VOL. 11, NO. 5, MARCH 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PREVENTION OF DDOS ATTACKS ON DISTRIBUTED CLOUD SERVERS BY PORT LOCK MECHANISM

R. Anandhi[1] and V. Naveen Raj[2]
[1]Department of Computer Science and Applications, D.G. Vaishnav College, Arumbakkam, Chennai, India
[2]Dr. Ambedkar Govt. Arts College, Vyasarpadi, Chennai, India
E-Mail: anandhi78@yahoo.com

ABSTRACT

Cloud computing is the process of using the network of remote hosted servers on the Internet. Cloud stores, manages and processes enormous amount of data without the use of local server or personal computers. The salient feature most share are on-demand scalability of highly available and reliable computing resources, secure access to metered services from anywhere and dislocation of data from inside of the organization to outside. While aspects of these features have been realized, still cloud computing remains a work in progress. Among them, one big challenge is about the security of data stored in cloud. The purpose of this paper is to provide an overview of cloud computing architecture and the security and privacy challenges involved. In specific, this paper deals with Distributed Denial of Service Attacks (DDOS) on the distributed cloud servers and also provides an effective solution to prevent those attacks by port lock mechanism using SFA algorithm (Server File Access algorithm).

Keywords: cloud computing, DDOS attacks, decryption, distributed cloud server, encryption, ports.

INTRODUCTION

Cloud Computing [1] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing consists of highly optimized datacenters. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization and other practicable efficiencies. But cloud computing is an emerging fro of distributed computing that is still in its infancy. The several deployment models [2] of cloud computing are:

a) Private cloud is wholly for an organization with more secured data.
b) Public cloud offers the highest level of efficiency and sharing among groups.
c) Community cloud is similar to private cloud, but the infrastructure and computational resources are shared by several organizations with common privacy.
d) Hybrid cloud is the composition of two or more private, public or community cloud.

Similarly the different service modes [3] supported by a cloud are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Figure-1 shows the differences in scope and control between the cloud subscriber and cloud provider for each of the service models.

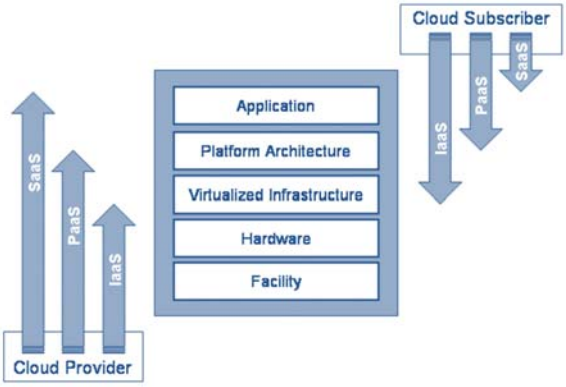

Figure-1. Cloud Deployment Models and Service Models.

Distributed cloud servers (Figure-2) of cloud datacenters are used to speed up the servers to shared computers and localized processes. The cloud provides software, hardware and information resources as per users need. Organization uses cloud available resources at minimal cost and uses scale up and scale down servers without expanding location and space. In recent studies, the data centres are prone to attacks for hacking the data.

MOTIVATION

The increased availability and use of social media and other publicly available sites [4] also have associated risks that are a concern, since they can negatively impact the security of the browser, its underlying platform, and cloud services accessed, through social engineering attacks. A successful defence against attacks requires securing both the client and server side of cloud computing. With emphasis typically placed on the latter, the former can be easily overlooked. Web browsers, a key

element for many cloud computing services, and the various available plug-ins and extensions for them are notorious for their security problems. Moreover, many browser add-ons do not provide automatic updates, increasing the persistence of any existing vulnerabilities. Data stored in the cloud typically resides in a shared environment collocated with data from other customers. Organizations moving sensitive and regulated data into the cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Many of the features that make cloud computing attractive can also be at odds with traditional security models and controls [5]. Determining the security of complex computer systems composed together is also a long-standing security issue that plagues large-scale computing in general, and cloud computing in particular. Organizational data must be protected in a manner consistent with policies, whether in the organization's computing center or the cloud. The organization must ensure that security and privacy controls are implemented correctly and operate as intended. Assessing and managing risk in cloud computing systems can be a challenge. Throughout the system lifecycle, risks that are identified must be carefully balanced against the security and privacy controls available and the expected benefits from their utilization. Too many controls can be inefficient and ineffective, if the benefits outweigh the costs and associated risks. 94% of threats to cloud servers are DDOS attacks [6]. So the paper deals with the approach how to control DDOS attacks on cloud datacenters in order to safeguard the data.

