Detection and Isolation of Zombie Attack under Cloud Computing

Sagar Choudhary[1], Garima Pundir[2], Yashveer Singh[3]

[1,2]Assistant Professor, Dept. of Computer Science and Engineering, Roorkee College of Engineering, Roorkee, Uttarakhand, India
[3]Head of Department, Dept. of Computer Science and Engineering, Roorkee College of Engineering, Roorkee, Uttarakhand, India

---

Abstract - Clouding Computing is very popular nowadays. It is the on demand availability of computer system resources like data storage and computing program, information or multimedia content. All these data or information is available to different user with the help of internet. The cloud computing architecture in which third party users, virtual machine and cloud service provider are involved for data uploading and downloading with the help of internet. Security of this architecture is the main issue, today*'s organizations, but there* exist many security vulnerabilities. Among all type of security attacks zombie attack is the most dangerous type of attack. This attack decreases the network performance in terms of delay, information and bandwidth consumption. In the zombie attack, some unauthorized user may join the network which spoof data of the authorized user and zombie nodes start communicate with virtual machine on the behalf of authorized user. In this proposed work, the technique based on the strong authentication which has been detecting malicious and unauthorized user from the network on cloud and isolates them from the cloud architecture. There are various techniques, methods and algorithms described in this paper to isolate a zombie attack and other security vulnerabilities at cloud architecture. We discuss the methods for detection and stopping this kind of zombie attack from cloud.

Key Words: Cloud Computing, Zombie Attack, DoS, Security, User, ID, Server Authentication

1. INTRODUCTION

Cloud computing is going to a new heights of computing technology, as we can have more resources to our hand now. Cloud Computing is an environment which offers the network only on-demand and for convenient access to computing resources like applications, storage, networks, servers and the another services which are effective. Cloud is a centralized data base of different type of data, in which a authorized user, who is actually the customer in cloud (free or paid), can retrieve and modifies the stored data. It means that the authorized user or the customer who is using the service of cloud has to pay (limited access for free clients) for whatever he/she is using or being used, stored and served. It is a technique which gives a large amount of applications under different network topologies and these network topologies provide some new specialized cloud services. Cloud computing provides shared resources, software and the information to the various computers and devices on demand because cloud computing is an internet based. E.g. Google cloud and other cloud service providers, a service of cloud and any user using their cloud either with premium account (account with some extra features) or free account. The problem of cloud computing is that any user can access the data of other user without the knowledge of that user.[1]

Network security, user security, data or information security and many other security types like the computer security together make the term "Cloud Security". It provides the large set of technologies, rules and controls that are used to provide the security to data and several applications that exist with the cloud computing environment. Security is the most concerning point to any cloud service; provide the cloud computing services to its clients. Only security ensures the privacy and integrity of the cloud data. There are many types of security issues exist:

1. Data Loss
2. Downtimes
3. Phishing
4. Password Cracking
5. Botnets
6. Sniffing
7. Spoofing
8. and Other Malware [1]

1.1 Service Models of Cloud Computing:

These three service models for cloud computing are:

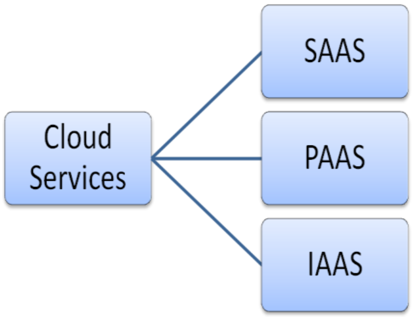

Figure 1: Service Model of Cloud Computing

- Cloud Software as a service (SaaS),
- Cloud Platform as a Service (PaaS) and
- Cloud Infrastructure as a Service (IaaS).

SaaS

To use the provider's applications running on a cloud infrastructure and available from different customer devices through a thin customer interface such as a Web browser. Saas is basically used for running the existing application like Facebook or Google Drive .The user does not deal with installation of any software on their physical machine. The cloud provides such software for running these types of applications.

