MAS BASED FRAMEWORK TO PROTECT CLOUD COMPUTING AGAINST DDOS ATTACK

Rohit Srivastava[1], Rohit Sharma[2], Avinash Verma[3]

[1]*Research Scholar, Computer Science Department, B.B.D. University, Lucknow, Uttar Pradesh, India*
[2]*Assistant Professor, Computer Science Department, SITM, Barabanki, Uttar Pradesh, India*
[3]*Senior Lecturer, Information Technology Department, B.B.D.N.I.T.M., Uttar Pradesh, India*
rohitcss710@gmail.com, rohitsharma2412@gmail.com, avinash.verma93@yahoo.com

Abstract

In the today's world cloud computing has become a very prominent technology in field of research and business. It can be realized as assimilated technology of parallel computing, network storage technology, grid computing, distributed computing and other modern existing technologies. According to our comprehensive approach we know that cloud computing provides resources and services to their clients on behalf of their demands. These cloud services are sometimes abjured due to receiving a huge amount of requests. This type of retraction in service providence of cloud environment is also considered as Denial of service attack in cloud environment. DDoS attack is the enhanced form of DOS attack. In this paper the author is going to represent a framework for recognizing and analyzing this attack with the help of multi agent system. Here the author describes the integration of the results achieved by the Intrusion detection agents (IDA), existing inside virtual machine of cloud system with a method of data fusion in front- end. At the time of attack the IDA generates alert signals which will be stored inside the My sql database residing in Cloud synthesizing unit (CSU). The author propose a quantitative approach to explore the alerts yielded by IDA using Dempester Shapher Theory operation having three valued logic and Fault tree Analysis described for various flooding attacks. Finally we combine the results achieved by various IDAs.

----------***----------

1. INTRODUCTION

In the modern era cloud computing [4] [5] is playing a vital role in various areas such as scientific, medicals, research and academics. It is a well known service to the end user known as pay on demand service. It has reduced various IT overheads. It may be defined as a secured, cost effective and flexible service for the end user. The most important feature of this technology is accessibility and availability. As it provides virtualized services and resources to the client via internet. So there is a major issue of security for both ends, client side as well as server side.

DDOS attack [9] [10] is one of the most important issues in cloud environment. This attack neither tends to change or modify the data nor focuses to illegal or unauthorized access. It basically blocks the server or the network in order to intercept the services provided to end user. It can be implemented through various techniques such as IP spoofing, bandwidth attack, smurfing, flooding etc.[11]. In DOS attack, generally it takes sufficient amount time to identify a single invalid request and response against it. When there are multiple attacks taking place , the server becomes busy to respond against these attacks and does not capable for providing services to the client during that period. Then it is considered as DDOS attack in the cloud environment.

A multi agent system [1] [2] [3] is used for packet monitoring and intrusion detection which will work in communicating and co-coordinating manner with their proactive and reactive features. Since there is a lot of workload on the server in order to handle each nonsense request therefore here the author has proposed a framework with combination of packet monitoring approach implemented through packet monitoring agent and Intrusion detection system implemented through Intrusion detection agent.

