ISSN:0975-9646

I. Mettildha Mary et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1803-1808

Secure Cloud Computing Environment against DDOS and EDOS Attacks

I. Mettildha Mary[1], P.V.Kavitha[2], Priyadharshini M[3], Vigneshwer S Ramana[4]

[1,2]*Asst.Professor/IT*, [3]*Asst. Professor(Sr.Gr)/IT*, [4]*UG Scholar/IT,*
Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India

Abstract Cloud computing is becoming one of the fastest growing field in the information technology. Cloud computing allows us to scale our servers in magnitude and availability in order to provide service to greater number of end users. Moreover, cloud service model are charged based on a pay-per-use basis of the cloud's server and network resource. In cloud computing where infrastructure is shared by potentially millions of users, Distributed Denial of Service (DDoS) attacks have the potential to have much greater impact than against single tenanted architectures. With this model, a conventional DDoS attack on server and network resources is transformed in a cloud environment to a new breed of attack that targets the cloud user's economic resource, namely Economic Denial of Service attacks. In this paper, we 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.

1. INTRODUCTION

Cloud computing is currently one of the most hyped information technology areas and has become one of the fastest growing segments in IT industry. Due to the flexibility, pay per use, elasticity, scalability, and other attributes promised by this paradigm, it gained the interest of large organizations and corporate for hosting their services onto the cloud. However, the ability to respond to security threats and events is listed as one of the main issues of concern in cloud computing.

Cloud computing allows us to scale up our servers and to serve a large number of requests for a service. The introduction of resource-rich cloud computing platforms, where users are charged based on the usage of the cloud's resources, known as "pay-as-you-use" or utility computing, has transformed the Distributed Denial of Service (DDoS) attack problem in the cloud to a financial one. This new type of attack targets the cloud adopter's economic resources, and is referred to as Economic Denial of Service or Sustainability (EDoS) attack.

Distributed Denial of Service is a type of attack that aims to make services or resources unavailable for indefinite amount of time by flooding it with useless traffic. The two main objectives of these attacks are, to exhaust computer resources (CPU time, Network bandwidth) so that it makes services unavailable to legitimate users.

In a general DDoS attack, the attacker usually disguises or 'spoofs' the IP address section of a packet header in order to hide their identity from their victim. This makes it extremely difficult to track the source of the attack. IP trace back is a scheme that provides an effective way to trace the source of DDoS attacks to its point of origin.

What makes this more disastrous is that it is extremely difficult to selectively filter the malicious traffic without impacting the service as a whole. This also means that any proposed mitigating technique must be highly intelligent; otherwise, the technique itself could be utilized by the attackers as a source of EDoS attack.

In this work, we propose a novel mitigation technique against DDos&EDoS attack in Cloud Computing, namely DDoS&EDoS Shield. The main idea 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. Cloud Trace Back model (CTB) is based upon Deterministic Packet Marking (DPM) algorithm [1][2]. However this work will check the Cloud Trace Back model using Flexible Deterministic Packet Marking, which provides a defence system with the ability to find out the real sources of attacking packets that traverse through the network [8].this technique is more efficient for avoid DDoS attacks.

EDoS attacks are shielded by forwarding the first request to a verifier node in our proposed architecture. This verifier node is responsible for the verification process and for updating the white and black lists based on the results of this verification process. The subsequent requests coming from the bots will be blocked by a virtual firewall since their IP addresses will be found in the black list. On the other hand, the subsequent requests coming from legitimate clients will be forwarded directly to the target cloud service since their IP addresses will be found in the white list. As a result, only the requests from legitimate clients will reach the target cloud service and thus mitigating the EDoS attack.

Our contributions are as follows: Section 2 introduces Cloud Trace Back model and Cloud protector. Section 3 introduces EDoS-shield and EdoS mitigation architecture. Section 4 discusses the algorithmic approach of EDoS & DDoS and section 5 summarizes, draws conclusions and indicates direction for further research.

