Cloud QoS, High Availability & Service Security Issues with Solutions

Muhammad Zakarya, Izaz ur Rahman *and* Mukhtaj Khan

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 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 ADS approach to mitigate the DDoS attack which further improves network performance in terms of computation time, QoS and HA under Cloud computing environment SaaS, PaaS, IaaS and IT Foundation are four basic types of Cloud Computing [30, 31, 32].

Index Terms: Anomaly Detection System, Distributed, Denial of Service, High Availability, Quality of Service, Software as a Service, Platform as a Service, Infrastructure as a Service, Intrusion Detection System, Authentication Serve, Group Leader, Geographic Node, Internet Protocol, Geographical Authentication & Authorization Server,Load Balancing, Cloud Site

I. 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. CISCO Cloud architecture is shown in Fig 1. Depending on the category and kind of resources provided by the Cloud, different layers can be defined as IaaS, SaaS, PaaS and IT Foundation [1, 30]. 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 [30, 31].

Department of Computer Science, Abdul Wali Khan University (AWKU), Mardan, Khyber Pakhtun Khwa (***KPK***), Pakistan
mohd.zakarya@awkum.edu.pk
izaz@awkum.edu.pk
mukhtaj.khan@awkum.edu.pk

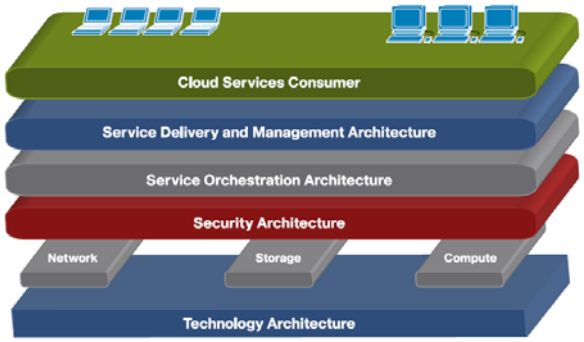

Fig.1. CISCO Cloud Architecture *[31]*

A. High Availability 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.

B. QoS in Cloud computing 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.

C. Security Issues & Problems

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 shows security model for distributed environment.

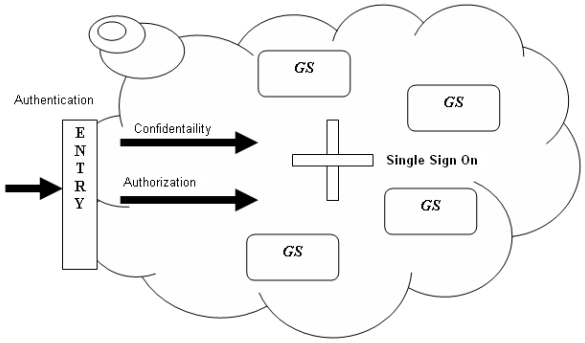

Fig. 2. Security model for Cloud Computing environment *[32]*

D. *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 3 below [2].

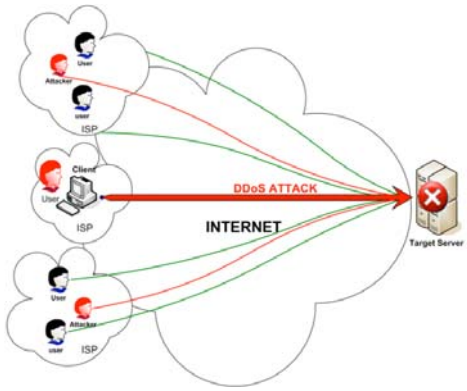

Fig .3. Attacker, Zombies and Victims *[29]*

E. *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.

The rest of paper is organized as follows. In section I we give some introduction, II is about related work. Section III, IV and V is about existing problem and proposed solution. IV describes statistical and simulation results. VII is about performance evaluation. We conclude in section VIII with challenges and future directions.

II. RELATED WORK & EXISTING TECHNIQUES:

In this section we discuss some existing mechanisms and techniques.

A. *Ingress & Egress Filtering*

Ingress & Egress filtering mechanism is shown diagrammatically in Fig 4 [10]. The firewall can easily drop that packet that is addressed for a node which is not present in its network. Similarly it has a check on those packets leaving the network. If source address is altered the firewall will drop the attack flow.