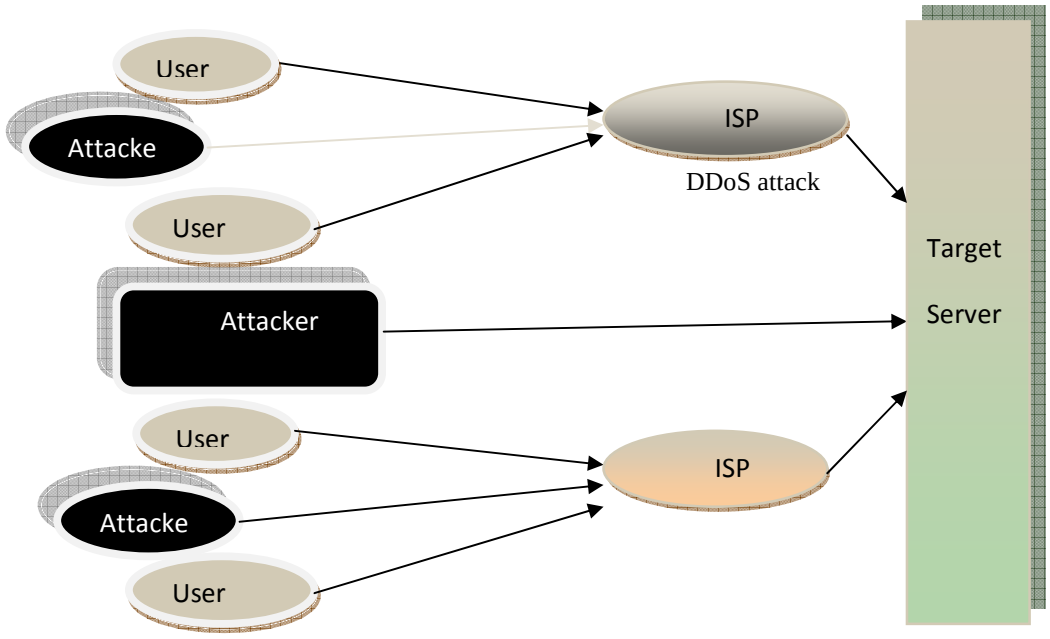

Fig 1: DOS attack

2. LITERATURE REVIEW

[1]. Alina Madalina Lonea Daniela Elena Popescu and Huaglory Tianfield [4], have described a concept for detecting DDoS attack in cloud computing by using IDS deployed in VMs of cloud system with a a data fusion methodology in front end. That generates alerts which is stored into the data base placed within cloud fusion unit of front end server. The basic concept is used to implement the task is Dampestar Shapher theory, fault tolerance analysis (for mentioned flooding attacks) and Dempestar's combination rule.

[2]. Vikas Chouhan & Sateesh Kumar Peddoju [6] have suggested a new way for protection of DDOS in cloud environment using packet monitoring approach which is also simulated in cloudsim toolkit. Here the author has given a concept of HOP count and filtering that provides a ungrudgingly available solution to protect cloud against DDOS attack. The algorithm requires regular monitoring of packets travelling in network and extracted the SYN flag, TTL value and IP information from the TCP/IP packets and checks that if SYN flag and TTL both values are not set then it provides the output that the packet is spoofed.

[3].J.J.Shah and Dr. L.G.Malik [7] have efficiently described the impact of DDOS attack in cloud computing and different types of DDOS attack at the different layers of OSI model with increasing complexity in performing attack and focuses more on prevention and detection of DDOS at different layer of OSI and effect of DDOS in cloud computing environment.

3. PROPOSED SOLUTION

As MAS is an emerging technology where complex problems are solved with collaboration, coordination and communication between agents where Agent can be simply viewed as self described autonomous software component or piece of codes. Here agent's capability and its characteristics like reactivity, pro-activeness, social ability etc are used to facilitate applications in cloud computing. Multi-Agent System will be beneficial for the construction of powerful, flexible, scalable and extensible system. It is helpful to detect and protect the cloud environment from DDOS attack and fault occurrence rate as it is now a challenging issue for researchers to protect cloud against this attack.

In this paper the author has focused to detect and remove basic two different intrusions as IP spoofing and flooding attacks with the help of multi agent system. In this approach the author has used multiple agents in order to detect and remove mention above DDoS attacks. Here the author has proposed an architecture in which packet monitoring agent is used to identify unauthorized packets travelling inside the network on the other hand an intrusion detection agent is used to detect and resolve various flooding attacks using TCP, UDP or ICMP packets. The complete working of the architecture is mentioned below-