PaaS

To set up on the cloud infrastructure customized applications using programming languages and tools supported by the provider (java, python, .Net). Paas provides the framework or platform on their own applications by using cloud and there is no need to install any platform on their own machine.

IaaS

To provision processing, storage, networks, and other fundamental computing resources where the customer is able to establish and run any software, which can consist of operating system and applications. Iaas provides a physical resources such as memory, processor etc.

2. ATTACKS IN CLOUD COMPUTING

There are many types of security issues as we discussed above are there in cloud computing. Due to these issues, attacks are possible in cloud. There are various potential attack vector criminals may attempt such as:

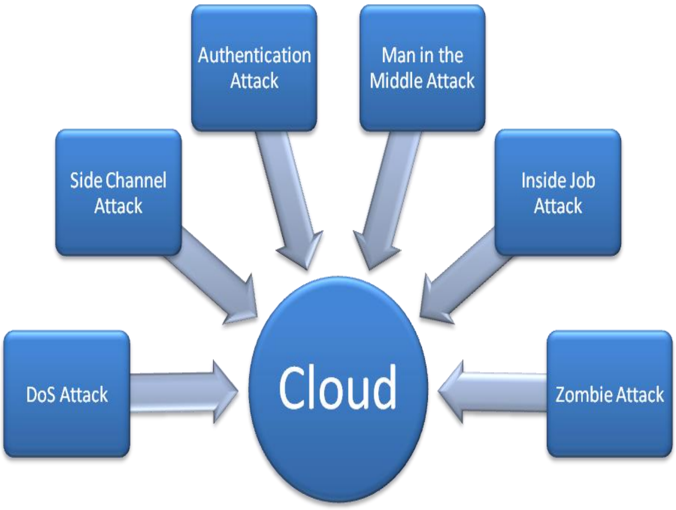

Figure 2: Type of Attack on Cloud Computing

2.1 Denial of Service (DoS) attacks

Many security specialized persons have contend that the cloud is more susceptible to DoS/DDOS attacks because this is shared by larger number of users which can create DoS attacks a lot more dangerous.[2]

2.2 Side Channel attacks

An attacker might try to compromise the cloud environment through placing a malicious virtual machine in close proximity to a target the cloud server and then take advantage of a side channel attack.

2.3 Authentication Attack

Authentication is a fragile point in virtual services as well as in hosted services and is frequently targeted. There is much different kind of ways to authenticate users for example based on what a person knows, has, or is. The technology used to secure the authentication process and the schemes used are a repeated aim of attackers.

2.4 Man-in-the-middle Cryptographic Attack

This type of attack is carried out when an attacker places himself between two communication parties. At anytime attackers can place themselves in the communication's path there is the probability that they can capture and modify communications message. In some cases users may be sending unencrypted information which means that the man-in-the-middle (MITM) can obtain any unencrypted data information. On other hand a user may be able to get hold of information from the attack but have to unencrypted the information before it can be read.

In the below figure is a sample of how a man-in-the-middle attack works. The attacker captures roughly or all traffics coming from the clients collect the information and then precede it to the target the user was initially intending to visit.

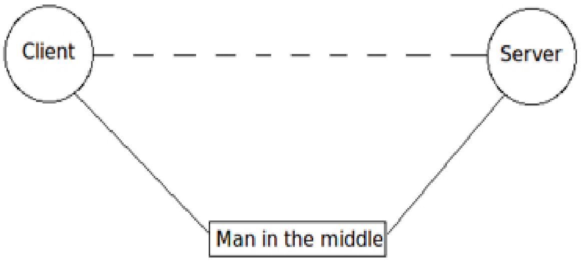

Figure 3: Man in the Middle Attack

2.5 Inside-job

These kind of attack is when the staffs, person or employee or who is knowledgeable of how the system move from client to server after that he can embed malicious codes to harm everything in the cloud environment.

