Cloud QoS, High Availability & Service Security Issues with Solutions

Muhammad Zakarya & Ayaz Ali Khan
CS Department, COMSATS Institute of Information Technology, Islamabad, Pakistan

Abstract:
Cloud Computing is a most recent and hottest buzzword nowadays, emerges as a key service of the Utility or On demand computing [1] which builds on decade of research in the ground of computer networking, World Wide Web and software services. It put forwards a service oriented architecture, reduced information technology overhead for the end-user, enormous and huge flexibility and reduced total cost of ownership. Recent attacks on the clouds especially Distributed Denial of Service (DDoS) poses as a potential intimidation and danger to this key technology of the expectations and future. In this paper we are going to present a new Cloud Environment and Architecture and an Entropy based Anomaly Detection System (ADS) approach to mitigate the DDoS attack which further improves network performance in terms of computation time, Quality of Service (QoS) and High Availability (HA) under Cloud Computing environment. Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and IT Foundation are four basic types of Cloud Computing [39].

1. Introduction & Concepts:

Computing is being changed and altered to a new model consisting of services that are commoditized and delivered in a style similar to conventional utilities such as water, gas, electricity, and telephony service. In such a model, customers access services based on their requirements without gaze at to where the services are hosted or how they are delivered. *Cloud computing* denotes the infrastructure as a "Cloud" from which businesses and customers are competent and capable to access applications from anywhere in the world using on demand techniques. Depending on the category and kind of resources provided by the Cloud, different layers can be defined as Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as service (PaaS) and IT Foundation *[1, 39]*. All of these layers come with the promise to reduce first of all capital expenditures (CapEx) as well as operational expenditures (OpEx) in terms of reduced hardware, certificate & license and area management. In contrast, along with these benefits, Cloud Computing also raises rigorous and harsh concerns especially on the subject of the security of the cloud Computing Environment *[38]*.

Manuscript received July 5, 2012
Manuscript revised July 20, 2012

1.1 Ha in cloud Systems

Any system which is always available to its customers is HA. High availability of cloud system can be achieved, through implementing a lot of architectures. For example reduce congestion. It is difficult to achieve HA in today's global village because more services are required to customers. The more congested the network, more systems are offline to its customers. Considering TCP congestion scenario, where TCP drops all extra packets resulting in increased queuing delays. Therefore using traditional TCP congestion detection, avoidance mechanisms are not to achieve HA.

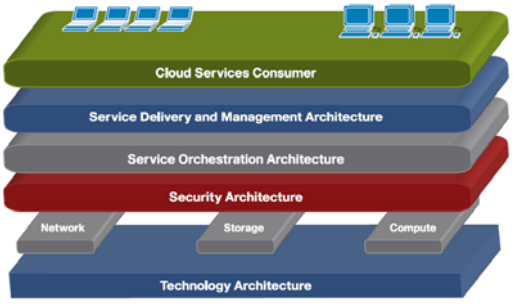

Fig 2.1 CISCO Cloud Architecture *[39]*

1.2 QoS in cloud environment

We are trying to study different service level security issues in Cloud computing especially in wireless Cloud, and will try to propose new solutions to their security improvements. As service level security issues like DoS Attacks & Network Congestion, are most important. Solving these issues results in High Availability as well as. In high available systems, QoS services are expected from service providers.

1.3 Security Issues

As networks are coming common to layperson in computer technology, the need to provide good services to its customers at any time is essential. Cloud computing provides its services to its customers on need basis, means whenever, what is required must be provided. Therefore

managing QoS and making the systems available, each and every time, to provide its services to Cloud users and customers, is a must. Although there is a obvious stipulate for in-depth conversation of security issues in Cloud Computing, the in progress surveys on Cloud security issues focus principally on data confidentiality, data protection and data privacy and discuss frequently organizational means to conquer these issues.

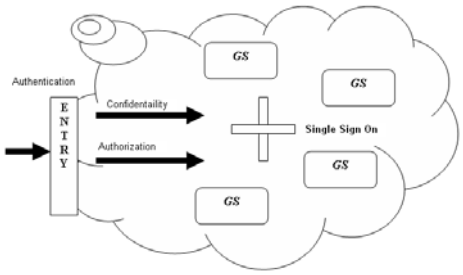

Fig 2.2 Security model for Cloud Computing environment

1.4 Distributed Dos Attack

DDoS attacks are launched by sending a large volume of packets to a target machine, using simultaneous cooperation of multiple hosts which are distributed throughout the Cloud computing environment. DDoS attacks on the Internet & especially on Cloud Computing has become an immediate problem in computer networks terminology. Gossip based DDoS attacks detection mechanism is used to detect such types of attacks in network, by exchanging traffic over line i.e. communication medium information. Mostly DDoS attacks are considered as congestion control problem. DDoS attacks are two phases attack. In first phase the attacker finds some vulnerable systems in the network. The attacker install some DDoS tools on these systems, also called zombies or agents. In second phase all zombies create the actual attack on the victim, as shown in figure 2.2 below *[2]*.