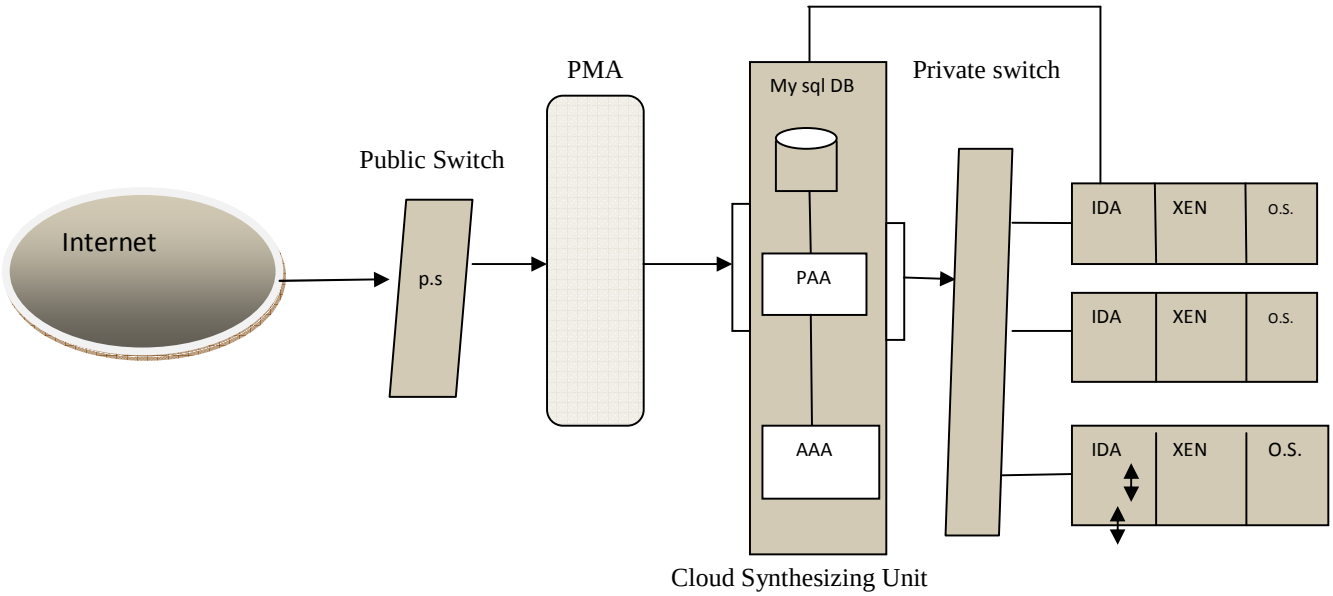

Fig 2: Implementation of MAS in cloud Intrusion Detection methodology

Packet Monitoring Agent: The basic aim of the packet monitoring agent is to regularly monitor the packets travelling in the cloud in order to determine spoofed packets. This can be implemented with the help of packet monitoring algorithm where various comparisons are performed with respect to SYN and TTL(Time to live) value. It is considered that each packet is associated with a SYN flag and TTL value whose value is stored in IP2HC table. The packet monitoring agent uses the approach of this packet monitoring algorithm in which at any instant of time if it is found that the SYN flag= 0 and Source IP value =0 and hop count is calculated by TTL, if the calculated hop is not equal to the stored hop in IP2HC table, it means that there are no any entries in the IP2HC table for that particular packet and that is not considered as an authentic packet and declared as a spoofed packet, because every authentic IP address having a TCP connection must have its entry in IP2HC table and it is blocked for further movement in the network.

Intrusion Detection Agent: There are multiple IDAs are used with each virtual machine in order to reduce the workload of single IDA. In large network access it is very difficult to analyze and resolve the attack by a single agent. Hence the network traffic is now splitted into the IDAs and each agent will work in communicating and collaborative manner. The packets forwarded through the PMA are further analyzed by the IDAs in order to check the mentioned flooding attacks. These IDAs generates alerts by ID sensors deployed with IDAs and these alerts are further stored in MY SQL data base deployed in Cloud synthesizing unit. The Cloud synthesizing unit having the capability to analyze the results using the Dempester Shapher Theory of proof containing 3 valued logic and an analysis of fault tree for IDAs for every virtual machines. At the end of the analysis the whole result transmitted by sensors are now integrated by using Dempester combination rule. The major objective of this paper is get a collaborating effort by each IDA. Whenever any IDA is out of work at any instant of time then it will request for work to another IDA, if the another IDA needs the help of requesting IDA then it will provide an acknowledgement signal to the requesting one, then the requesting IDA will also work in a collaborative manner in order to remove the attack from the specific node, due to this feature the multi agent system will be more helpful to get rid of problem of agent overloading and slow handling against each nonsense request.