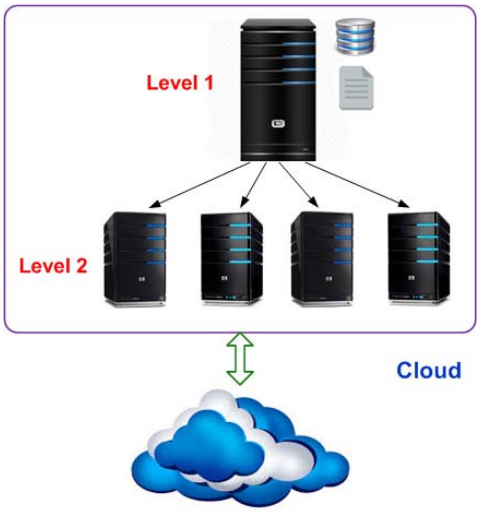

Figure-2. Distributed cloud servers.

DDOS Attacks

DDOS attacks stands for Distributed Denial of Service attacks [7]. The goal of these attacks is to slow down or entirely crash the server. The types of DDOS attacks:

1. **Smurf attacks [8]** means the attacker uses the features of smurf software to make the network totally inoperable. It makes use of IP (Internet Protocol) and ICMP (Internet Control Message Protocol) packets for this attack since these are used for error notification purpose during transfer. The node returns reply with an echo message in response to ping. The pings are sent as echo to reply back to the vulnerable address. So it creates more traffic on the cloud network which results in waste of bandwidth and server crashes since server is made to hear only a type of message. The cloud environment is prone to these attacks as it uses shared network components.

2. **SYNflood attack [9]** acts on three way handshake protocol. Recalling the normal handshaking protocol,

   a. Client sends SYN message to server
   b. Server sends ACK for the received SYN message to client
   c. Client sends ACK back to the server

Here the server will buffer the SYN request of the client until it receives proper ACK from client (i.e.) the connection is half-open. Using this, the attacker machine starts to work faster and it will now continuously send SYN message to the victim server. As the server works on the concept of timeout mechanism, since it does not receive ACK for the previous SYN message, it will drop out the connection and again indulge in new connection setup which also ends in failure.

3. **Ping of death [10]** means larger size of TCP/IP packets is sent to servers. Most networks and operating systems do not know how to respond to large sized packets. As a result, it will freeze and saturate without responding to any other requests. Heavy sized packets more than 65536 bytes will arrive at the server which leads to crash, since it is unable to handle such a large packets.

d. **Land attack [11]** means attackers set the IP address and port number of server as same. So if any request arrives at the server, machine may get confuse since it will look like same machine made request.

The main aim of DDoS attack is to make the network flood with unwanted packets so that even for authorized and legitimate users, the server will become unavailable. Since the source address of the packets is spoofed, the attacker machines will remain undetected. DDoS attacks are performed by a network of remote nodes called Zombies [12]. Attacker launches the attack with the help of zombies and targets the single system to make its resource unavailable to its beneficiaries. The target systems are flooded with requests from non-users, and often from non-visitors to the website. DDoS attacks create a huge amount of false traffic and as a result

legitimate traffic intended for authorized web users is slowed down or delayed. If the server becomes too slow, the network may be entirely useless to end users. DDoS attacks focus on three kinds of resources as Network, Application and Server [13].