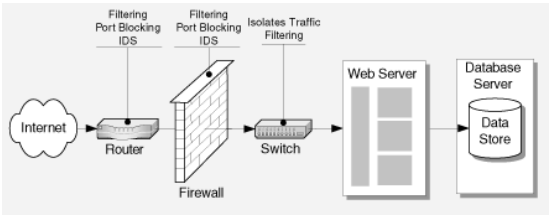

Fig.4. Ingress & egress filtering *[10]*

B. *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.

C. Moving Target Defense technique

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.

D. Rate Limiting mechanism

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.

E. 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].

F. 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. 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 5 [10].

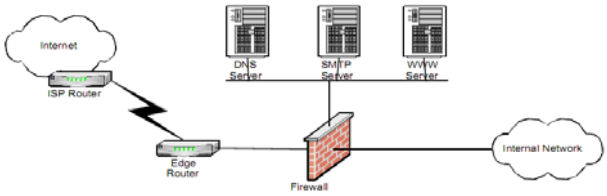

Fig.5. IP Version 6

G. 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 6.

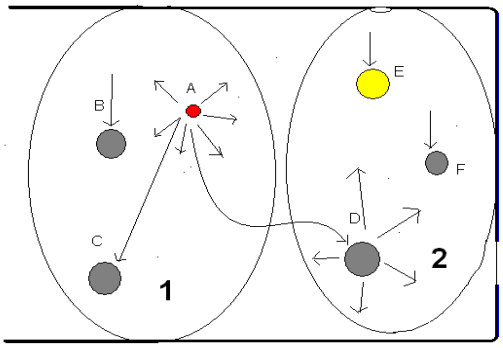

Fig.6. Mutually guarded approach *[32]*

III. 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.

IV. PROPOSED SOLUTION:

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

A. 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.

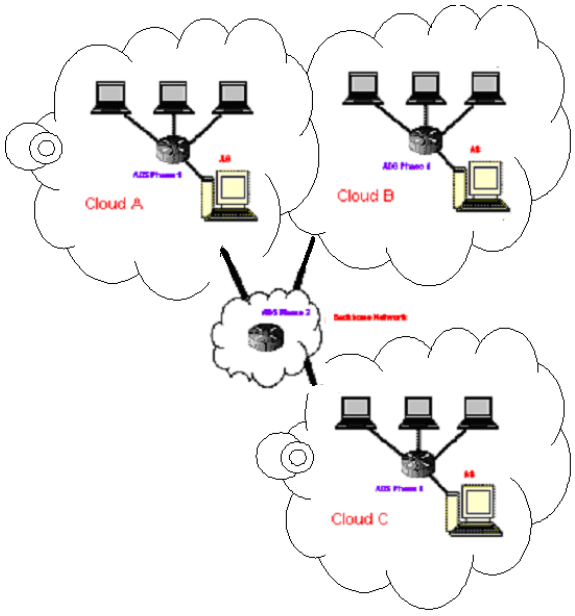

Fig.7. Proposed Cloud Architecture

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

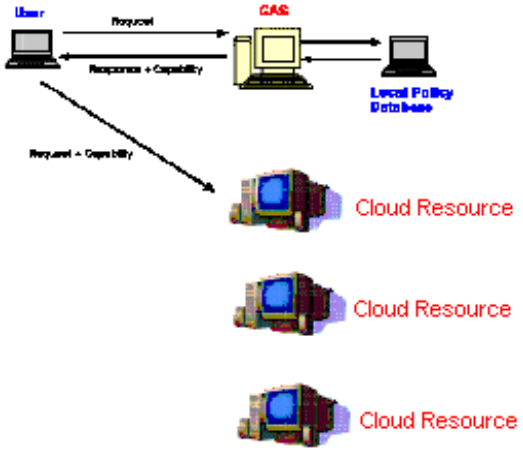

Fig.8. Working diagram of Proposed Cloud Architecture

PROS & CONS

- Local Security Policy
- Little computation involved as compared to Global security policy
- No overhead of extra packet
- User accesses GAS, hence fully authenticated & authorization check & balance
- Performance Scalability + LB + QoS
- No need for resources to check the user identity
- Local & Quick allocation of resources by GAS
- No Single point of failure, affects only a or some part of the Cloud environment
- GAS are required to inform all corresponding GAS in case of new node to any geographical society
- GAS is attacked by DDoS, not possible here
- Near to the source detection facility