In our proposed solution we have implemented a private cloud containing three nodes and after completing the detection phase by IDAs implemented within the virtual machines the attack assessment process is executed by the Attack Assessment Agent. This agent basically requires the probability assignment of each packet .Which can be done by using Probability Assignment Agent.

Probability Assignment Agent: The basic work of this agent is to assign the probability to each packet for possible flooding as TCP, UDP, and ICMP. Here we use an state space K and three valued DST operations (YES, NO, (YES, NO)) for possible flooding attacks as TCP, UDP, and ICMP for every virtual machine based IDAs. Then some imitation code is provided in order to convert the alert accessed from IDAs. The

basic aim of this code is to obtain mentioned below probabilities of alerts received from IDAs.

Suppose that:
Mass of UDP=A
Mass of TCP=B
Mass of ICMP=C

Then we can write it as

(mA(y),mA(N),mA(Y,N))

(mB(y),mB(N),mB(Y,N))

(mC(y),mC(N),mC(Y,N))

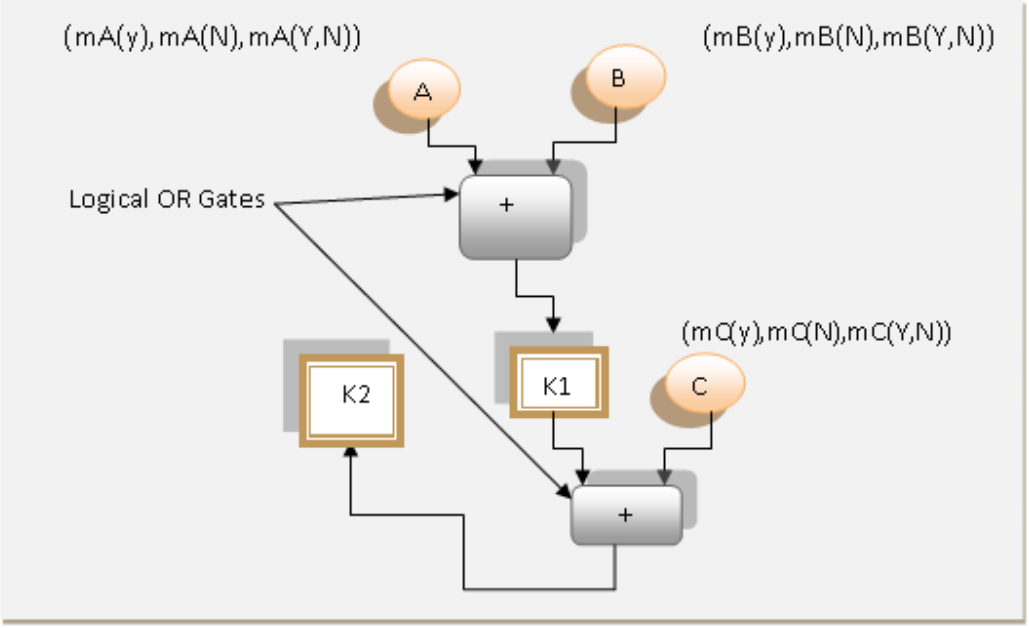

Fig 3 Computation for probability assignment

Conversion of Alerts into Probability Assignments using code:
For every node
Start

For all E □ (TCP, ICMP, UDP)

1) Query for alerts from My-Sql when any attack E takes place for specified host name.
2) Query the possible alerts against attack E for each for all hostname.
3) If the attack E is unknown then make a query from My Sql Database.
4) Compute "Yes" for E such as :
   Yes (E) = result obtained from *first* step/ result obtained from *Second* step
5) Compute " *(Yes, NO)"* for attack E such as :
   Yes, No (E) = result obtained from *Third* step/ result obtained from *Second* step
6) Compute "No" for E such as:
   No (E) = 1- (yes (E) + yes, No (E))

End

After computing the probabilities for each attack packet , the probability for each IDA should be calculated mentioned below the fault tree as described in figure 3 which contains the total calculated probability of attack on the first IDA represented by T. It can be represented as:

mT1(y), mT1(N),mT1 (y,N).