EXISTING SYSTEMS

a. Firecol [14] system developed by J. Franccois model detects flooding DDoS attacks from the victim host. It hosts a botnet tracker to stop the operation of the remote control network. After tracking, Firecol shuts down the source and hence the system is protected from further attacks.
b. Rajdeep Singh [15] discussed attacks on MANET and suggested the methods to provide the security against the DDOS attacks.
c. Mukesh Kumar [16] proposed a methodology that can minimize a concrete kind of DDoS attack - flood attack.
d. A. Kazmanovic and E. W. Knightly [17] give two approaches to stop DDoS attacks. They are Statistical approach, which requires human involvement and Congestion Adaptation, which can apply only simplistic signatures.
e. Vikas Chouhan [18] proposed a system which uses hop count as their quantification to detect if the packet emanates from same source or different. But this system may again fail to estimate the Hop count if the assailant does not utilize the standard values for initial TTL in the packets.
f. J. Yuan [19] has suggested a method that will predicate on only on a few observation points to monitor the macroscopic effect of DDoS flooding attacks.

MATERIAL AND METHODS

Port lock mechanism

Above stated approaches work after the initiation of file access and they do not concentrate to secure the ports from which the access flows. So this paper focuses on the concept of securing the ports through which only file access and transfer occurs. The DDOS attack will often focus on the application layerand ports. In computer networking, a port [20] is an endpoint of communication in an operating system. While the term is also used for hardware devices, in software it is a logical construct that identifies a specific process or a type of service. The popular administrative ports in a server are TCP 22 and 3389. TCP 22 port [21] handles the full file system and TCP 3389 has the capability to show remote desktop screen on server. TCP 22 port is frequently used for Secure Shell (SSH), secure logins, file transfers and port forwarding. TCP 3389 port [22] is registered for Microsoft WBT Server, used for Windows Remote Desktop and Remote Assistance connections (RDP - Remote Desktop Protocol) and also used by Windows Terminal Server. This port is vulnerable to Denial of Service Attack against Windows NT Terminal Server. A remote attacker can quickly cause a server to reach full memory utilization by creating a large number of normal TCP connections to port 3389. Individual connections will timeout, but a low bandwidth continuous attack will maintain a terminal server at maximum memory utilization and prevent new connections from a legitimate source from taking place. Legitimate new connections will fail at this point with an error of either a connection timeout, or the terminal server has ended the connection. It should be noted that these ports are purely virtual since they are created and run by files. These ports can be logged by any machine geographically located.

If we lock the ports, it is unable for the hackers to steal the data. It is called as Port Lock Mechanism. It is surely efficient that firewalls since the firewalls do not restrict the malicious transfer as it asks the user itself to allow that file or not. Moreover, firewalls scan the purity of file only with the help of the valid sequences given by the user. The working of port lock mechanism is explained as follows:

First GPO (Group Policy Object) [23] will be built for users and files. GPO will handle the ports at server. A well-formed GPO will provide authorized and secured access towards the data at server. So locking the ports for bad users, port lock mechanism at level 1 server will aid for secured file access by level 2 servers. An authorized user will login the system with his user id and password. As a result, a trip password will be generated and sent to his network maid id. The trip password should be used within allotted time duration else it will expire and he has to request for a new trip password. The file system will be listed for that user. Let he wishes to access the file say “X”. Each and every file will be assigned with a key and password. In the distributed server architecture as shown in Figure 1, Level 2 servers will not have any rights to do any process while Level 1 holds the Master Server. If Level 2 servers want to access storage file at the Master Server, they need software to perform the process of administrative access transaction.

Secured File Access Algorithm-SFA algorithm

First the password P associated with the selected file F is divided into two passwords P1 and P2. Using the first half password P1, the full file will be encrypted as F’ by grouping every 3 characters. Next the encrypted file F’ will be again divided into 3 files-F1, F2 and F3. These three segments of files are again encrypted using the second half password P2. After the three segments F1’, F2’ and F3’ will be combined based on a combination technique into a single file F’’. This double encrypted file F’’ will only travel from Level 1 server to the requested Level 2 server. The encryption is done at the master server of level 1. The working of encryption procedure is given in the following Figure-3.

The decryption (Figure-4) will be taken in reverse order at the request placed Level 2 server (i.e) the received file F” will split into three segments-F1, F2 and F3. Those

segments will be decrypted using second half password P2. After decryption, the three segments will be combined to have file F'. Next the file F' will be decrypted using the first half password P1, which will give the original file F. The decryption is done at the file requested level 2 server. An additional security measure is adopted by the SFA algorithm during both encryption and decryption in file combining phase. If the 3 digit key is exactly divisible by 3, then the sequence of file segments to be combined is F3, F1 and F2 (Right Left Middle-RLM). If the 3 digit key leaves the remainder 1 after dividing by 3, the sequence of file to be combined is F2, F3 and F2 (Middle Right Left-MRL). If the 3 digit key leaves the remainder 2 after dividing by 3, the sequence of file to be combined is F2, F1 and F3 (Middle Left Right-MLR). The above said combination only will lead to a meaningful original text file else a wrong file will be resulted.

