	Defense against unauthorized packets	NEIF technique and ingress filtering
Priyanka Negi et al [17]	correlation pattern to mitigate DDoS attacks	Discards an trusted packets	confidence based filtering method (CBF)
Chu-Hsing Lin et al [18]	PHP dynamic pages	monitoring malicious browsing behaviors	semantic concept
Ashley chonka et al [19]	HTTP and XML	find the source of attacks	cloud protector
A.M. Lonea et al [20]	intrusion detection systems (IDS)	reduce the false alarm rates of attacks	data fusion methodology with VM based IDS
A.S.Syed Navaz et al [21]	Attack notification	Notify the client and cloud service provider (CSP) to identify the attacks.	hereto merge entropy based system and anomaly detection System
Mettildha Mary et al [22]	economic denial of sustainability	verify the requests coming from	deterministic packet marking

		the users (legitimate person or generated by bots)	(DPM) algorithm
Bing Wang et al [23]	graphic model based attack	graph model to determine malicious	relational graph between patterns (normal or malicious)
N. Jeyanthi et al [24]	address spoofing	ensure that the incoming request packet is legitimate	cloud authenticati on system (CAS)
Sanchika Gupta et al [25]	malicious insiders and outsiders	early detection of network attacks	Profile Based Network Intrusion Detection and Prevention System
Namrata and Prof. D. S. Datar [26]	Botnet attack	balances the load in the network	based collaborativ e network
Danveer Singh et al [27]	denial of service violent behavior	detect DDoS violence	network traffic and data analysis based DDoS detection
Osanaiye [28]	operating system and applications attacks	detecting IP spoofing	host based operating system fingerprinti ng

IV. CONCLUSION

With large amount of clouds in networks today, attacks increase more and more by using several attack techniques, methods and tools. The most important type of attacks are related to the network denial of services concepts such as distributed network denial of services and domain name system denial of services. In this paper we present a main point of attacks methods in clouds related to denial of services and review of possible security threads models those will used to make some of defense against mentioned attacks. The revision of security models depends on the investigated area that represents the type of attack and on the methodology taken to make defense such as artificial intelligent methods, monitoring and identifying method, filtering and network based methods. In this paper we propose many models for security issues in denial of services attacks, and most of these models investigate on flooding attack, spoofing and on unauthorized access. The proposed security based on three schemes detecting attacks, monitoring / identifying attack, and filtering to discard attack.

V. REFERENCES

[1] P. Vijaya Vardhan Reddy* and Dr. Lakshmi Rajamani ," Performance Evaluation of Hypervisors in the Private Cloud based on System Information using SIGAR Framework and for System Workloads using Pass mark", International Journal of Advanced Science and Technology Vol.70 (2014), pp.17-32.

[2] Chao Shen and Weiqin Tong," Review on the Cloud Computing Programming Model", International Journal of Advanced Science and Technology, Vol.70 (2014), pp.11-16.

[3] Farhan Bashir Shaikh and Sajjad Haider," Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates.

[4] Elmustafa Sayed Ali Ahmed1 and Rashid A. Saeed2; "A Survey of Big Data Cloud Computing Security"; International Journal of Computer Science and Software Engineering , Volume 3, Issue 1, December 2014.

[5] K. Santhi," A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks", International Journal of Advanced Research in Computer Science and Software Engineering ", Volume 3, Issue 5, May 2013.

[6] Stephen M. Specht and Ruby B. Lee," Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures"; Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, pp. 543-550, September 2004.

[7] K.Santhi ; "A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks"; International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013 , pages 1-5.

[8] Georgios Kambourakis, Tassos Moschos, Dimitris Geneiatakis and Stefanos Gritzalis , "A Fair Solution to DNS Amplification Attacks", Laboratory of Information and Communication Systems Security , University of the Aegean, Karlovassi, GR-83200 Samos, Greece 2008 ,pages 1-10.

[9] Jun Xu; Wooyong Lee; "Sustaining availability of Web services under distributed denial of service attacks"; Computers, IEEE Transactions on , vol.52, no.2, pp. 195- 208, Feb. 2003.

[10] Shui Yu; "Distributed Denial of Service Attack and Defense"; springer October 23, 2013.

[11] Suriadi, S et al ; "Defending Web Services against Denial of Service Attacks Using Client Puzzles , Web Services (ICWS)"; IEEE International Conference 4-9 July 2011.

[12] Joshi, B. ; Vijayan, A.S. ; Joshi, B.K.; "Securing cloud computing environment against DDoS attacks "; Computer Communication and Informatics (ICCCI), International Conference 10-12 Jan. 2012.