2.6 Zombie Attack

Zombie attack is one of the advance attacks in cloud computing environment which degrades the performance of the network and throughput of the network. There are malicious nodes which act as a zombie of one of the connected users. A system that has been inserted with a program that puts it under the control of malicious users without the awareness of the system user. Zombie is used by malicious users to launch DoS or DDoS attacks. Through an open communication port, the illegitimate user sends commands to the zombie.

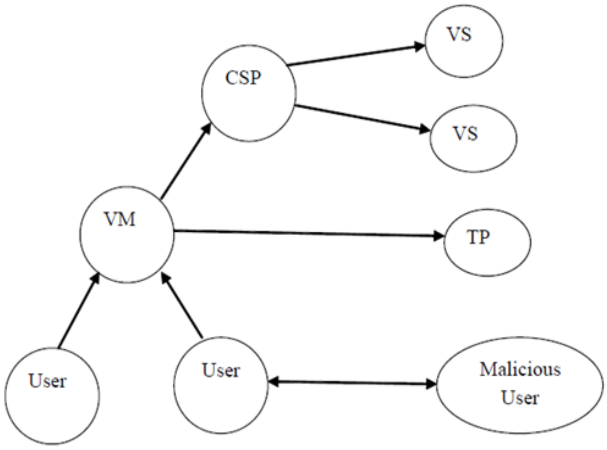

Figure 4: Zombie Attack

On command, the zombie system sends a huge amount of packets of worthless information to a targeted web site in order to block the site's router and keep genuine users from having access to the site. Traffic sent to web site is puzzling and as a result the system receiving the data use time and resource just to understand the flow of data has been sent out by the zombies.

According to above figure, Virtual Machine (VM) is described. VM is connected with cloud service provider (CSP) which is further connected with virtual server (VS). Third Party (TP) is available, which is directly connected with virtual machine. There are number of users which are connected to virtual machines. There is also one malicious user which spoofs credentials of connected user and act as a user, the whole process comes under zombie attack. [2]

3. VIRTUAL MACHINE AS ZOMBIES

Compromised machines are one of the major challenges in cloud systems which are used to launch various security threats to make the resources should not able to authenticate users. Such compromised virtual system grouped together is called virtual machine as Zombies. Within the cloud system, particularly the Infrastructure-as-a-Service (IaaS) clouds, the detection of such zombie exploration attacks is tremendously difficult because cloud users may install vulnerable applications on their virtual machines. To prevent such susceptible virtual cloud system from being compromised, we proposed NICE mechanism to provide countermeasure against Zombies with help of an attack graph-based model.

4. RESEARCH METHODOLOGY

In this paper, we propose Zombie attack detection and its counter measure which detects zombie attack and also stop it. For better attack detection this project incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design Zombie attack does not intend to improve any of the existing intrusion detection algorithms; indeed, Zombie creates a reconfigurable virtual networking approach to detect and counter the Zombie attack.[3]

4.1 Design Module

User Module We create a window which shows the network by sing c# language in dot.net. After that we show how the data is flow from source to destination. Than we create a zombie attack and show its behavior and than we do its counter measure to stop the zombie attack. Steps are to create a network, than path is created to show how the data is travel after that we create a routing table and also create a encryption and decryption key for key management and security using MD5 and 3DES algorithm.[4]

4.2 Countermeasure Selection

To detect zombie attack we create its counter measure which actually stops the attack and save the power consumption of the machine.