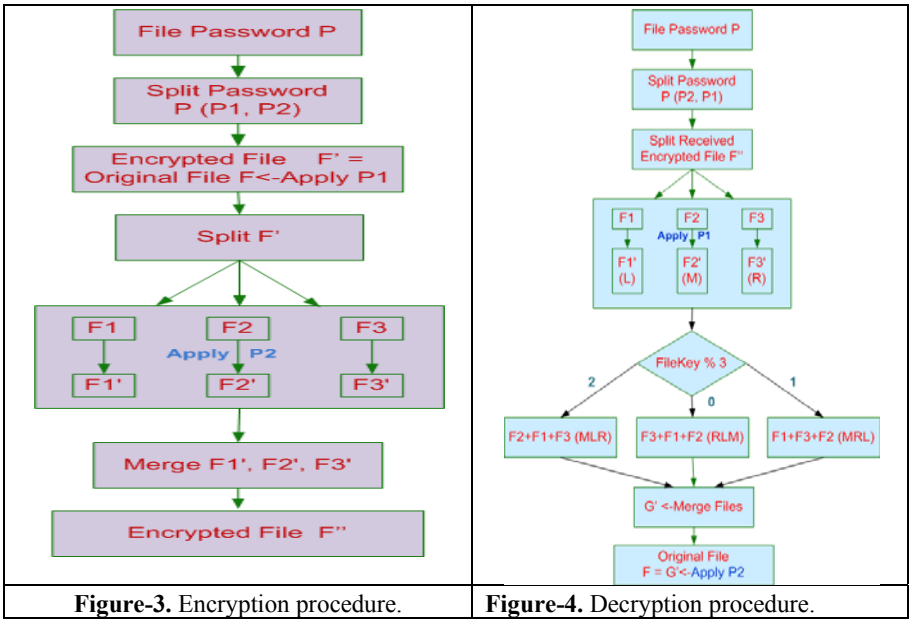

Figure-3. Encryption procedure.

Figure-4. Decryption procedure.

The following section shows the algorithm for file encryption and decryption. These algorithms will be helpful for secured file transfer without vulnerable to hacking.

ALGORITHM ENCRYPT (key, password)

```
//Initialize character set, charlist and replacelist (source and destination)
split passwords into two halves-p1 and p2
prepos=1
for i=0 to p1 {
        for k=0 to k<=length    step 3 {
                Tpos=((num(password[i])*prepos)*key) mod length
                For j=prepos to j%3==0 {
                //orderly changing character set on replace list based on Tpos return value
                prepos=j
                }
        }
//Assign characters in String for encrypt
prepos=password[i]
}
// file split into 3 parts and do encryption using p2
//Combine into single file as RLM, MRL or MLR fashion
```

END ENCRYPT.

ALGORITHM DECRYPT (key, password)

```
//split the files into 3 parts based on combined fashion-RLM, MRL or MLR
split passwords into two halves-p1 and p2
swap p1 and p2
prepos=1
for i=0 to p1{
        for k=0 to k<=length    step 3 {
                Tpos=((num(password[i])*prepos)*key) mod length
                for j=prepos to j%3==0 {
                //orderly changing character set on replace list based on Tpos return value
                prepos=j
                }
        }
Prepos=password[i]
}
//p1 processes the above resultant file and gets back the original file.
```

END DECRYPT.

Formula used in algorithm

T_{pos}= ((num (password[i]) * prepos) * key) (mod) length

Term used	Meaning
T_{pos}	Resultant character either during encryption or decryption
password	Password of file
key	Key of file
prepos	Previous Position
length	Character Set Length
num()	Function to convert character into number
i	Position of password character
mod	mod operator to generate remainder

Note

a) prepos for first character is 1.
b) Encrypt or decrypt for every 3 characters.
c) File key must be 3 digits.
d) File password will be at least 8 characters with combination of numbers, alphabets, special characters from the character set we use.

