International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 1, January - 2014

Secure Cloud Computing Environment Against DDoSand EDoS Attacks

Vigneshwer. S. Ramana
Department of IT

Seenivasan. S
Department of IT,

TharmaDurai. M
Department of IT,

M. Priyadharsini
Assitant Professor
Sri Ramakrishna Engineering College, Coimbatore

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 hypedinformation technology areas and has become one of thefastest growing segments in IT industry. Due to theflexibility, pay per use, elasticity, scalability, and otherattributes promised by this paradigm, it gained the interest oflarge organizations and corporate for hosting their servicesonto the cloud. However, the ability to respond to securitythreats and events is listed as one of the main issues ofconcern in cloud computing.

Cloud computing allows us to scale up our servers and toserve a large number of requests for a service. Theintroduction of resource-rich cloud computing platforms,where users are charged based on the usage of the cloud'sresources, 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 typeof attack targets the cloud adopter's economic resources, andis referred to as Economic Denial of Service or Sustainability (EDoS) attack.

Distributed Denial of Service is a type of attack thataims to make services or resources unavailable for indefinite amount of time by flooding it with useless traffic. Thetwo main objectives of these attacks are, to exhaustcomputer 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 DDoSattacks to its point of origin.

What makes this more disastrous is that it is extremelydifficult to selectively filter the malicious traffic withoutimpacting the service as a whole. This also means that anyproposed mitigating technique must be highly intelligent;otherwise, the technique itself could be utilized by theattackers as a source of EDoS attack.

In this work, we propose a novel mitigation techniqueagainst DDos&EDoS attack in Cloud Computing, namely DDoS&EDoSShield. The main idea is to verify whether the requestscoming from the users are from a legitimate person orgenerated by bots.This work will test the efficiency of a Cloud Trace Backmodel 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 CloudTrace Back model using Flexible Deterministic PacketMarking, which provides a defence system with the abilityto find out the real sources of attacking packets that traversethrough 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 proposedarchitecture. Thisverifier node is responsible for the verification process andfor updating the white and black lists based on the results ofthis verification process. The subsequent requests comingfrom the bots will be blocked by a virtual firewall since theirIP addresses will be found in the black list. On the otherhand, the subsequent requests coming from legitimate clientswill be forwarded directly to the target cloud service sincetheir IP addresses will be found in the white list. As a result, only the requests from legitimate clients will reach the targetcloud service and thusmitigating the EDoS attack.

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

2. CLOUD TRACE BACKMODEL AND CLOUD PROTECTOR

The main focus of proposed model shown in Fig. 1 is tooffer a solution to Trace Back through our applicationmodule Cloud Trace Back (CTB) to find the source ofDDoS attacks, and introduce the use of a back propagationneutral network, called Cloud Protector, which was trainedto detect and filter such attack traffic.Techniques for mitigating EDoS attacks are much neededfor protecting the cloud infrastructure against the ripplingeffect 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 objectiveis is to apply a SOA approach to Trace Back methodology, inorder to identify the true source of a DDoS. CTB is basedupon 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 ismarked, outgoing packets are usually ignored. The markedpackets will remain unchanged for as long as the packettraverses the network.

We propose, in a CTB framework, toemploy the FDPM methodology by placing our Cloud TraceBack Mark (CTM) within a web service message [6]. CTBis deployed at the edge routers in order to be close to thesource end of the cloud network. Usually, if no securityservices are in place for web services, the system becomesquite vulnerable to attacks. Fig.1 demonstrates how CTBcan remedy this by being located before the Web Server, inorder to place a Cloud Trace Back Mark (CTM) tag withinthe CTB header. As a result, all service requests are firstsent to the CTB for marking, thereby effectively removingthe service provider's address and preventing a direct attack.If an attack is discovered or was successful at bringingdown the web server, the victim will be able to recover andreconstruct the CTM tag and as a result reveal the identity ofthe source.

In an attack scenario, the attack client will request a webservice from CTB, which in turn will pass the request to theweb server. The attack client will then formulate a SOAPrequest message based on the service description. Uponreceipt of SOAP request message, CTB will place a CTMwithin the header. Once the CTM has been placed, theSOAP message will be sent to the Web Server. Upondiscovery of an attack, the victim will ask for reconstructionto extract themarkand inform them of the origin of themessage. The reconstruction will also begin to filter out theattack traffic. The message is normal, the SOAP messageis then forwarded to the request handler for processing.