4.3 Attack Analyzer

The system has level of security for protection of data which verifies the packet for detection of intruder so that the countermeasure can be applied attacks usually involve early stage actions such as multistep exploitation, vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the system, especially the detection of zombie exploration attacks is very difficult. Another important function of the network controller is to assist the attack analyzer module. According to the controller gets the first packet of a flow, it holds the packet and checks the flow for complying traffic policies. [5]

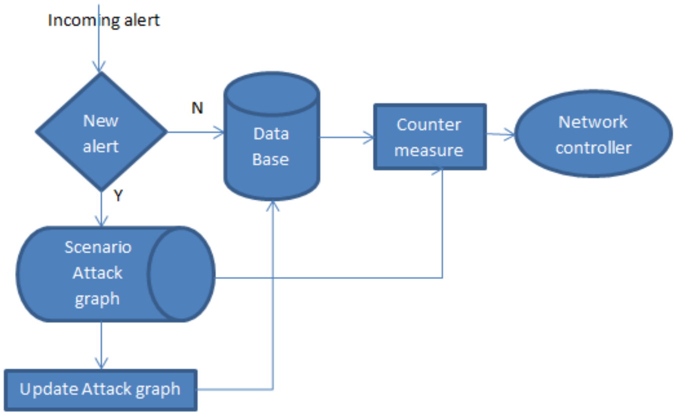

Figure 5: Monitoring and Updating Attack Graph

The methods for selecting the counter measures for a given attack scenario. When vulnerabilities are searched or some are identified as suspicious and dangerous, several countermeasures can be taken to stop or restrict attacker's capabilities and it is important to differentiate between compromised and suspicious packets. The countermeasure serves the purpose of:

1) Protecting the target VMs from being compromised, and

2) Making attack behavior stand prominent so that the attacker's actions can be firstly identified and then resolve.

The proposed system is useful for any kind of network because verification methodology is implemented at each hop through which attack accuracy is improved. Attack is countermeasure before attack is going to be happened in network.

The proposed solution is implemented in Network intrusion Detection System (NICE) and Host-based Intrusion Detection which also improved the attack detection accuracy. Network traffic is not disturbed because attack completely countermeasure. Data and information is secured after attack happened because it prevented before its reaction. Countermeasure selection is useful after attack happened because with used of it network traffic is not disturb.

NICE-Agent scans the complete cloud network periodically; once it finds vulnerability in cloud network it generates alert information and sends it to attack analyzer for further steps. Each path is a successful attack. Attack analyzer checks whether the alert is new or old one. If the incoming alert is of new vulnerability and is not present in the attack graph, the attack analyzer inserts the alert into the attack graph and then reconstructs it. Once construction gets completed, attack analyzer provides the countermeasure that is applied by the network controller based on the severity of evaluation results. Thus, we implement NICE mechanism to provide countermeasure against attacks.

5. IMPLEMENTATION

NICE- A is implemented in isolated bridges that are located between VM and Cloud server. NICE analyzes the cloud traffic with the help of a light weighted mirroring based detection agent system for avoidance of zombie attacks. Traffic generated by attacker through the virtual machine is monitored by NICE-A. Based on vulnerability, it generates and alerts the attack analyzer. Attack analyzer checks if it is new or old one, if alert is old, selects appropriate countermeasure otherwise construct SAG with the information gained from network controller, VM profiling and conducting some penetration test, VM profiling is a database that contains information about state, service running in VM, traffic vulnerability which is from SAG and NICE-A and it select countermeasure which is send it to the network controller, which issued to implement countermeasure and updates SAG.