B. 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 [32].

C. 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

$$H(X) = -\sum_{x \in \mathcal{X}}^{n} p(x) \log p(x) \qquad (1)$$

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

$$m = \sum_{i=1}^{n} mi \quad (2)$$

Putting these values in entropy equation 1, we get

$$H(X) = -\sum_{i=1}^{n} (m_i/m) \log (m_i/m) \quad (3)$$

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 [26]. Mathematically given as

$$P(x) = \frac{\text{Number of packets with } x_i \text{ as source (destination) address}}{\text{Total number of packets}} \quad (4)$$

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

$$P(x) = \frac{\text{Number of packets with x as source (destination) port}}{\text{Total number of packets}} \quad (5)$$

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

$$\text{Normalized entropy} = (H / \log n_0) \quad (6)$$

Where n_0 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

$$H(\chi) = \lim_{n \to \infty} \frac{1}{n} H(x_1, x_2 \ldots x_n) \quad (7)$$

V. PROPOSED ALGORITHMS:

DETECTION

- *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 (6)*
- *If normalized entropy < δ_1, identify malicious attack flow*

CONFIRMATION

- *Decide a threshold value δ_2*
- *Calculate entropy rate on edge router using Equation (7)*
- *Compare entropy rates on that router, if =< δ_2, DDoS confirmed*
- *Drop the attack flow*

In this paper we have not considered confirmation algorithm for our mathematical & simulations study, as that is our next target. In Fig 9, the flow diagram for our proposed scheme is given.

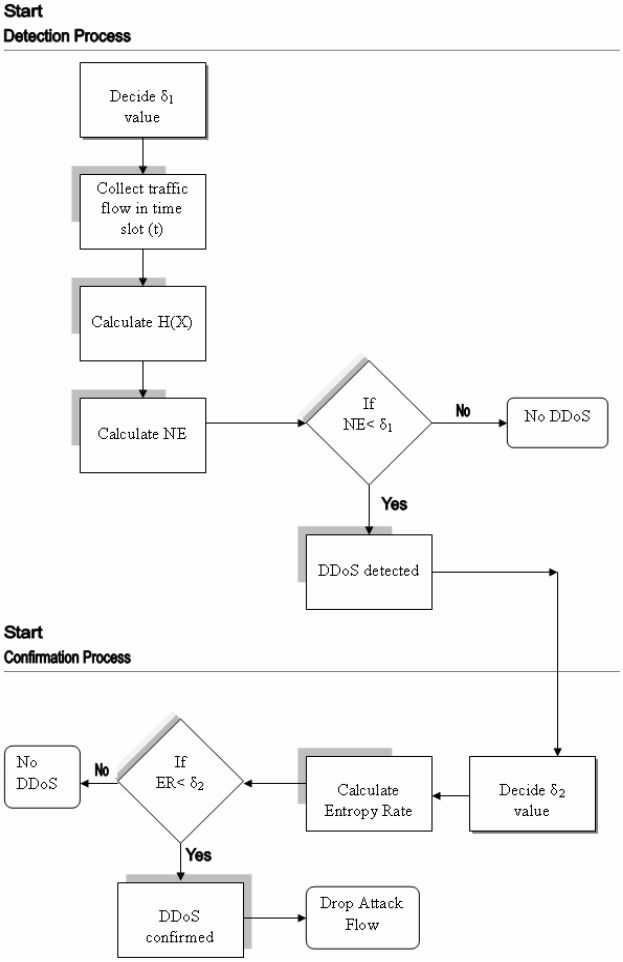

Fig 9 Flow / Transition Diagram *[32]*

VI. IMPLEMENTATION, SIMULATION & RESULTS:

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. We have used a Cloud Simulator i.e. CloudSim for testing our solutions. We run our proposed algorithms several time on the same system, on the basis of which we derived performance evaluation results. Here in this article we have shown only case 1.