2. CLOUD TRACE BACKMODEL AND CLOUD PROTECTOR

The main focus of proposed model shown in Fig. 1 is to offer a solution to Trace Back through our application module Cloud Trace Back (CTB) to find the source of DDoS attacks, and introduce the use of a back propagation neutral network, called Cloud Protector, which was trained to detect and filter such attack traffic.Techniques for mitigating EDoS attacks are much needed for protecting the cloud infrastructure against the rippling effect of cost incurred on legitimate users through EDoS attacks. In our research we couple the DDoS Protecting techniques of

CTB, CP and EDoS protecting techniques of V-Nodes and Virtual Firewalls.These are acts like a shield for DDoS & EDoS attacks

2.1Cloud Trace back (CTB)

Cloud Trace Back Architecture's (CTB) main objective is to apply a SOA approach to Trace Back methodology, in order to identify the true source of a DDoS. CTB is based upon Deterministic Packet Marking (DPM) algorithm.DPM marks the ID field and reserved flag within the IP header. As each incoming packet enters an edge ingress router it is marked, outgoing packets are usually ignored. The marked packets will remain unchanged for as long as the packet traverses the network.

We propose, in a CTB framework, to employ the FDPM methodology by placing our Cloud Trace Back Mark (CTM) within a web service message [6]. CTB is deployed at the edge routers in order to be close to the source end of the cloud network. Usually, if no security services are in place for web services, the system becomes quite vulnerable to attacks. Fig.1 demonstrates how CTB can remedy this by being located before the Web Server, in order to place a Cloud Trace Back Mark (CTM) tag within the CTB header. As a result, all service requests are first sent to the CTB for marking, thereby effectively removing the service provider's address and preventing a direct attack. If an attack is discovered or was successful at bringing down the web server, the victim will be able to recover and reconstruct the CTM tag and as a result reveal the identity of the source.

In an attack scenario, the attack client will request a web service from CTB, which in turn will pass the request to the web server. The attack client will then formulate a SOAP request message based on the service description. Upon receipt of SOAP request message, CTB will place a CTM within the header. Once the CTM has been placed, the SOAP message will be sent to the Web Server. Upon discovery of an attack, the victim will ask for reconstruction to extract the mark and inform them of the origin of the message. The reconstruction will also begin to filter out the attack traffic. The message is normal, the SOAP message is then forwarded to the request handler for processing.

Upon receipt of the SOAP request; the Web Service will prepare a SOAP response. The web server then takes the SOAP response and sends it back to the client. as part of the HTTP response. CTB will not interfere with the response requests or any outgoing message.

2.2Cloud Protector

CTB does not directly eliminate a DDoS attack message.This is left for the filter section of a defence system called Cloud Protector. The Cloud Protector is a trained back propagation neural network (NN), to help detect and filter out DDoS messages. A neural network is a set of connected units made up of input, hidden and output layers [4] [5].

Each of the connections in a neural network has a weight associated with it. In a neural net the focus is on the threshold logic unit (TLU).

The TLU inserts input objects into an array of weighted quantities and sums them up to see if they are above the threshold. The cloud protector system is implemented in five different phases as shown in Fig. 2 and described below.

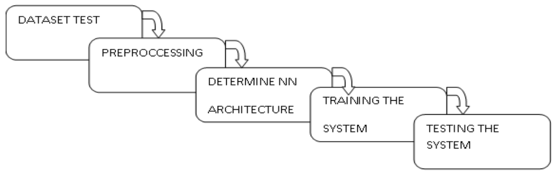


Fig. 2: Implementation phases

2.2.1 Dataset for Training and Testing

The efficiency of the neural network depends on the training data. If the training data is more accurate then Performance of trained system will be improved. Therefore collecting of data for training is a critical problem. This can be obtained by three ways as by using real traffic, by using sanitized traffic and by using simulated traffic [1]. The third and the most common way to obtain data are to create a tested network and generate background traffic on this network. In the tested environment, background traffic is generated either by using complex traffic generators modelling actual network statistics, or by using simpler commercial traffic generators creating small number of packets at a high rate.

2.2.2 Pre-processing Dataset

The data set is pre-processed so that it may be able to give it as an input to the developed system. This data set consists of numeric and symbolic features and it is converted in numeric form so that it can be given as inputs to required neural network. Now this modified data set is ready to be used as training and testing of the neural network.

2.2.3 Determining the NN architecture

There is no certain mathematical approach for obtaining the optimum number of hidden layers and their neurons. For choosing optimum set of hidden layers and its no. of neuron a comparison is made for many cases and optimum is selected.