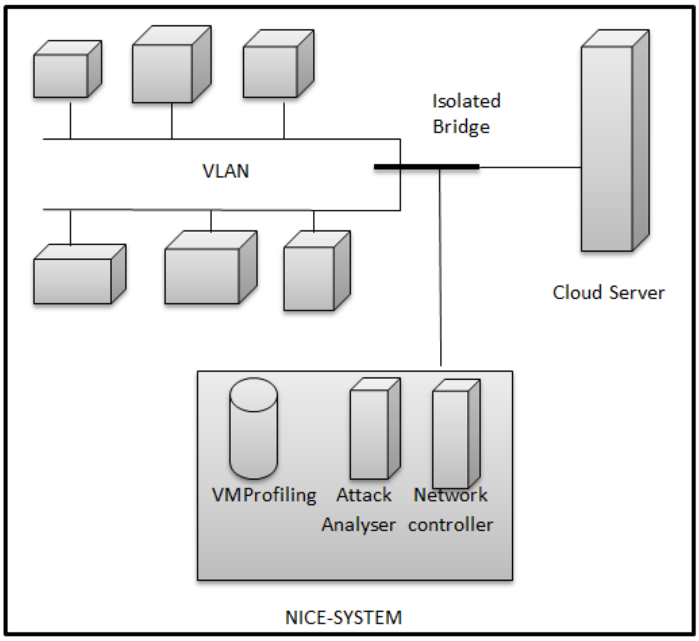

Figure 6: Architecture of NICE System

The countermeasure is based on dynamic that reconstruct filtering rules, rearranging allow & deny conditions, achieved by software switch which is controlled by network controller. So we are providing dynamic production against attack. NICE sniffs the traffic generated by attacker using SPAN. So the new affects original traffic. NICE allows the cloud server to provide service to requested customer or user continuously, at the same time it provides security to cloud server also.[9]

6. PERFORMANCE METRICS

Security matrices are needed to assess the risk. The distance to every target node must be determined before countermeasure selection. If the distance is too long, a countermeasure should not be selected, instead we update the ACG for an alert. [10]

A. CPU utilization

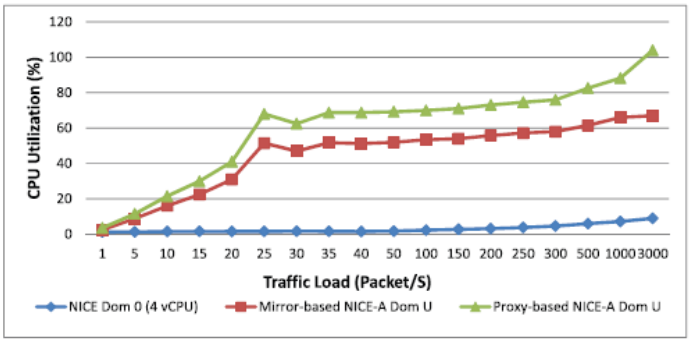

Figure 7: CPU utilization graph

NICE-A Dom O is better way for IDS because it utilizes less amount of CPU process that can be installed at bridges level

B. Network communication delay

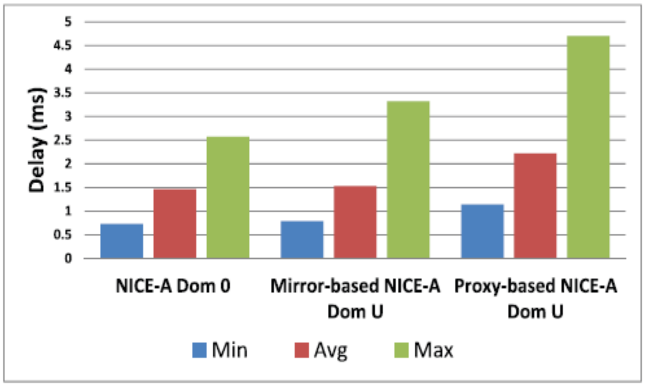

Figure 8: Performance of Network Communication

NICE–A Dom O is better because it uses SPAN to monitor traffic which makes less amount of delay. NICE-A Proxy based use original traffic to monitor the incoming outgoing packet. [11]