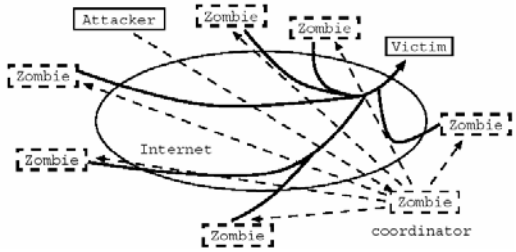

Fig 2.3 Attacker, Zombies and Victims *[2]*

1.5 IP Spoofing

Change of source address in the header of an IP packet is called IP Spoofing. It requires privileged access to network stack (raw socket access). A partial solution to IP Spoofing is to associate a fixed MAC address with each IP address in a subnet to detect spoofing.

2. Related Work & Existing techniques:

In this section we discuss some existing mechanisms and techniques.

2.1 Mutually Guarded Approach

In wireless communication medium, if a node-A (attacker) (masquerade itself as node-B), sends packets to node-C, where nodes A & B are in the same coverage area, then that packet will also be received by node-B. Therefore node-B will easily catch the attack. But if nodes B & C are in different coverage area, or both nodes B & C are out of range to each other, in that scenario the attacker will successfully launch its attack, as shown in Fig 3.1.

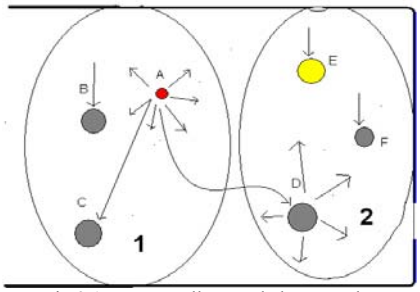

Fig 3.1 Mutually guarded approach

2.2 Ingress & Egress Filtering

Ingress & Egress filtering mechanism is shown diagrammatically in Fig 3.2 *[10]*.

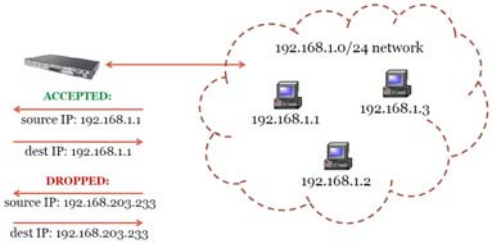

Fig 3.2 Ingress & egress filtering *[10]*

2.3 IP trace-back mechanism

In this technique the attacker is traced, by location. Actually without any mobility, it is some what easy, but when mobility is involved, the attacker cannot be traced easily.

2.4 Distributed Change point Detection (DCD)

In *[6]* the authors have proposed a new detection mechanism for DDoS. A CAT is constructed. Nodes in a CAT are ATRs that participate in forwarding the malicious flows. The links in the CAT indicate the path along which attacking traffic goes towards the victim. Once a CAT is constructed, a DDoS attack is detected and ATRs are identified. The next task is to filter out malicious flows.

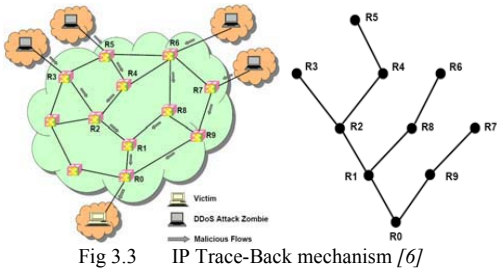

Fig 3.3 IP Trace-Back mechanism *[6]*

2.5 Moving Target Defense

A Band-Aid solution to a DDoS attack is to change the IP address of the victim computer, thereby invalidating the old address. The technique may work in some cases but administrators must make a series of changes to DNS entries, routing table entries etc.

2.6 Rate Limiting

Rate-limiting mechanisms compel a rate limit on a set of packets that have been characterized as nasty by the detection mechanism. It is a moderate response technique that is usually deployed when the detection mechanism has many false positives or cannot accurately illustrate the attack flow.

2.7 Mitigating DDoS Attacks via Attestation (Assayer)

In *[9]* the authors have proposed a new hardware based attestation mechanism to detect and prevent DDoS attacks. On a per-packet basis, they proposed to provide the network with the dominant ability to identify, the code on the end host that generated or permitted the packet. The story is shown in Fig 3.4 below.