[13] T. Siva, E.S. Phalguna Krishna; "Controlling various network based A DoS Attacks in cloud computing environment: By Using Port Hopping Technique"; International Journal of Engineering Trends and Technology (IJETT)-Volume 4 Issue 5-May 2013.

[14] Upma Goyal1, Gayatri Bhatti2and Sandeep Mehmi; "A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model"; International Journal of Application or Innovation in Engineering & Management , Volume 2, Issue 3, March 2013.

[15] N.Ch.S.N. Iyengar1, Arindam Banerjee2 and Gopinath Ganapathy3; "A Fuzzy Logic based Defense Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment"; International Journal of Communication Networks and Information Security, Vol. 6, No. 3, December 2014.

[16] J.RAMESHBABU,*B.SAMBALAJI,*R.WESLE Y DANIEL,**K.MALATH;" PREVENTION OF DD OS A TTACKS IN CLOUD USING NEIF TECHNIQUES"; International Journal of Scientific and Research Publications, Volume 4, Issue 4, April 2014.

[17] Priyanka Negi1, Anupama Mishra2and B. B. Gupta; "Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment";http://arxiv.org/ftp/arxiv/papers /1304/1304. 7073. pdf. Accessed in 18 Aug. 2015].

[18] Chu-Hsing Lin et al ; "A detection scheme for flooding attack on application layer based on semantic concept"; Computer Symposium (ICS), International 16-18 Dec. 2010.

[19] Ashley chonka et al ; "Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks"; Journal of Network and Computer Application Volume 34 Issue 4, July, 2011.

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

[21] A.S.Syed Navaz, V.Sangeetha, C.Prabhadevi; "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud"; International Journal of Computer Applications (0975 –8887) Volume 62–No.15, January 2013.

[22] Mettildha Mary1, P.V.Kavitha2, Priyadharshini; "Vigneshwer S Ramana, Secure Cloud Computing Environment against DDOS and EDOS Attacks" ;International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1803-1808.

[23] Bing Wang ; Yao Zheng ; Wenjing Lou ; Hou, Y.T.; "DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking"; Network Protocols (ICNP), IEEE 22nd International Conference, 21-24 Oct. 2014.

[24] N. Jeyanthi*, Uttara Barde, M. Sravani and Venu Tiwari; "Detection of distributed denial of service attacks in cloud computing by identifying spoofed IP"; Int. J. Communication Networks and Distributed Systems, Vol. 11, No. 3, 2013.

[25] Sanchika Gupta,1Padam Kumar,1and Ajith Abraham; "A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment" ;Hindawi Publishing Corporation International Journal of Distributed

Sensor Networks Volume 2013, Article ID 364575,12pages.
[26] Namrata A. Sable and Prof. Mr. D. S. Datar;"Cloud Computing Based -Collaborative Network Security Management System Using Botnet"; international Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 10 October 2014.
[27] Danveer Singh, 2.Basant Kumar Gupta 3.Harshit Gupta, DDOS Attack and Detection for Secured Cloud Computing Resources, International Journal Of Engineering And Computer Science Volume 3 Issue 4 April, 2014 Page No. 5392-5395.
[28] Osanaiye, O.A.; "Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing"; Intelligence in Next Generation Networks (ICIN), 17-19 Feb. 2015.

VI. Authors Biography

Elmustafa Sayed Ali Ahmed received his M.Sc. degree in electronic engineering, Telecommunication from Sudan University of science and technology in 2012, and B.Sc. (Honor) degree in electrical engineering, Telecommunication from Red Sea University in 2008. He was a wireless networks (Tetra system, Wi-Fi and Wi-Max) engineer in Sudan Sea Port Corporation for four years and a head department of electrical and electronics engineering, faculty of engineering in Red Sea University for one year. He published papers on wireless communications and networking in peer-reviewed academic international journals and book chapters in big data clouds. His areas of research interest include MANETs, wireless networks, VANETs, image processing, computer networks, and Cloud computing.

Rasha Eltayeb Abd Elatif received her B.Sc. degree in aeronautical engineering, avionics from Sudan university of science and technology in 2006.She was a teacher assistant for one year in Sudan university of science and technology 2007-2008 then she worked as technical engineer in Sudan university of science and technology engineering college aeronautical department from 2008 to present. She mandated to Red Sea university department of electrical engineering since 2012. Her research interest on DSP, Mobile Networks and Routing Protocols.