3. EDOS SHIELD AND EDOS MITIGATION ARCHITECTURE AND APPROACH

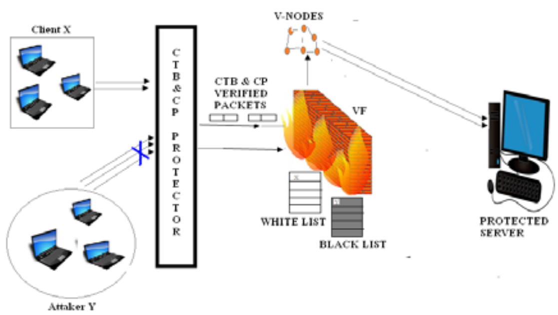


Fig.1: The Proposed Model

Fig. 1 shows the proposed architecture of the DDoS & EDoS shield for mitigating the EDoS in a cloud computing environment. The main components of the architecture are virtual firewalls (VF) and verifier cloud nodes (V-Nodes).

The virtual firewalls work as filter mechanisms based on white and black lists that hold IP addresses of the originating nodes. And, the verifier cloud nodes update the lists based on the results of the verification process.

The virtual firewall can be implemented in the cloud as a virtual machine that has the capabilities of filtering and routing. The VF uses two lists, a white list and a blacklist, to make a decision regarding the incoming packets from outside the cloud and destined to some services hosted in the cloud.

The whitelist is used to track the authenticated source IP addresses so that the incoming traffic originating from these addresses will be allowed to pass the firewall towards the destined services. The blacklist is used to hold those unauthenticated source IP addresses so that the firewall will drop the incoming packets originating from these IP addresses, these two lists have to be updated periodically.

Another component in our proposed architecture is the verifier nodes (V-Nodes) which are represented by a pool of virtual machine nodes implemented based on the cloud infrastructure. The V-Nodes constitute a cloud-based overlay network. A V-Node has the capabilities to verify legitimate requests at the application level using unique Turing tests, such as UNIQUE QUESTION TESTING. Another role of the VNode is to update the lists used by the VF as was explained earlier.

If the application request gets verified successfully, then the source IP address of that request will be added to the whitelist and the request will be forwarded to the destined service in the cloud. All the subsequent packets passing through the VF and having this IP address as a source address will be forwarded to the destined service. If the application request fails, then the source IP address of that request will be added to the blacklist, and subsequent packets originating from that source IP address will be dropped.

Fig. 2 shows a case of a legitimate request from a client *X*, where the first request gets verified by a V-Node and passes the Question test.

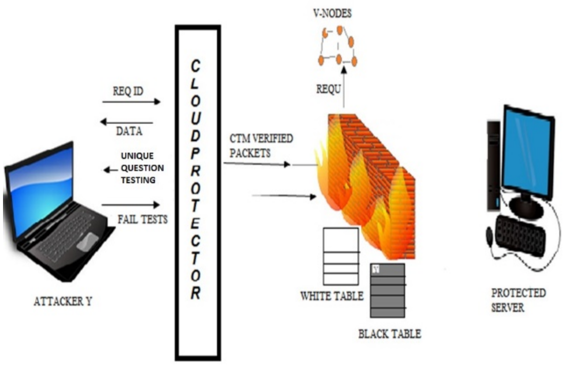


Fig.2: Normal Request Scenario

Thus, its source IP address, *X*, has been added to the whitelist and the subsequent requests from *X* to the destination *D* have been forwarded directly to *D*.

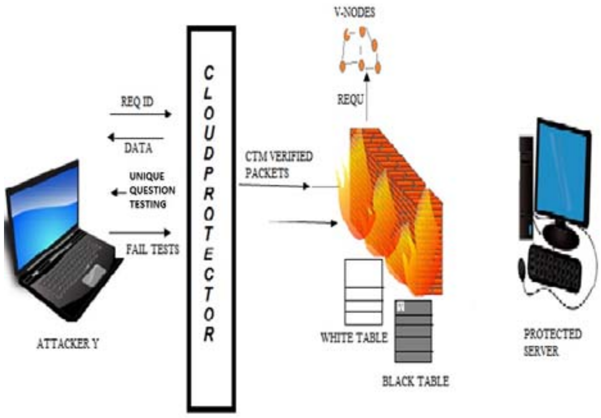


Fig. 3 Shows a case of a request coming from an attacker (a bot), *Y*, where the first request gets verified by a V-Node and fails the Turing test.