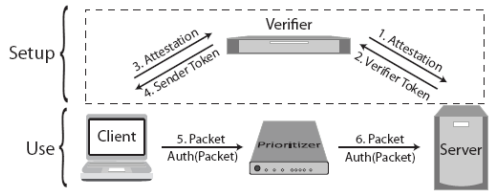

Fig 3.4 ASSAYER *[9]*

2.8 Traffic Shaping

A number of routers available in the bazaar today have features that permit you to limit the amount of bandwidth that some specific type of traffic can consume. This is occasionally referred to as "traffic shaping" technique *[10]*.

2.9 Internet Protocol Version 6 (IPv6)

IPv.4 does not have any check or methods to authenticate whether the IP address i.e. source address, that the sender puts into an IPv.4 packet header field, is justifiable or not, the DoS attacker can use any spoofed IP source address or Inactive IP source address exclusive of any concern of being caught. As a result, the authentication of source IP address is to be anticipated to enhance and improve an Internet Security against current DoS attacks as shown in Fig 3.5 *[10]*.

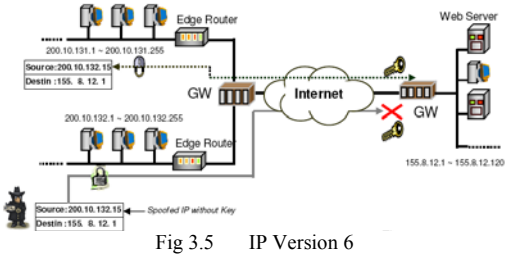

Fig 3.5 IP Version 6

2.10 Pushback: Router-Based Defense against DDoS Attacks

Pushback is a mechanism for defending against DDoS attacks. Each router has the ability to detect and preferentially drop packets that possibly belong to an attack. Upstream routers are also notified to drop such packets (therefore named as Pushback), in order that the router's resources are used to route legitimate traffic only *[28], [29]*.

3. Existing Problem:

We are going to propose a DDoS detection and prevention mechanism, that has the beauty of being easy to adapt and more reliable than existing counterparts. As, in service level security issues DoS Attacks, DDoS & Network Congestion, are most important. Solving the issue of DDoS also results in High Availability as well as good QoS.

4. Proposed Solution:

After a deep study of available techniques, we are going to introduce a new IDS, which can be implemented on our own proposed architecture, resulting in DDoS detection and prevention mechanism.

4.1 Proposed Architecture

In our proposed architecture, we have divided the whole Cloud System into regional areas i.e. GS, where each GS is protected by an AS / GL. Our developed ADS is installed on two places i.e. every Cloud Node & AS or on their respective routers. A packet which is detected as cruel once at AS, is marked out, so that Client node can be informed. In our proposed architecture (for future direction), DDoS source is detected for future prevention. A tree is maintained at every router, by marking every packet with path modification strategy, so that the victim is able to trace the sender of the packet. Any packet which was detected as malicious flow, can be confirmed in a second try i.e. confirmation process at GN i.e. victim node. In phase 1 we detect malicious flow, while in phase 2 we have a confirmation algorithm so either to drop the attack flow, or to pass it otherwise. In the given scenario, we consider that AS is configured properly for policed address i.e. the attacker node address or victim IP address.

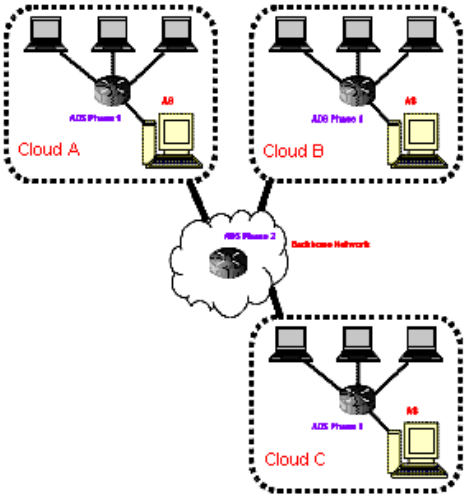

Fig 5.1 Proposed Cloud Architecture

- Authentication Server (AS) or Geographical Authentication & Authorization Server (GAS) is responsible for controlling the geographical area where defined.
- Locally phase 1 is executed & at the core router phase 2 takes place.