A. Mathematical Proof

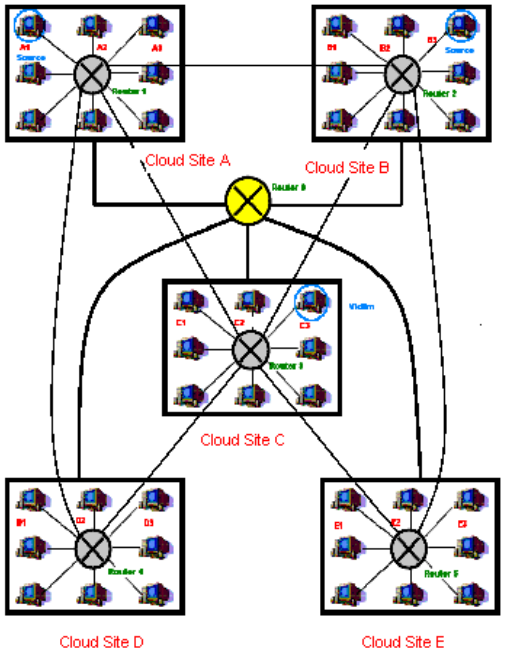

Fig.10. Environment for statistical study

Consider Fig 9, 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 1 and table 2, table 3 and table 4 respectively.

TABLE 1: TRAFFIC AT ROUTER 1

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

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

TABLE 2: TRAFFIC AT ROUTER 2

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

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

TABLE 3: TRAFFIC AT ROUTER 4

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

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

TABLE 4: TRAFFIC AT ROUTER 5

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

Therefore Router Entropy for Router 2 is 0.43 + 0.43 + 0.52 + 0.52 = 1.90 & as $\log_2 4 = \log 4/\log 2 = 2$ Hence NE 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 NE decreases. If we have a perfect threshold value δ, suppose 0.94 then our proposed ADS will consider flows coming from A1 (CS A) and B3 (CS 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.

B. Simulations Study

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 5 users with 2 posers of DDoS attack, 3 routers and 3 resources containing any single victim node on the same time, as shown in Fig 11.

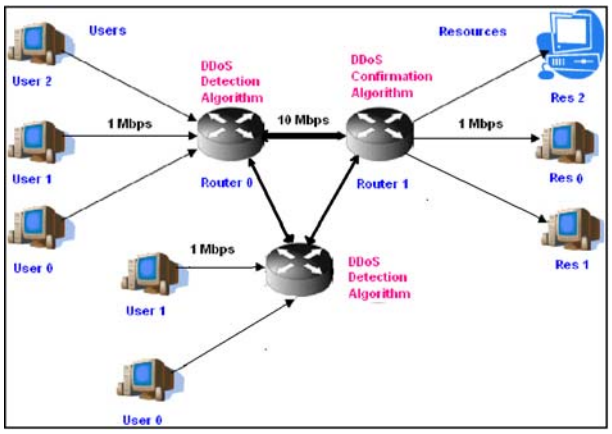

Fig.11. Environment for simulation study

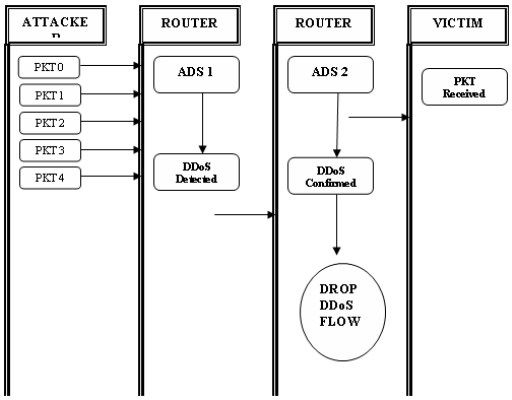

Fig.12. Transition Diagram [32]

Both routers are connected to each other over a 10 Mbps link, while all other connections are made at 1 Mbps link. Detection algorithm is implemented on router 0, while confirmation is supposed to be implemented on router 1. The process is show in state transition diagram given in Fig 12.