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

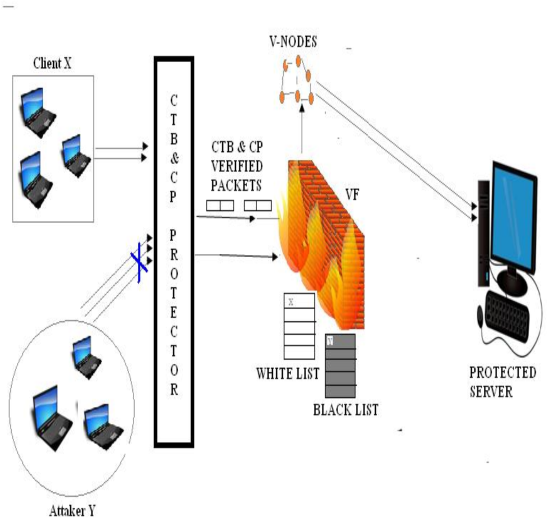


Fig.1: The Proposed Model

2.2Cloud Protector

CTB does not directly eliminate a DDoS attack message.This is left for the filter section of a defence systemcalledCloud Protector. The Cloud Protector is a trained backpropagation neural network (NN), to help detect and filterout DDoS messages. A neural network is a set of connectedunits made up of input, hidden and output layers [4] [5].
Each of the connections in a neural network has a weightassociated with it. In a neural net the focus is on thethreshold logic unit (TLU).
The TLU inserts input objectsinto an array of weighted quantities and sums them up to seeif they are above the threshold. The cloud protector system isimplemented in five different phases as shown in Fig. 2 anddescribed below.

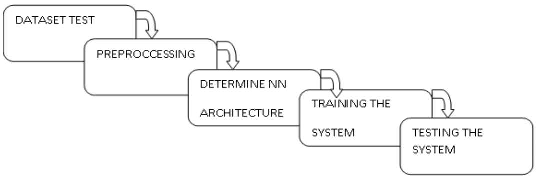


Fig. 2: Implementation phases

2.2.1 Dataset for Training and Testing

The efficiency of the neural network depends onthe training data. If the training data is more accurate thenPerformance of trained system will be improved. Thereforecollecting of data for training is a critical problem. This canbe obtained by three ways as by using real traffic, by usingsanitized traffic and by using simulated traffic [1]. The thirdand the most common way to obtain data are to create atested network and generate background traffic on thisnetwork. In the tested environment, background traffic isgenerated either by using complex traffic generatorsmodelling actual network statistics, or by using simplercommercial traffic generators creating small number ofpackets at a high rate.

2.2.2 Pre-processing Dataset

The data set is pre-processed so that it may be able togive it as an input to the developed system. This data setconsists of numeric and symbolic features and it isconverted in numeric form so that it can be given as inputsto required neural network. Now this modified data set isready to be used as training and testing of the neuralnetwork.

2.2.3 Determining the NN architecture

There is no certain mathematical approach forobtaining the optimum number of hidden layers and theirneurons. For choosing optimum set of hidden layers and itsno. of neuron a comparison is made for many cases andoptimum is selected.

3. EDOS SHIELD AND EDOS MITIGATIONARCHITECTURE AND APPROACH

Fig. 1 shows the proposed architecture of the DDoS & EDoS shieldfor mitigating the EDoS in a cloud computingenvironment. The main components of the architecture arevirtual firewalls (VF) and verifier cloud nodes (V-Nodes).The virtual firewalls work as filter mechanisms based onwhite and black lists that hold IP addresses of the originatingnodes. And, the verifier cloud nodes update the lists based onthe results of the verification process.
The virtual firewall can be implemented in the cloud as avirtual machine that has the capabilities of filtering androuting. The VF uses two lists, a white list and a blacklist, tomake a decision regarding the incoming packets fromoutside the cloud and destined to some services hosted in thecloud.
The whitelist is used to track the authenticated sourceIP addresses so that the incoming traffic originating fromthese addresses will be allowed to pass the firewall towardsthe destined services. The blacklist is used to holdthose unauthenticated source IP addresses so that the firewall willdrop the incoming packets originating from these IP addresses, these two lists have to be updated periodically.
Another component in our proposed architecture is theverifier nodes (V-Nodes) which are represented by a pool ofvirtual machine nodes implemented based on the cloudinfrastructure. The V-Nodes constitute a cloud-based overlaynetwork. A V-Node has the capabilities to verify legitimaterequests at the application level using unique Turing tests, such as UNIQUE QUESTION TESTING. Another role of the VNodeis to update the lists used by the VF as was explainedearlier.
If the application request gets verified successfully, then the source IP address of that request will be added to thewhitelist and the request will be forwarded to the destinedservice in the cloud. All the subsequent packets passingthrough the VF and having this IP address as a sourceaddress will be forwarded to the destined service. If theapplication request fails, then the source IP address of thatrequest will be added to the blacklist, and subsequent packetsoriginating from that source IP address will be dropped.