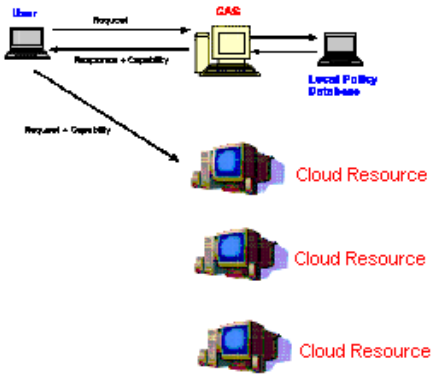

Fig 5.2 Working diagram of Proposed Cloud Architecture

PROS & CONS

- Local Security Policy
- Little computation as compared to Global security policy
- Near the source detection
- No overhead of extra packet
- User accesses GAS, authenticated & authorization check
- Performance Scalability + load balancing + QoS
- No need for resources to check the user identity
- Local & Quick allocation of resources by GAS
- No Single point of failure, affect some part of the Cloud
- GAS are required to inform all corresponding GAS in case of new node to any geographical community
- GAS is attacked by DDoS, not possible

4.2 Intrusion Detection System

IDS may be in software form and/or in hardware form, that will monitor the network for disbelieving activity and alerts the network administrator to take a particular action accordingly. Signature based IDS will observe packets on the network and judge against them to a database maintained with well-known threats. On the other hand, using an ADS, if deviation of user activity is exterior a certain threshold value, it is marked as nasty and a reaction is triggered. After a deep survey of DDoS detection & prevention mechanism we reach to the point that Entropy may be used as DDoS detection metric.

4.3 Information Theory & Entropy Based Ads

According to *[14]*, any statements that have some surprise and meaning are called information. Some consider that information theory is to be a subset of communication theory, but we consider it much more. The word entropy is rented from physics, in which entropy is a measure of the chaos of a group of particles i.e. 2nd law of thermodynamics. If there are a number of possible

messages, then each one can be expected to occur after certain fraction of time. This fraction is called the probability of the message. In *[23], [24]* Shannon proved that information content of a message is inversely related to its probability of occurrence. To summarize, the more unlikely a message is, the more information it contains. *In [15],* Entropy H(X) is given by

$$H(X) = -\sum_{x \in \mathcal{X}}^{n} p(x) \log p(x)$$

The log is to the base 2 and entropy is expressed in bits. To say randomness is directly proportional to entropy i.e. more random they are, more entropy is there. The value of sample entropy lies between 0 and log(n). The entropy value is smaller when the class distribution belongs to only one & same class while entropy value is larger when the class distribution is more even. Therefore, comparing entropy values of some traffic feature to that of another traffic feature provides a mechanism for detecting changes in the randomness. We use traffic distribution like IP Address & application Port Number i.e. (IP address, Port). If we wants to calculate entropy of packets at a single or unique source i.e. destination, then maximum value of n must be 2^{32} for IPV4 address. Similarly if we want to gauge entropy at multiple application ports then value of n is the total number of ports *[16]*. In similar way, p(x) where x ϵ X, is the probability that X takes the value x. We randomly examine X for a fix time window (w), then $p(x) = m_i/m$ Where, m_i is the total number we examine that X takes value x i.e

$$m = \sum_{i=1}^{n} mi$$

Putting these values in entropy equation 1, we get

$$H(X) = -\sum_{i=1}^{n} (m_i/m) \log (m_i/m)$$

Similarly, if we want to calculate the probability p(x), then m is the entire number of packets, but m_i is the number of packets with value x at destination as source *[37]*. Mathematically given as

$$P(x) = \frac{\text{Number of packets with x as source (destination) port}}{\text{Total number of packets}}$$

Again if we want to calculate probability p(x) for each destination port, then

$$P(x) = \frac{\text{Number of packets with } x_i \text{ as source (destination) address}}{\text{Total number of packets}}$$

Remember that total number of packets is the number of packets observed in a specific time slot (w). When this calculation finishes, normalized entropy is calculated to get the overall probability of the captured flow in a specific time window (w). Normalized Entropy is given by

$$\text{Normalized entropy} = (H / \log n_0)$$

Where n_o is the number of dissimilar values of x, in a specific time slot (w). During the attack, the attack flow dominates the whole traffic, resulting in decreased normalized entropy. To confirm our attack detection, again we have to calculate the entropy rate i.e. growth of entropy values for random variables, provided that the limit exists, and is given by

$$H(\chi) = \lim_{n \to \infty} \frac{1}{n} H(x_1, x_2 \ldots x_n)$$

If a discrete source sends one packet each after a specific amount of time, then we can find its information rate as given by $\mathbf{R} = r_s$ **H(X)**
Where R stands for information rate, r_s is the specific amount of time and **H(X)** is the entropy of that source. For example suppose node A sends five packet each after one milliseconds with probability of ½, ¼, 1/8, 1/16 and 1/16 respectively, then its

