Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.177 – 184

RESEARCH ARTICLE

EFFECTIVE INTRUSION DETECTION AND REDUCING SECURITY RISKS IN VIRTUAL NETWORKS (EDSV)

B.Ashok[1], V.Sucharitha[2]

[1]M.Tech 2nd year, Dept. of CSE, ASCET, Gudur, India

[2]Associate Professor, Dept. of CSE, ASCET, Gudur, India

[1] ashok20.86@gmail.com; [2] jesuchi78@yahoo.com

***Abstract:** Cloud computing provides multiple services to the cloud users, particularly in Infrastructure as a service (Ias) clouds user may install vulnerable software on their virtual machines. Attackers exploit these virtual machines to compromise as zombie and by using it attacker can perform Distributed denial of service (DDOS) attacks. The Distributed Denial of service attacks (DDOS) caused by the extreme flow of requests from clients to the cloud sever at the same time. The DDOS attacks are very much high in the existing Intrusion detection systems. To overcome these problems a modified approach called Effective Intrusion Detection and reducing Security risks in Virtual Networks (EDSV) is proposed. It enhances the intrusion detection by closely inspecting the suspicious cloud traffic and determines the compromised machines A novel attack graph based alert correlation algorithm is used to detect DDOS attacks and reduced to low level by incorporating access control and software switching mechanism. It also reduces the infrastructure response time and CPU utilization.*

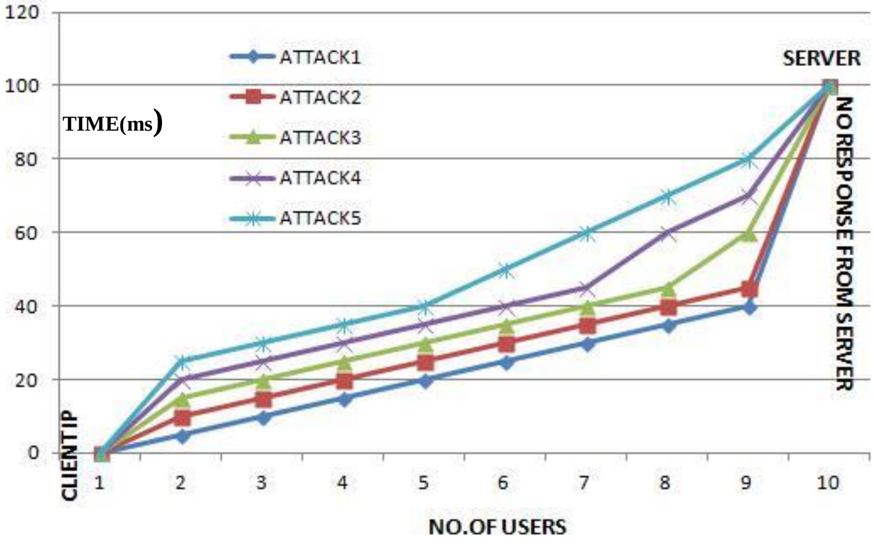
***Keywords:** cloud computing, Network Security, DDOS, Intruder, Zombie detection*

I. INTRODUCTION

Cloud computing is a model for facilitating convenient, on-demand network access to a shared pool of configurable computing resources. It supports three important models such as platform as a service (Paas), infrastructure as a service (IaaS) and software as a service (saas). In IaaS, the cloud provider supplies a set of virtualized infrastructural components such as virtual machines (VMs) and storage on which customers can build and run applications. These applications are reside on their VM and the virtual operating system. Issues such as trusting the VM image, securing inter-host communication, hardening hosts are critical in cloud environment. However, customers are also very concerned about the risks of Cloud Computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable. The major threats for cloud system include: Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage. This paper focuses on Abuse and Nefarious Use of Cloud Computing. SLA is a service level agreement between the service provider and the consumer. It consists the common understanding about services, priorities, responsibilities, warranties and guarantees. In cloud computing environment SLAs are necessary to control the use of computing resources. However, patching known security holes in cloud data centers where cloud user have access to control their software installed virtual machines may not work effectively and that violates service level agreements. Virtualization is considered to be one of the important technologies that help abstract infrastructure and resources to be made available to clients as isolated VMs. A hypervisor or VM monitor is a piece of platform-virtualization software that lets multiple operating systems run on a host computer simultaneously. Also this technology allows generating virtualized resources for sharing and it also increase the attack surface. We need a mechanism to isolate virtual machines and secure communication between them. This cloud computing is done with flexible access control mechanism that governs the control and sharing capabilities between VMs with in a host. Compromised machines are one of the major security threats over the internet. They are often used to launch a variety of security attacks such as Distributed denial of service attack (DDOS), spamming, and identity theft. Security issues over cloud computing is definitely one of the major concerns it prevent the rapid development of cloud computing.