2) Simulation Results

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

CASE 1:

TABLE 5: TRAFFIC AT ROUTER FOR USER_0

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

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

Hence Normalized Entropy is $1.48/ \log_2 3 = 0.93$

TABLE 6: TRAFFIC AT ROUTER FOR USER_1

Source node	Total No of packets	Probability	Entropy
Res_0	3	0.3	0.52
Res_1	4	0.4	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 $1.57/ \log_2 3 = 0.99$

TABLE 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 $0.88/ \log_2 2 = 0.88$

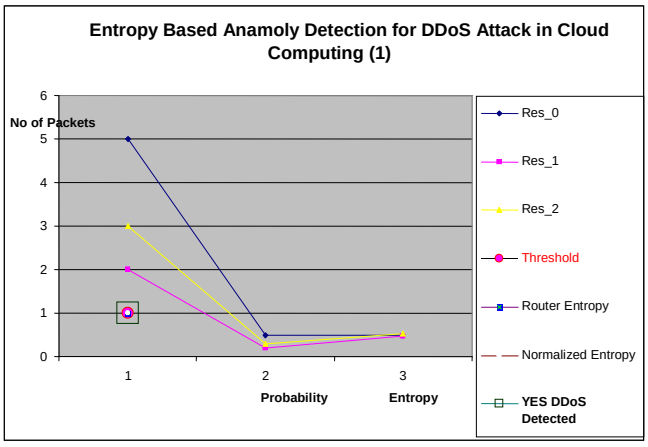

Fig.13. Simulation results (Case 1)

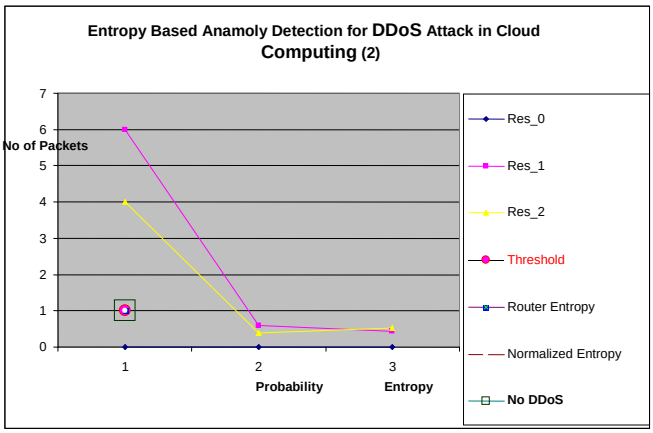

Fig.14. Simulation results (Case 2)

VII. PERFORMANCE EVALUATION:

Our ADS can detect 100% DDoS attack only in case of good threshold value, which is one of the most challenging tasks in developing any ADS. We conclude our story that a threshold value of 0.94 results in good detection rate. A value greater than 0.94, results in good detection rate i.e. 100 % DDoS detection but generate more false positive alarms, as the value is increased from 0.94 to 1.0. The reports are shown in figure 14 and figure 15, are self explanatory.