H(X) = 1.875 bits/symbol &
R = 1000 * 1.875 bits/second

5. Proposed Algorithms:

FOR DETECTION OF DDOS ATTACK

- *Decide a threshold value δ_1*
- *On edge routers collect traffic flows for a specific time window (w)*
- *Find probability P(X) for each node packets*
- *Calculate link entropy of all active nodes separately*
- *Calculate H(X) for routers using Equation (1)*
- *Find normalized entropy using Equation (3)*
  If normalized entropy < δ_1, identify malicious attack flow

FOR CONFIRMATION OF ATTACK FLOWS

- *Decide a threshold value δ_2*
- *Calculate entropy rate on edge router using Equation (4)*
- *Compare entropy rates on that router, if =< δ_2, DDoS confirmed*

COMPUTATIONAL COMPLEXITY

The running time of this algorithm can be expressed as a(n) + b for constants values a & b that are dependant on other statements cost. Therefore it is a linear function of n and is given asymptotically by **O(n)**. So best case running time is **O(n)**, while worst case running time is $\mathbf{\Theta(n^2)}$.

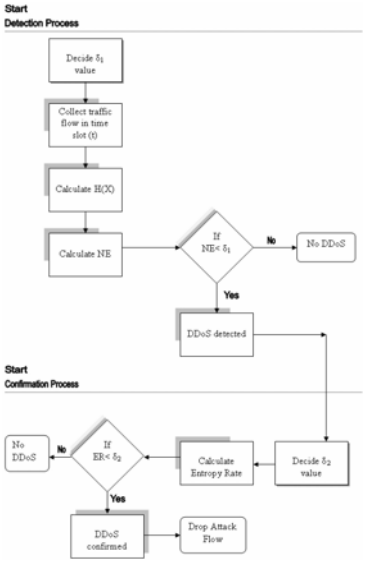

Fig 6.1 Flow / Transition Diagram

6. Implementation, Simulation & Results:

In this chapter we are going to discuss that how our proposed ADS will be implemented in Cloud environment, and also how routers communicate with each other to detect DDoS attack. In this section we describe that how to mathematically or statically implement our proposed scheme, while in section coming after that we have shown our simulation results along with charts form with a practical environment.

6.1 Mathematical Proof

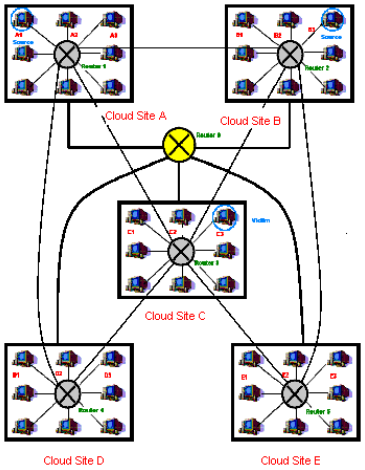

Fig 7.1 Environment for statistical study

Consider Fig 6.1, A1 and B3 are attack sources at different Cloud Sites, while C3 is the target victim machine. Router 1 will capture traffic flow coming from A1 and Router 2 will capture attack flow thrown by B3, for a specified time window (w). Suppose that we capture the following traffic flow at Router 1 and Router 2, shown in table 7.1 and table 7.2, 7.3 and 7.4 respectively.

TABLE 7.1: TRAFFIC AT ROUTER 1

Source node	*Destination node*	*No of packets*	*Entropy*
A1	C3	7	0.50
A2	B1	2	0.40
A3	B3	3	0.47
A4	E1	2	0.40

Therefore Router Entropy for Router 1 is 0.50 + 0.40 + 0.47 + 0.40 = 1.77 & as $\log_2 4 = \log 4/\log 2 = 2$
Hence Normalized Entropy is 1.77/ $\log_2 4 = 0.88$

TABLE 7.2: TRAFFIC AT ROUTER 2

Source node	*Destination node*	*No of packets*	*Entropy*
B1	D1	2	0.44
B2	A3	1	0.31
B3	C3	6	0.47
B4	E2	2	0.44

Therefore Router Entropy for Router 2 is 0.44 + 0.31 + 0.47 + 0.44 = 1.66 & as $\log_2 4 = \log 4/\log 2 = 2$
Hence Normalized Entropy is 1.66/ $\log_2 4 = 0.83$

TABLE 7.3: TRAFFIC AT ROUTER 4

Source node	*Destination node*	*No of packets*	*Entropy*
D1	A1	2	0.46
D2	A3	2	0.46
D3	E3	3	0.52
D4	C2	3	0.52