RESULTS AND DISCUSSIONS

Test bed uses Windows 7 operating system with Core i3 4th generation processor of 2.3GHZ speed. The time taken shown also includes the execution time taken by algorithm along with time spent at memory and CPU. Table-1 tabulates the results of port lock mechanism (i.e.) how the algorithm works to detect the attackers among the set of users logged into the system. The port lock mechanism however restricts the unauthorized users (attackers) from using the system.

Table-1. Detection of attackers by Port Lock Mechanism.

Logged-in users	Legitimate users	Attackers	Time to categorize users (Sec.)
3	2	1	1
2	2	0	1
5	3	2	2
11	7	4	4

The tables show the performance of SFA algorithm with one node at level 2 and five nodes at level 2. It is evident from the graphs drawn (Figure-5 and Figure-6) that the time taken for file transfer from Level 1 server along with encryption and decryption technology is not directly proportional to the file size. The data for the graphs drawn are correspondingly shown in Table-2 and Table-3.

Table-2. Encrytion and Decryption time taken with one node at Level 2.

Data (KB)	Encryption (Sec)	Decryption (Sec)
1	0.032	0.055
10	0.749	0.786
50	19.157	20.134
100	77.002	79.537

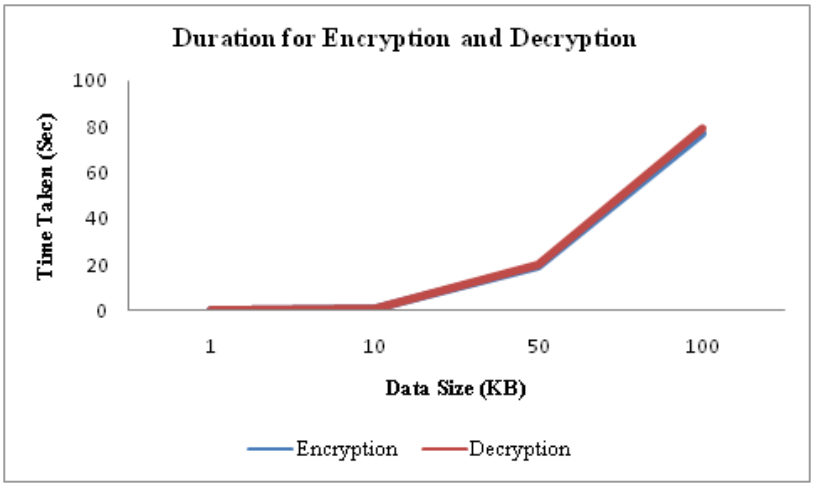

Figure-5. Graph showing the encryption and decryption time with one node at Level 2.

Table-3. Encryption and Decryption time taken with five nodes at Level 2.

Data (KB)	**Encryption** (Sec)	**Decryption** (Sec)
1	0.065	0.092
10	0.985	1.359
50	23.586	26.689
100	91.562	97.353

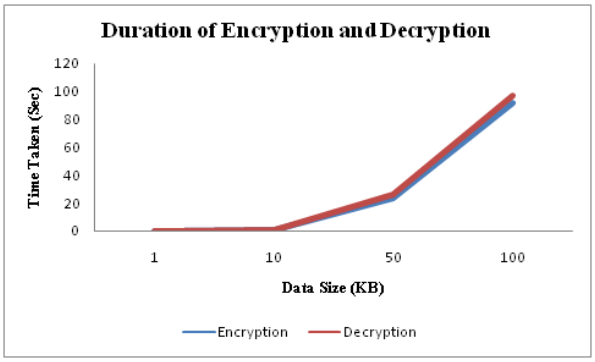

Figure-6. Graph showing the Encryption and Decryption time with five nodes at Level 2.