Thus, its source IP address, *Y*, has been added to the blacklist and the subsequent requests from *Y* to the destination *D* have been blocked by the VF.

Since the requests originating from the bots, i.e., compromised machines, will fail at the verification stage, all the automated malicious requests will not reach the victim in the cloud. Therefore, the customer will not be charged for such attacker

3.1Security Issues

The goal of such proposed architecture is to mitigate the risk of the EDoS attacks against the cloud services. The main idea is to verify whether a request coming from a user is originated by a human or it is an automated one.

The objective of such verification is to distinguish between legitimate and malicious users. This is achieved by directing the first request to a V-Node that is responsible for the verification process using UNIQUE QUESTION TESTING.

The subsequent requests coming from the bots will be blocked by the VF (because they will fail the verification phase) and will not reach the victim (i.e., customer) and thus the customer will not be charged for these requests. Such proposed architecture is mainly used for protecting the cloud application services from the impact of application EDoS attacks. The non-HTTP traffic such as network layer attacks which targets the protected cloud service will be dropped by the VF pass through it. One challenge related to security is the IP spoofing attacks. These are more dangerous for cloud resources and services in the public and private cloud network.

This is due to the fact that we are mainly protecting cloud application services, and the cloud infrastructure only allows Web traffic to For our proposed decision to forward a packet or to drop it is mainly based on the source IP address present in the white and black lists. To overcome such problem, techniques like could be used to detect and prevent the IP spoofing attacks.

Algorithm 1 and Algorithm 2 show the actions taken by the VF and the V-Node when considering that the architecture is protected against the IP spoofing attacks.

3.2 Deployment

Regarding the deployment of our proposed technique, the proposed architecture requires no modifications in the client side, the protected cloud service side, or the Internet network protocols. It requires only deploying a VF in the cloud computing system infrastructure and implementing V-Nodes as a pool of virtual machines which can grow in numbers to defeat the DDoS attack based on the scalability property of the cloud computing system.

3. ALGORITHMIC APPROACH FOR DDOS & EDOS ATTACKS

Algorithm 1: CTM Actions

If (CTP places CTM in header)
{
Soap message will be sent to the server
}
Else
{
Wait for place the CTM in headers
}
End if

If (Soap message sent to web server=TRUE)
{
If (verifies the message=no victims)
{
SOAP message is then forwarded to the request handler for processing to the web server (Respond to HTTP Request).
}
Else
{
Ask for reconstruction to extract the mark and inform them of the origin of the message.
}
End
End

Algorithm 1: VF Actions

Input:
P ← Packet
S← Packet source IP address
D← Packet destination IP address
B← Blacklist
W←Whitelist
Begin:
If (S∈W && S∉B)
Forward P to D
Else If (S ∈B) **Drop** p **Else** forward p to a V-node **End**

Algorithm 2: V-NODE Actions

Input:
P ←Packet
S← Packet source IP address
D← Packet destination IP address
B← Blacklist
W←Whitelist
Begin:
If (S ∉B && S∉W) {
Send to S a unique Question test
If (Question test passes) {
W_W+S
Forward P to D.
}
Else
B_B+S
END

3.3 FDPM MARKING SCHEME

3.3.1 The Encoding Procedure

Before the FDPM mark can be generated, the length of the mark must be determined based on the network Protocols deployed within the network to be protected. According to different situations, the mark length could be 24 bits long at most, 19 bits at middle, and 16 bits at least

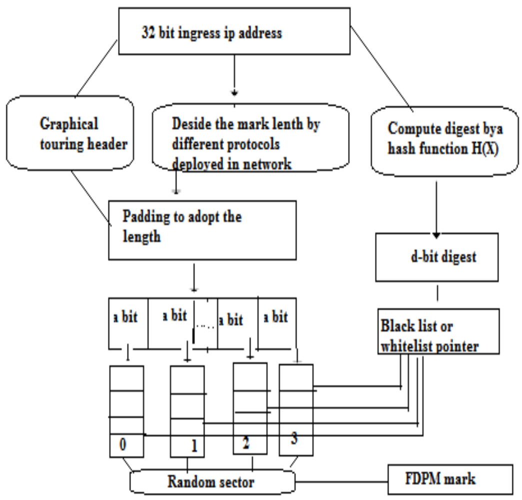


Fig. 4: FPDM encoding procedure

3.3.2 The Reconstruction Procedure

Mark recognition and Address recovery are the two main steps of the reconstruction procedure. The mark recognition step is the reverse process of the encoding process.