Fig. 1 shows a case of a legitimate request from a client*X*, where the first request gets verified by a V-Node andpasses the Question test.

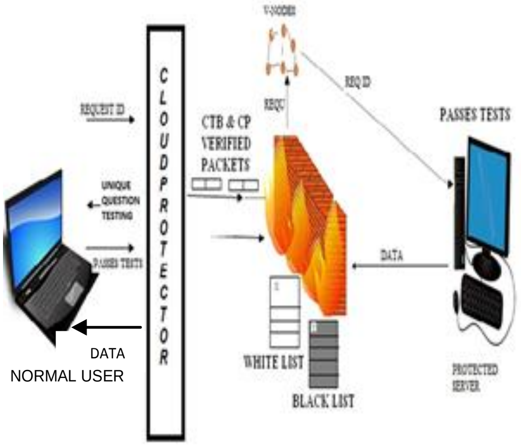


Fig.3: Normal Request Scenario

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

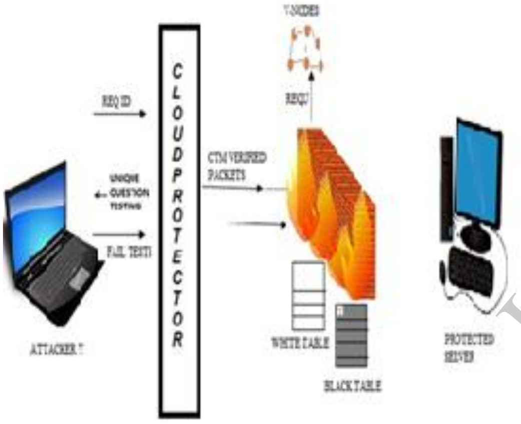


Fig.4: Request from Hacker

Fig. 4 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*, hasbeen 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, allthe automatedmalicious requests will not reach the victim inthe cloud. Therefore, the customer will not be charged forsuch attacker

3.1Security Issues

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

Theobjective of such verification is to distinguish betweenlegitimate and malicious users. This is achieved by directingthe first request to a V-Node that is responsible for theverification process using UNIQUE QUESTION TESTING.

The subsequentrequests coming from the bots will be blocked by the VF(because they will fail the verification phase) and will notreach the victim (i.e., customer) and thus the customer willnot be charged for these requests.Such proposed architecture is mainly used for protectingthe cloud application services from the impact of applicationEDoS attacks. The non-HTTP traffic such as network layerattacks which targets the protected cloud service will bedropped 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 infrastructureonly allows Web traffic to For our proposed decision to forward a packet or to drop it is mainly based onthe source IP address present in the white and black lists. Toovercome 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 theVF and the V-Node when considering that the architecture isprotected against the IP spoofing attacks.