CONCLUSIONS

Cloud computing is recently emerged technology that has revolutionized the storage of large volume of data. The paper clearly explains about the port lock mechanism in distributed cloud server. It may avoid the denial of service attack of anonymous person. They are not able to try anything on the server because the administrative ports are locked and they can't use the port for sending floods and hence not able to handle files without authorization. A trip password method is used in order to make a valid session without keeping an unauthorized person idle in just watching the contents of file. Each file is also having a key and password and with the help of password, the SFA algorithm encrypts the file to be transferred and decrypts the file received. During decryption, the segments of file are combined in a fashion of MLR, RLM or MRL depending upon the key leaving the hackers unable to guess the combination to retrieve the original file. Hence one of the security threats in Cloud computing, DDOS attacks have been handled effectively by the above said SFA algorithms. This research word can be extended in future for transferring the multimedia files.

REFERENCES

[1] B. Furht and A. Escalante. 2010. Handbook of Cloud Computing: Springer. pp. 3-11.

[2] Mohiuddin Ahmed, Abu Sina Md. Raju Chowdhury, Mustaq Ahmed, Md. Mahmudul HasanRafee. 2012. An Advanced Survey on Cloud Computing and State-of-the-art Research Issues. IJCSI International Journal of Computer Science Issues, 9(Issue 1, No 1), ISSN (Online): 1694-0814, pp-201-207.

[3] Qi Zhang, Lu Cheng, Raouf Boutaba. 2010. Cloud Computing: State-of the-art and research challenges. The Brazilian Computer Society 2010.

[4] C. Wang, Q. Wang, K. Ren and W. Lou. 2012. Towards Secure and Dependable Storage Services in Cloud Computing. IEEE Trans. Service Computing. 5(2): 220-232.

[5] H. A. J. Narayanan and M. H. Gunes. 2013. Ensuring Access Control in Cloud Provisioned Health Care

Systems. Proceedings of the IEEE Consumer Communications and Networking Conference.

[6] Manpreet Kaur, Sahil Vashist. 2014. A Review of the DOS-DDOS Attacks and Their Prevention Mechanisms in Cloud. International Journal of Computer Application and Technology (IJCAT). 1(1), ISSN: 2349-1841.

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

[8] http://www.cert.org/techtips=denialofservice:html.

[9] S. Sanka, C. Hota and M. Rajarajan. 2010. Secure Data Access in Cloud Computing. Proceedings of the 4th IEEE International Conference on Internet Multimedia Services.

[10] Shuai Han, Jianchuan Xing. 2012. Ensuring Data Storage Security through a Novel Third Party Auditor Scheme in Cloud Computing. Proceedings of IEEE CCIS2011, 978-1-61284-204-2, pp. 264-268.

[11] S. Yu, C. Wang, K. Ren and W. Lou. 2010. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. Proceedings of the 29th IEEE International Conference on Information Communication. pp. 534-542.

[12] Upma Goyal, Gayatri Bhatti and Sandeep Mehmi. 2013. A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model. International Journal of Application or Innovation in Engineering and Management (IJAIEM). 2(3): 34-39.

[13] Mehmud Abliz. Internet Denial of Service Attacks and Defense Mechanisms. Department of Computer Science, University of Pittsburgh.

[14] J. Franccois, A. El Atawy, E. Al Shaer and R.Boutaba. 2007. A Collaborative Approach for Proactive Detection of Distributed Denial of Service Attacks.in Proc. IEEE MonAM, Toulouse, France.Vol. 11.

[15] Rajdeep Singh, Prajeet Sharma, Niresh Sharma. 2012. International Journal of Computer Applications. (0975-8887). 41(21).

[16] Mukesh Kumar, Naresh Kumar. 2013. International Journal of Application or Innovation in Engineering Management. (IJAIEM). 2(7), ISSN 2319- 4847.

[17] A. Kazmanovic and E. W. Knightly. 2003. Low-Rate TCP- Targeted Denial of Service Attacks, in Proc. Symp. Commun. Arch. Protocols, Karlesruhe, Germany. pp. 345-350.

[18] Vikas Chouhan, Sateesh Kumar Peddoju. 2012. Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing. International Journal of Computer Science and Electrical Engineering (IJCSEE), ISSN No. 2315-4209, Vol-1 Iss-1.

[19] J. Yuan K. Mills. 2005. Monitoring the Macroscopic Effect of DDoS Flooding attacks, IEEE Trans. Dependable and Secure Computing. 2(4): 324-335.

[20] https://en.wikipedia.org/wiki/Port_(computer_networking).

[21] https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

[22] www.speedguide.net / Ports Database.