Therefore Router Entropy for Router 1 is 0.46 + 0.46 + 0.52 + 0.52 = 1.96 & as $\log_2 4 = \log 4/\log 2 = 2$
Hence Normalized Entropy is 1.96/ $\log_2 4 = 0.98$

TABLE 7.4: TRAFFIC AT ROUTER 5

Source node	*Destination node*	*No of packets*	*Entropy*
D1	C3	2	0.52
D2	C1	1	0.43
D3	D1	2	0.52
D4	A4	1	0.43

Therefore Router Entropy for Router 2 is 0.52 + 0.43 + 0.52 + 0.43 = 1.90 & as $\log_2 4 = \log 4/\log 2 = 2$
Hence Normalized Entropy is 1.90/ $\log_2 4 = 0.95$
We can see that as at both routers i.e. Router 1 and Router 2, routers entropy is lesser as only one flow conquered the whole bandwidth. As an outcome normalized entropy decreases. If we have a perfect threshold value δ, suppose

0.94 then our proposed ADS will consider flows coming from A1 (GS A) and B3 (GS B) as malicious flows, while Cloud Site D & Cloud Site E have entropy value greater than our considered threshold value 0.94, no attack is detected at these sites. Entropy rates are calculated for A1 at Router 1 and Router 0 and are compared. If entropy rates are same or near to similarity, malicious flow is dropped. The process is show in state transition diagram given in Fig 7.2.

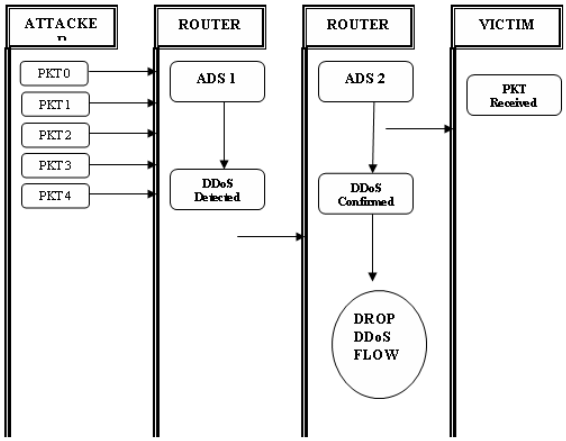

Fig 7.2 Transition Diagram

6.2 Simulations study

6.2.1 Simulation Environment

CloudSim was used as a simulation environment, for testing the results of our proposed Idea. To simulate our proposed idea we have 3 users with 2 posers of DDoS attack, 2 routers and 3 resources containing any single victim node on the same time. The environment is shown in Fig 7.3

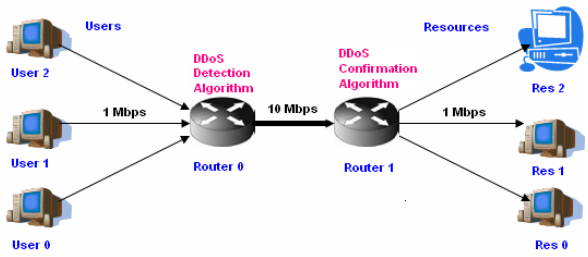

Fig 7.3 Environment for simulation study

For simplicity we take equal size bandwidth media. Both routers are connected to each other over a 10 Mbps link, while all other connections are made at 1 Mbps link. DDoS detection algorithm is implemented on router 0, while DDoS confirmation algorithm is supposed to be implemented on router 1.

6.2.2. Simulation Results

In this section we consider only DDoS detection algorithm on router 0, not to confirm attack.

CASE 1:

TABLE 7.5: TRAFFIC AT ROUTER FOR USER_0

Destination node	Total No of packets	Probability	Entropy
Res_0	5	0.5	0.5
Res_1	2	0.2	0.46
Res_2	3	0.3	0.52

Therefore Router Entropy for Router 2 is 0.5 + 0.46 + 0.52 = 1.48 & as $\log_2 3 = \log 3/\log 2 = 1.58$

Hence Normalized Entropy is 1.48/ $\log_2 3$ = 0.93 **(DDoS Detected)**

TABLE 7.6: TRAFFIC AT ROUTER FOR USER_1

Source node	*Total No of packets*	*Probability*	*Entropy*
Res_0	4	0.4	0.52
Res_1	3	0.3	0.52
Res_2	3	0.3	0.52

Therefore Router Entropy for Router 2 is 0.52 + 0.52 + 0.52 = 1.57 & as $\log_2 3 = \log 3/\log 2 = 1.58$

Hence Normalized Entropy is 1.57/ $\log_2 3$ = 0.99 **(DDoS Not Detected)**

TABLE 7.7: TRAFFIC AT ROUTER FOR USER_2

Source node	*Total No of packets*	*Probability*	*Entropy*
Res_0	0	0.0	0.0
Res_1	3	0.3	0.52
Res_2	7	0.7	0.36