3.2 Deployment

Regarding the deployment of our proposed technique, theproposed architecture requires no modifications in the clientside, the protected cloud service side, or the Internet networkprotocols. It requires only deploying a VF in the cloudcomputing system infrastructure and implementing V-Nodesas a pool of virtual machines which can grow in numbers todefeat the DDoS attack based on the scalability property ofthe 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 messageis then forwarded to the request handler for processing to the web server (Respond to HTTP Request).
}
Else
{
Ask for reconstructionto extract the mark and inform them of the origin of themessage.
}
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 ($S \epsilon W$ && $S \notin B$)
Forward P to D
Else If ($S \epsilon B$)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 ($S \notin B$ && $S \notin W$) {
Send to S a uniqueQuestion test
If (Question test passes) {
W_W+S
Forward P to D.
}
Else
B_B+S
END
```

3.3FDPM MARKING SCHEME

3.3.1 The Encoding Procedure

Before the FDPM mark can be generated, the lengthofthemark must be determined based on the networkProtocols deployed within the network to be protected.According to different situations, the mark length could be24 bits long at most, 19 bits at middle, and 16 bits atleast

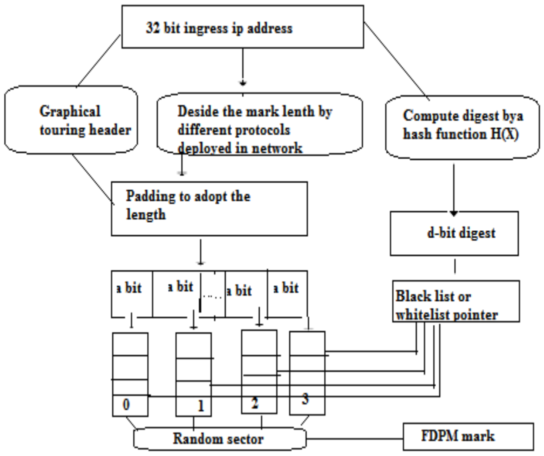

32 bit ingress ip address
Graphical touring header
Deside the mark lenth by different protocols deployed in network
Compute digest bya hash function H(X)
Padding to adopt the length
d-bit digest
a bit
a bit
a bit
a bit
Black list or whitelist pointer
0
1
2
3
Random sector
FDPM mark

Fig. 5: FPDM encoding procedure

3.3.2The Reconstruction Procedure

Mark recognition and Address recovery are the twomain steps of the reconstruction procedure. The markrecognition step is the reverse process of the encodingprocess.

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

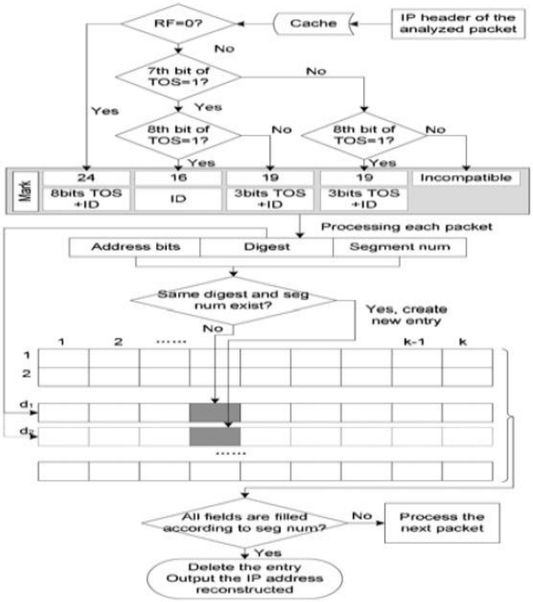


Fig. 6: FDPM reconstruction scheme

Fig. 6 shows the reconstruction scheme. When all fieldsin one entry are filled according to the segment number, thissource IP address is reconstructed and the entry in therecovery table is then deleted.

4. RESULT AND DISCUSSION

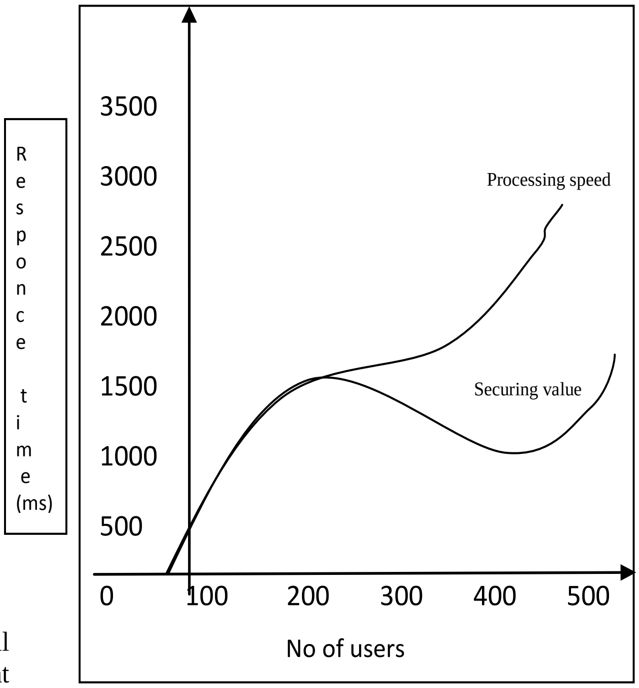
4.1 Training and Testing

The result of the Cloud Protector shown in Fig. 7(a, b) demonstrates that on its training sets it detected around91% of with a miss rating of 9%. Also, against the testdataset, the results slightly varied down by 3% (88% ofattack traffic).

In Fig.5: 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.

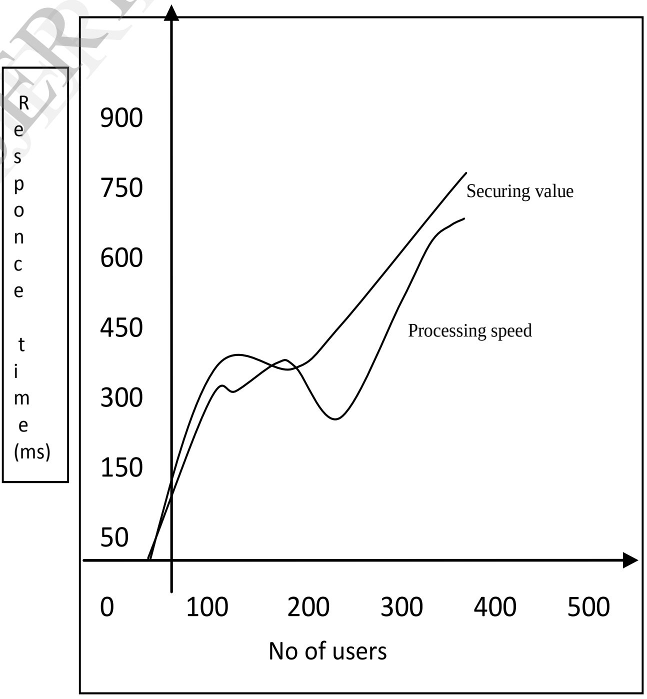