Hence using this approach we can can also compute the Belief and Possibility of attack for all IDA as :

Belief= mT1(y) and

Possibility= mT1(y)+ mT1(y,N)

Attack Assessment Agent:The basic work of this agent is to assess the attack by analyzing the combination of result provided by various IDAs . This can be easily achieved by using Dempester's combination rule. Which is helpful to increase the "TRUE DDoS positive rates" and decrease the" False DDoS positive rates."

CONCLUSIONS

As it is very clear to us that here Dempester Shapher Theory is used to analyze and detect the DDoS in Cloud implemented with Intrusion Detection Agent. But here the author has used various factors which are helpful to detect and avoid DDoS from cloud. The use of multiagent system makes the proposed methodology more efficient with reference to extra workload and speed up factors.

Besides this the communicating and collaborative property of the agents are used in which at any instant of time if one agent is busy enough in order to handle with nonsense request and not capable to provide services to authentic users then the free agent communicates with the busy one in order to share the workload of busy agent this also makes the processing faster comparatively previous solutions.

REFERENCES

[1] M. Wooldridge, "Intelligent agents," in Multi-Agent Systems, M. Wooldridge and G. Weiss, Eds., pp. 3–51, MIT Press, Cambridge, Mass, USA, 1999.

[2] S.M. Wooldridge and N. R. Jennings, "Intelligent agents: theory and practice," The Knowledge Engineering Review, vol. 10, no. 2, pp. 115–152, 1995.

[3] M. Wooldridge, An Introduction to Multi-agent Systems, John Willey & Sons, New York, NY, USA, 2003.

[4] A.M. Lonea, D.E. Popescu, H. Tianfield, Detecting DDoS Attacks in Cloud Computing Environment, INT J COMPUT COMMUN, ISSN 1841-9836, 8(1):70-78, February, 2013.

[5] Muhammad Zakarya, DDoS Verification and Attack Packet Dropping Algorithm in Cloud Computing, World Applied Sciences Journal 23 (11): 1418-1424, 2013,ISSN 1818-4952,© IDOSI Publications, 2013,DOI: 10.5829/idosi.wasj.2013.23.11.950.

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

[7] J.J.Shah Dr. L.G.Malik, Impact of DDOS Attacks on Cloud Environment, International Journal of Research in Computer and Communication Technology, Vol 2, Issue 7, July-2013,ISSN(Online) 2278-5841,ISSN (Print) 2320-5156.

[8] Priyanka Negi, Anupama Mishra and B. B. Gupta Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment.

[9] Nisha H. Bhandari, Survey on DDoS Attacks and its Detection & Defence Approaches, International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-3, February 2013.

[10] Amit Khajuria, Roshan Srivastava, Analysis of the DDoS Defence Stratigies in Cloud Computing, INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS,VOL. 2, ISSUE 2, FEB.-2013 ISSN NO: 2319-7471.

[11] Upma Goyal, Gayatri Bhatti and Sandeep Mehmi ,A Dual mechanism for defeating DDoS in cloud computing Model, International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 – 4847, Volume 2, Issue 3, March 2013.

BIOGRAPHIES

Rohit Srivastav is pursuing M.Tech. from B.B.D. University and completed his B.Tech. in Computer science. He has also published papers in international journal.

Dr. Rohit Sharma received his Ph.D. degree in computer science and guided number of M.Tech. thesis. He has also published research papers in international journal and also a reviewer of few international journals.

Avinash Verma received his M.Tech. degree in Computer Science and also pursuing Ph.D. in Computer Science. He has guided various M.Tech. thesis.