Therefore Router Entropy for Router 2 is 0.0 + 0.52 + 0.36 = 0.88 & as $\log_2 2 = \log 2/\log 2 = 1$

Hence Normalized Entropy is 0.88/ $\log_2 2$ = 0.88 **(DDoS Detected)**

7. Performance Evaluation:

After a deep study of the proposed scheme we concluded that our ADS can detect 100% DDoS only in case of good threshold value. A value of 0.94 results in good detection rate. A value greater than 0.94, results in good detection rate but generate more false positive alarms. The reports are shown in graphs below.

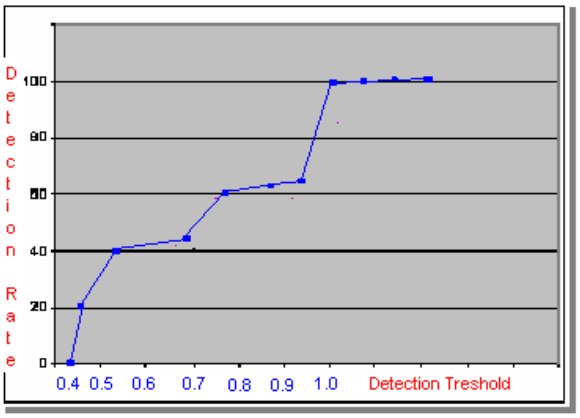

Fig 8.1 DDoS detection rate

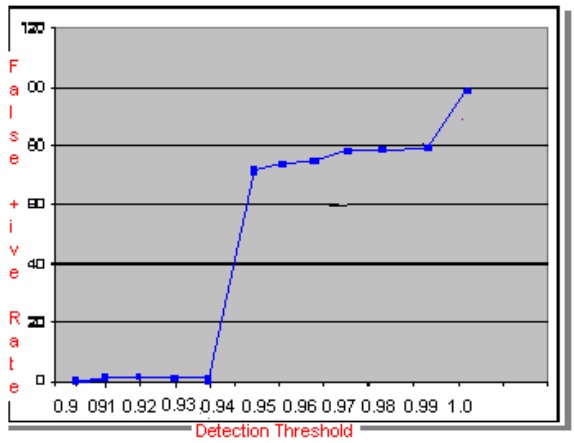

Fig 8.2 DDoS false positive rate

8. Conclusion & Future Work:

In this paper, we have proposed a new architecture for Cloud Computing platform, where the whole Cloud System is divided into multiple administrative domain, which is controlled separately by its own Authentication & Certification Authority i.e. AS. We have also developed ADS for detection & early prevention of DDoS attacks in our proposed architecture. In future the proposed idea may be actually implemented over Cloud environment to accurately detect DDoS attacks. The idea may also be extended for recovery mechanism for DDoS attacks. Following are some challenges which might be addressed for further enhancement by researchers and scholars.

- *Setting perfect threshold values δ_1, δ_2, some time it must be dynamic in nature to detect DDoS with high accuracy*
- *Usually in DDoS same function is used for posing the attack, but what about different functions when used for creating attack packets*
- *Huge network access results in malicious flow detection, so in such a scenario separating legitimate flows from attack flows is a challenging task*

References:

[1] "Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia", "Above the Clouds: A Berkeley View of Cloud Computing", Technical Report No. UCB/EECS-2009-28

[2] "Kashan Samad, Ejaz Ahmed, Riaz A. Shaikh, Ahmad Ali Iqbal", "ANALYSIS OF DDOS ATTACKS AND DEFENSE MECHANISMS", 2005

[3] "Hang Chau", Network Security – Mydoom, Doomjuice, Win32/Doomjuice Worms and DoS/DDoS Attacks", USA

[4] "Puneet Zaroo", "A Survey of DDoS attacks and some DDoS defence mechanisms", Advanced Information Assurance (CS 626).