In our novel solution it may lead to the very effective performance compared with CTB & CP because it coupled with EDOS shield techniques. And it can provide the very effective security from the any type of service oriented or resource oriented attacks.

The main issue from the results was that the responsetime varied significantly from being able to detect the attack traffic within a matter of 9ms from 20-30ms. One hypothesis isthat the dataset was scattered far apart, and so the error ratiowithin the neural network kept fluctuating. Anotherhypothesis is that it could be the back propagation. Theseresults 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. 7.a: Training set results



CTP, CP WITH VF & VNODE in HTTP Requests
Fig. 7.b: Testing set results

5. CONCLUSION

The cloud computing model has the ability to scalecomputer resources on demand, and give users a number ofadvantages to progress their conventional cluster system. Infact the total cost of going towards cloud is almost zerowhen resources are not in use. Therefore it is no wonder thatacademic research and industry are moving towards cloudcomputing. However, Security should in fact beimplemented it along side functionality and performance.One of the most serious threats to cloud computing securityitself comes from Distributed Denial of Service attacks.These types of attacks are simple and easy to implement bythe attacker, but to security experts they are twice asdifficult to stop. So, a solution model is offered to TraceBack through proposed Cloud Trace Back (CTB) to find thesource of real attacks, and introduce the use of a backpropagation 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 resultwe achieved was around 88% and 91%, for testing andtraining datasets, respectively. The proposed model'sresults show that it is able to detect most of the attackmessages within a very short period of time. We also showthat CTB can successfully traceback 75-81% In the future,we will be setting up to begin real-time data gathering andtesting of Cloud Protector. This will allow us to fine tuneCTB 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 PerspectiveStudy," New Generation Computing Volume 28, Number 2, 137-146,
DOI: 10.1007/s00354-008-0081-5

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

[5]Iftikhar A., Azween B. A., Abdullah S.A.,(2009), "Application ofArtificial neural Network in Detection of DoS attacks," SIN'09, Oct6-10.

[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), "CloudSecurity defenses to protect cloud computing against HTTP-DoS andXML –DoS attacks," Journal of Network and Computer Applications, doi: 10.1016/j.jnca.2010.06.004.