By reading the control fields in the mark, the length of the mark and which fields in the IP header store the mark can be recognized. If the RF is 0, the mark length is 24 (both TOS and ID are deployed). If the RF is 1, according to different protocols of TOS used, the mark length is 16 or 19. The second step, address recovery, analyzes the mark and stores it in a recovery table. It is a linked-list table; the number of rows is a variable, and the number of columns in the table is **k**, representing the number of segments used to carry the source address in the packets. Here, the segment number is used to correlate the data into the correct order. The row of the table means the entry and each digest owns one entry (source IP address).

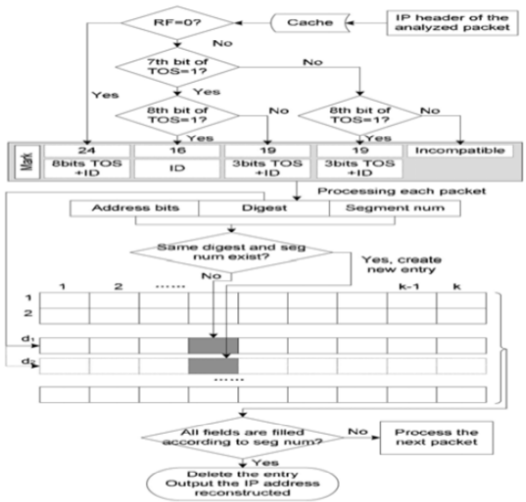


Fig. 5 : FDPM reconstruction scheme

Fig. 5 shows the reconstruction scheme. When all fields in one entry are filled according to the segment number, this source IP address is reconstructed and the entry in the recovery table is then deleted.

4. RESULT AND DISCUSSION

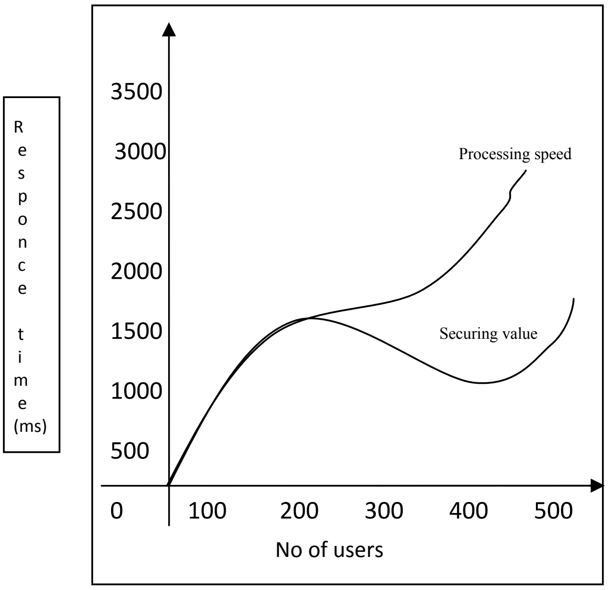
4.1 Training and Testing

The result of the Cloud Protector shown in Fig. 7(a, b) demonstrates that on its training sets it detected around 91% of with a miss rating of 9%. Also, against the test dataset, the results slightly varied down by 3% (88% of attack traffic).

In Fig.6: it consists only the Cloud trace back and Cloud Protector techniques it may lead to allow the un trusted packets when they have same cloud trace back messages while using it in resources So these leads unsafety for the resources. But in our solution in this CTB and CP relatively coupled with the virtual firewall and v-nodes so it can provide the advance security for the repeated or same attackers spoofing packets.