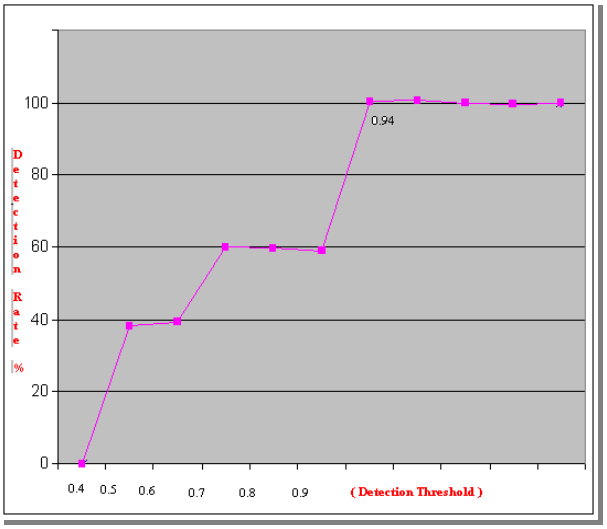

Fig. 15. DDoS detection rate

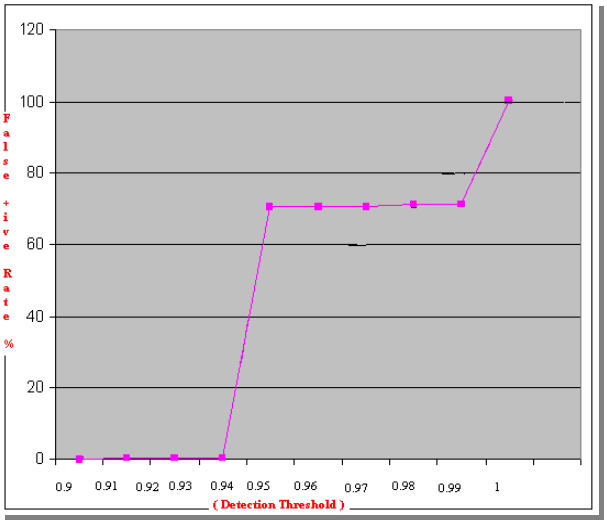

Fig.16. DDoS false positive rate

VIII. CONCLUSION

In this paper, we have proposed a new architecture for Cloud On-Demand Computing platform, where the whole Cloud System is divided into numerous administrative domains, which are controlled independently by its own Authentication & Certification Authority i.e. AS. We also introduced an ADS for detection & early prevention of DDoS attacks in our proposed architecture. In future the proposed design and suggestion may be actually implemented over Cloud computing platform to precisely detect DDoS attacks. The idea may also be extended for recovery mechanism for DDoS attacks. Following are some major challenges which might be addressed for further enhancement by researchers and scholars.

- *In case of huge network access separating legitimate flows from attack flows is a challenging task; our next task is to confirm the dropping of only attack packet.*
- *what about different mathematical functions when used for creating attack packets*
- *In case of Huge network access separating legitimate flows from attack flows is a challenging task*

ACKNOWLEDGMENT

This work is fully supported by Abdul Wali Khan University, Mardan, Khyber Pakhtun Khwa (KPK), Pakistan. The author(s) of this article are greatly thankful to Dr. Nasro Min Allah from COMSATS Institute of Information Technology (CIIT), Islamabad for full guidance and major support. The author(s) are also thankful to Mr. Aftab Alam from Computer Science Department, Abdul Wali Khan University, Mardan, for their contribution and cooperation.

REFERENCES

[1] B. Jacob, Michael Brown, Kentaro Fukui, Nihar Trivedi, "Introduction to Grid Computing", 2005

[2] K. Samad, Ejaz Ahmed, Riaz A. Shaikh, Ahmad Ali Iqbal, "Analysis of DDoS attacks & defence 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] S. 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] K. 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] M. Thomas 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] R. 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] M. 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] E. Claude Shannon, "A Mathematical Theory of Communication", 1948

[24] E. Claude 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] George Nychis, "An Empirical Evaluation of Entropy-based Anomaly Detection", May 2007

[27] Point of View White Paper for U.S. Public Sector, "Cisco Cloud Computing Data Center Strategy, Architecture, and Solutions", 1st Edition

[28] CloudSim documentation for programming and simulations

[29] D. Angelos Keromytis, "Denial of Service Attacks and Resilient Overlay Networks", Columbia University

[30] R. Buyya, CheeShinYeo, SrikumarVenugopal, JamesBroberg, IvonaBrandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", 2008 Elsevier B.V. All rights reserved

[31] R. Buyya, Suraj Pandey and Christian Vecchiola, "Cloudbus Toolkit for Market-Oriented Cloud Computing", M.G. Jaatun, G. Zhao, and C. Rong (Eds.): CloudCom 2009, LNCS 5931, pp. 24–44, 2009. © Springer-Verlag Berlin Heidelberg 2009

[32] Muhammad Zakarya, Ayaz Ali Khan, Hameed Hussain, "Grid High Availability & Service Security Issues with Solutions", ICIIT 2010, 978-1-4244-813 8-5/10 / $ 26.00 C 2010 IEEE