II. EXISTING SYSTEM

In a cloud system, where the infrastructure is shared by potentially millions of users, attackers can explore the vulnerabilities of the cloud and use of its resource to deploy attacks in more efficient ways. Existing system focuses on the detection of compromised machines that have been recruited to serve as spam zombies. The DDOS attacks have been counter measured by using approaches such as Entropy Variation method and Puzzle based Game theoretic strategy. If the number of requests made by the attacker increases the efficiency of the entire system will be reduced.

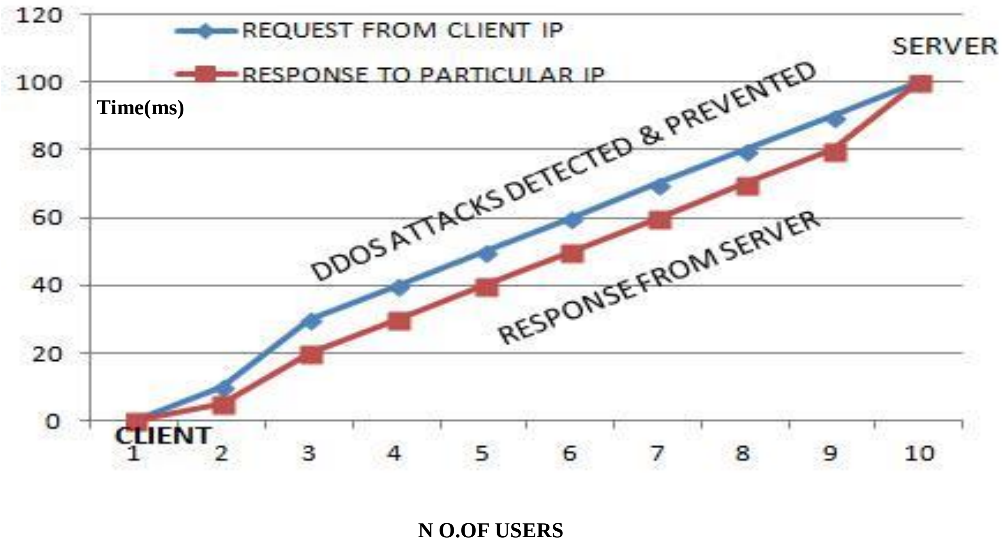


The above fig X-axis specifies the number of users and Y-axis specifies the time in milliseconds. The fig shows that attacker performs five distributed denial of service attacks in few milliseconds. As a result of these attacks, client may wait and expect response from the server but the server does not register the response according to the client request. This automatically increases the infrastructure response time which also cause increase CPU utilization i.e. it is also increase time taken to create virtual machines.

III. PROPOSED SYSTEM

In the proposed system, avoiding compromised virtual machines by using multiphase distributed vulnerability attack detection and measurement. Analytical attack graph model is used for attack detection and prevention by correlating attack behavior and suggests effective countermeasures.

Attack graph is constructed by specifying each node in the graph represent exploits and each path from initial node to target node represent successful attack. EDSV incorporates software switching solution to isolate suspicious virtual machine for further detailed investigation.



The above fig X-axis specifies the number of users and Y-axis specifies the time in milliseconds. The fig shows that the number of users and duration using the system is same as in previous approach. In EDSV, DDOS attacks are effectively prevented before they incorporate into cloud and causing further damage to the cloud system. The client waiting for the response from the server is delivered in appropriate time. So that it reduces the infrastructure response time and also CPU utilization i.e. it is also cause less time to create virtual profile.

i. **Authorization and Access control:**

The cloud service provider allows authenticated users to access a server for storing and retrieving data. Virtual machines allows to store the information about the client requests like port no,ip address, MAC address etc .This Intrusion detection management system detects the alert by maintaining five tables and timer. The tables are Account T1, Intruders table T2, Authenticated client T3, Unauthenticated client T4, client list T5.T1 is used to check the client by using MAC address.T2 contains the address of already known intruders.T3 contains the MAC address of the clients who are in communication process, login time and logout time.T4 records the MAC address login and logout time of clients.T5 contains the MAC address and login time of all clients.

Alg1:Authentication and Access control

```
Event type (login, logout)
If (event Request = login)   then
    int_mac_a = get_ Mac_Address() //Get the mac address of the client
    If (int_mac_a is in T2)  then //Check the intruder list
        (Ignore the request)
    else if ( int_mac_a is in T3)  then //Check authenticated client list
        (Ignore login request) and (store int_mac_a in T2)
    else if ( int_mac_a is in T5)   then //Check Current Client's List
        (Ignore the request)
    else
        (Accept the login request) and (Start communication)
    end_ if
    end_ if
    end_ if
end_ if
```

ii **Intrusion detection by using Alert correlation**

Attack analyser performs three major functions such as attack graph construction, alert correlation and countermeasure selection. The process of constructing scenario attack graph (SAG) consists of three major functions such as information gathering, attack graph construction and exploit path analysis. Attack graph is constructed by specifying each node in the graph represent exploits and each path from initial node to target node represent successful attack. The Attack analyser also performs alert correlation and analysis by constructing Alert correlation graph and providing threat information to network controller. When Attack analyser receives an alert it checks the alert already exist in the attack graph and performs countermeasure selection. It notifies network controller to deploy countermeasure actions or mitigating the risk. If the alert is new then attack analyser performs alert correlation and then update SAG, ACG .If the alert is a new vulnerability and not present in attack graph then attack analyser reconstructing the graph by adding it.