[5] "Stephen M. Specht, Ruby B. Lee", "Distributed Denial of Service : Taxonomies of Attacks, Tools and Countermeasures", September 2004

[6] "Yu Chen, Kai Hwang, Wei-Shinn Ku", Distributed Change point Detection of DDoS Attacks: Experimental Results on DETER Testbed", 2007

[7] "Preeti, Yogesh Chaba, Yudhvir Singh", "Review of Detection and Prevention Policies for Distributed Denial of Service Attack in MANET", March 2008

[8] "S.Meenakshi, Dr.S.K.Srivatsa", "A Comprehensive Mechanism to reduce the detection time of SYN Flooding Attack", 2009

[9] "Bryan Parno, Zongwei Zhou, Adrian Perrig", "Don't Talk to Zombies: Mitigating DDoS Attacks via Attestation", June 2009

[10] "Konstantinos Meintanis, Brian Bedingfield, Hyoseon Kim", "The Detection & Defense of DDoS Attack", University of Texas

[11] "A. Lakhina, M. Crovella, and C. Diot.", "Diagnosing Network-Wide Traffic Anomalies", ACM SIGCOMM Computer Communication Review, Portland, 2004

[12] "L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred", "Statistical approaches to DDoS attack detection and response", 2003

[13] "W. Lee, D. Xiang", "Information-theoretic measures for anomaly Detection", IEEE, 2001

[14] "DAVID APPLEBAUM", "PROBABILITY AND INFORMATION (An Integrated Approach)", CAMBRIDGE UNIVERSITY PRESS, 2008

[15] "THOMAS M. COVER, JOY A. THOMAS", "ELEMENTS OF INFORMATION THEORY", Second Edition, 2006

[16] "Dennis Arturo Ludeña Romaña, Yasuo Musashi", "Entropy Based Analysis of DNS Query Traffic in the Campus Network", Japan

[17] "Rajkumar Buyya, Manzur Murshed", "GridSim: a toolkit for the modeling and simulation of distributed resource management and scheduling for Grid computing", 2002

[18] "Anthony Sulistio, Gokul Poduval, Rajkumar Buyya, Chen-Kong Tham", "Constructing A Grid Simulation with Differentiated Network Service using GridSim", University of Melbourne, Australia

[19] "Manzur Murshed, Rajkumar Buyya", "Using the GridSim Toolkit for Enabling Grid Computing Education", Monash University, Australia

[20] "Anthony Sulistio, Uros Cibej, Srikumar Venugopal, Borut Robic, Rajkumar Buyya", "A toolkit for modelling and

simulating data Grids: an extension to GridSim", March 2008
[21] "Anthony Sulistio, Chee Shin Yeo, Rajkumar Buyya", "Visual Modeler for Grid Modeling and Simulation (GridSim) Toolkit", 2003
[22] "Microsoft Encarta Encyclopedia", 2009
[23] "Claude E. Shannon", "A Mathematical Theory of Communication", 1948
[24] "Claude E. Shannon", "Communication Theory of Secrecy Systems", 1949
[25] "Yi-Chi Wu, Wuu Yang, Rong-Horg Jan", "DDoS Detection and Trace-back with Decision Tree and Gray Relational Analysis", National Chiao Tung University, Taiwan.
[26] "Ian. Foster, C. Kesselman", "The Grid: Blueprint for a new computing infrastructure", Morgan Kaufmann publishers, 1999.
[27] "Kumar, S. and E.H. Spafford", "A Pattern Matching Model For Misuse Intrusion Detection", 1994
[28] "JU WANG", "Tolerating Denial-of-Service Attacks – A System Approach", 2005
[29] "Dawei Yao", "Adaptive Firewalls for Grid Computing", 2005
[30] http://www.gridbus.org/gridsim/
[31] http://www.buyya.com/gridsim/
[32] "B. B. Gupta, Manoj Misra and R. C. Joshi", "An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach", 2008
[33] "J. Mirkovic, P. Reiher", "A Taxonomy of DDoS Attack and DDoS defense Mechanisms", April 2004
[34] "Mobin Javed, Ayesha Binte Ashfaq, M. Zubair Shafiq, Syed Ali Khayam", "On the Inefficient Use of Entropy for Anomaly Detection", NUST & FAST, Pakistan.
[35] "Thomas M. Cover, Joy A. Thomas", "ELEMENTS OF INFORMATION THEORY", Chapter 4, 1991
[36] "Tao Peng", "Defending Against Distributed Denial of Service Attacks", April 2004
[37] "George Nychis", "An Empirical Evaluation of Entropy-based Anomaly Detection", May 2007
[38] "Palvinder Singh Mann, Dinesh Kumar", "An Analytical Approach to Mitigate DDoS Attacks and improve Network Performance under Collaborative Software as a Service (SaaS) Cloud Computing Environment", DAV Institute of Engineering & Technology Jalandhar, Punjab, India
[39] "Point of View White Paper for U.S. Public Sector", "Cisco Cloud Computing Data Center Strategy, Architecture, and Solutions", 1st Edition
[40] CloudSim documentation for programming and simulations

The author of this paper is a new researcher to the field of new emerging computing technologies like Grid, Cloud and Green Computing. He has done MS in Computer Science and is interested for a doctorate degree in computer engineering.