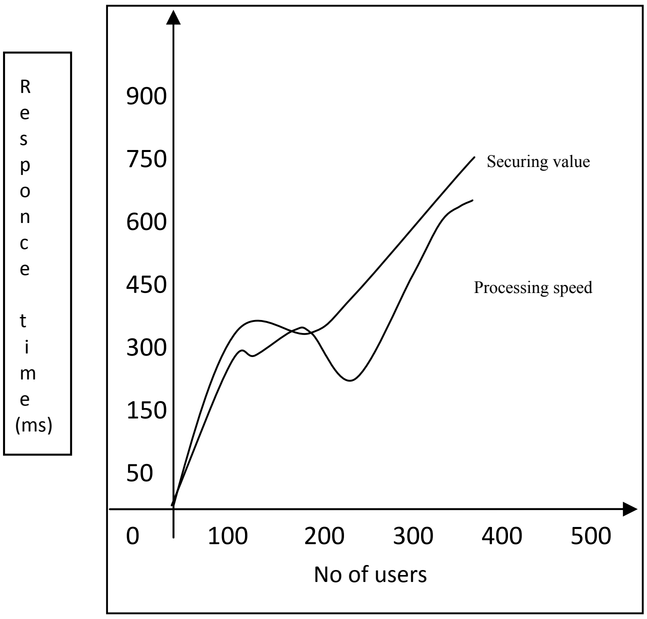
In our novel solution it may lead to the very effective performance compared with CTB & CP because it coupled with EDOS shield techniques. And it can provide the very effective security from the any type of service oriented or resource oriented attacks.

The main issue from the results was that the response time varied significantly from being able to detect the attack traffic within a matter of 9 ms to 20-30ms. One hypothesis is that the dataset was scattered far apart, and so the error ratio within the neural network kept fluctuating. Another hypothesis is that it could be the back propagation. These results are at 4 Neuron Layers, Learning Rate of 0.2, Momentum of 0.6, and a variable threshold of 0.1.



Only CTB & CP in HTTP Request

Fig. 6.a: Training set results



CTP, CP WITH VF & VNODE in HTTP Requests

Fig. 6.b: Testing set results

5. CONCLUSION

The cloud computing model has the ability to scale computer resources on demand, and give users a number of advantages to progress their conventional cluster system. In fact the total cost of going towards cloud is almost zero when resources are not in use. Therefore it is no wonder that academic research and industry are moving towards cloud computing. However, Security should in fact be implemented it along side functionality and performance. One of the most serious threats to cloud computing security itself comes from Distributed Denial of Service attacks. These types of attacks are simple and easy to implement by the attacker, but to security experts they are twice as difficult to stop. So, a solution model is offered to Trace Back through proposed Cloud Trace Back (CTB) to find the source of real attacks, and introduce the use of a back propagation neutral network, called Cloud Protector, Economic Denial of Sustainability attacks are more relatively connected to the economical resources coupled to the cloud environment those are should be secured. This was trained to detect and filter such attack traffic. The result we achieved was around 88% and 91%, for testing and training datasets, respectively. The proposed model's results show that it is able to detect most of the attack messages within a very short period of time. We also show that CTB can successfully traceback 75-81% In the future, we will be setting up to begin real-time data gathering and testing of Cloud Protector. This will allow us to fine tune CTB to better detect and filter DDoS attacks and the vframe and vnode actions are the best approaches to shield the DDoS & EDoS attacks. Here we join the DDoS and EDoS security approaches so it leads the best filtering and shielding mechanism for DDoS and EDoS attacks.

REFERENCES

[1]Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi,"Securing cloud computing environment against ddos attacks"International Conference on Communication, Volume 5.

[2]Edos-Shield - A Two-Steps Mitigation Technique against Edos Attacks In Cloud Computing," 2011 Fourth IEEE International Conference on Utility and Cloud Computing"

[3]Lizhe W. and Gregor V. L., (2008), "Cloud Computing: a Perspective Study," New Generation Computing Volume 28, Number 2, 137-146, DOI: 10.1007/s00354-008-0081-5

[4]Trostle J, (2006), "protecting Against Distributed Denial of service attacks Using Distributed Filtering," Securecomm and Workshops, Aug 28 2006- sept1 2006, pp 1-11

[5]Iftikhar A., Azween B. A., Abdullah S.A.,(2009), "Application of Artificial neural Network in Detection of DoS attacks," SIN'09, Oct 6-10.

[6]Bhaskaran M., Natrarajan.A.M. and Sivanandam. S.N.,(2007),"Trace Backing the Spoofed IP Packets in Multi ISP Domains with"Secured Communication," IEEE-ICSCN 2007, pp 579-584.

[7]Chonka A, Xiang Y., Zhou W., Allusion. (2010), "Cloud Security defenses to protect cloud computing against HTTP-DoS and XML – DoS attacks," Journal of Network and Computer Applications, doi: 10.1016/j.jnca.2010.06.004.