Algorithm2: Alert correlation algorithm

step1: **preparation**- In the preparation phase, all the system and network information is loaded, the database with alert classifications is imported, and the attack graph AG for the network is loaded.

Step 2: **Mapping**: The mapping function *maps* the matching alerts to specific nodes in the AG. Alert mapping can be done by determining source, destination of and classification of alerts.

Step 3: **Aggregation:** Let alerts A is subset of *A* be the set of alert that is supposed to be aggregated. Let *th* be a threshold, The alert aggregation combines alerts that are similar but where created together in a short time ,i.e., the difference of the timestamps is below a certain threshold *th.*

Step 4: **Alert Dependencies:** Let *Am is a subset of A* be the set of alerts that have been matched to a node in an AG: The dependency graph *DG* is defined by the matched and aggregated alerts *Am* as vertices and the relations between these alerts as edges.

Step5: **Searching:** Each path in the alert dependency graph *DG* specifies a subset of alerts that might be part of an attack scenario. *Dependency Graph is* used in the last step to determine the most interesting subsets of alerts and also the most interesting path in the alert dependency graph.

iii **Software Switching Solution**

The network controller is a major component to supports the programmable networking capability to realize the virtual network reconfiguration feature based on the Open Flow protocol. In EDSV, each cloud server consists a software switch which is used as the edge switch for VMs to handle traffic in and out from VMs. Conceptually switch function is divided into two pieces such as control plane and data plane. The control plane is the core part of switch which handles the discovery, routing, path communication and communication with other switches. The control plane creates a flow table and it is used by the data plane to process the incoming packets. Open flow protocol lets you delegate the control plane of all the switches to the central controller and lets the central software to define the behaviour of the network.

The network controller is responsible for collecting network information of current attack graphs it includes current data paths on each switch and the detailed flow of information associated with these paths, such as TCP/IP and MAC header. The network controller automatically receives information about network flow and topology changes after that it sends the information to attack analyser to reconstruct attack graph. We integrate the control functions for both open flow switch, open virtual switch so that that allows the cloud system to set the security and filtering rules in secure and comprehensive manner. Based on the security index of Virtual machine and severity of an alert, countermeasures are selected and executed by Network controller.

IV. CONCLUSIONS

In this paper, we proposed a solution to detect DDOS attacks early and preventing the system from attacks. We have used a novel alert correlation algorithm which creates alert correlations and suggests effective countermeasures. Software switches based solutions used to improve the detection accuracy as a result there is an improvement in the performance of the cloud with the depletion in the CPU utilization, Infrastructure response time and VM creation time. In order to improve the detection accuracy, hybrid intrusion detection solutions are needed to be incorporated and to cover the whole spectrum of IDS systems in the cloud system.

References

1. H. Takabi, J. B. Joshi, and G. Ahn, “Security and privacy challenges in cloud computing environments,” IEEE Security & Privacy,vol. 8, no. 6, pp. 24–31, Dec. 2010.

2. B. Joshi, A. Vijayan, and B. Joshi, “Securing cloud computing environment against DDoS attacks,” IEEE Int’l Conf. Computer Communication and Informatics (ICCCI ’12), Jan. 2012

3. Cloud Security Alliance, “Top threats to cloud computing v1.0,” https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf,March 2010.

4. Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, “Detecting spam zombies by monitoring outgoing messages,” IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198–210, Apr. 2012.

5. R. Sadoddin and A. Ghorbani, “Alert correlation survey: framework and techniques,” Proc. ACM Int’l Conf. on Privacy, SecurityAnd Trust: Bridge the Gap Between PST Technologies and Business Services (PST ’06), pp. 37:1–37:10. 2006.

6. S. Roschke, F. Cheng, and C. Meinel, “A new alert correlation algorithm based on attack graph,” Computational Intelligence in Security for Information Systems, LNCS, vol. 6694, pp. 58–67.Springer, 2011.

7. P. Ammann, D. Wijesekera, and S. Kaushik, “Scalable, graph based network vulnerability analysis,” Proc. 9th ACM Conf. Computer and Comm. Security (CCS ’02), pp. 217-224, 2002.

8. S. H. Ahmadinejad, S. Jalili, and M. Abadi, “A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs,” Computer Networks, vol. 55, no. 9, pp.2221–2240, Jun. 2011.

9. “Open vSwitch project,” http://openvswitch.org, May 2012.

10. L. Wang, A. Liu, and S. Jajodia, “Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts,” Computer Communications, vol. 29, no. 15, pp. 2917–2933, Sep .2006