C. Success Measure Rate

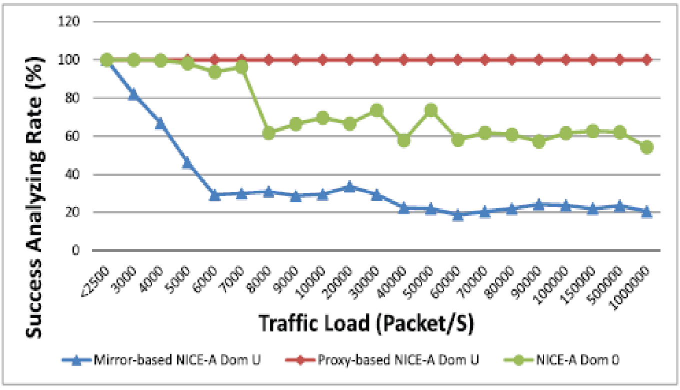

Figure 9: Success Measure Rate of Network Communication

Success analyze rate= No of analyzed packet/Total received packet

NICE-A Dom U is better because it uses original net traffic and it never bothers about packet delay. With the attack graph, we can get a holistic view of the security condition and make predictions.[12]

7. CONCLUSIONS

In the cloud architecture, some malicious nodes may join the network which is responsible to trigger zombie attack in the network. These zombie nodes can spoof the information of the legitimate user and communicate with virtual machine on the behalf of legitimate user. This will leads to reduction in network performance in terms of delay and bandwidth consumption. As cloud computing faces various security issues which lead to the exposure of confidential data of users. These security issues make users unstable about the efficiency, safety and reliability in cloud computing.

In this review paper, we presented NICE to protect cloud virtual networking environment from DDoS attack. NICE construct attack graph predicts the next step of the attackers and provides optimized countermeasure. NICE software switches implement the countermeasure against zombie explorative attack dynamically. To improve the detection accuracy, NICE are needed to be implement in distributed fashion. The proposed solution can reduce the risk of cloud system being misused by internal and external attack. The experimental results show less amount of CPU utilization and better success measure rate of traffic load.

8. ACKNOWLEDGEMENT

Authors would like to thank Roorkee College of Engineering, Roorkee, Dist-Haridwar, Uttarakhand.

9. REFERENCES

[1]Simanjot Kaura Anurag Singh Tomara Shashi Kant Shankara and Manmohan Sharma 2016. To Detect and Isolate Zombie Attack in Cloud Computing. International Journal of Control Theory and Applications, 9(45): 227-238.

[2] Kumar & Singh, Detection and Isolation of Zombie Attack under Cloud Environment, Orient. J. Comp. Sci. & Technol., Vol. 10(2), 338-344 (2017)

[3] B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf. Computer Comm. and Informatics (ICCCI '12), Jan. 2012.

[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] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation,” Proc. 16th USENIX Security Symp. (SS ’07), pp. 12:1-12:16, Aug. 2007.

[6] Chun-Jen Chung, Tianyi Xing, Pankaj Khatkar, Jeongkeun Lee,Dijiang Huang, on “NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems” IEEE transaction on dependable and secure computing, no.4,vol. 10, , pp.198-211, 2013 July/Aug..

[7] Lizhe W. and Gregor V. L. ,(2008), “ a Perspective Study: Cloud Computing,” volume 28 of Computing’s new Generation, Number 2, 137-146, DOI: 10. 1007/s00354-008-0081-5

[8] Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi “Securing Cloud Computing Environment Against DDoS Attacks”2012 international conference on computer informatics and communication Jan. 2012.

[9] Hassan Takabi and James B. D. Joshi University of Pittsburgh Gail- Joon Ahn Arizona State University www.computer.org/security Copublished by the IEEE Computer and Reliability Societies 1540 7993/10/$26. 00 © 2010 IEEE November/December 2010

[10] Bouzida Y, Cuppens F, Gombault S, (2006) on “Detecting and Reacting against Distributed Denial of Service Attacks,”IEEE International Conference on Communication. Volume 5

[11] Wayne Jansen, Timothy Grance, (Dec. 2011), “Guidelines on Security and Privacy in Public Cloud Computing” NLST-National

[12] K. Periasamy & B. Latha, “Zombie Avoidance using Attack Analyzer in Cloud Environment”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 3 Issue 4, April – 2014, pp-1869-1871

10. BIOGRAPHIES

Sagar Choudhary graduated from Uttarakhand Technical University, Dehradun, India (B.Tech-I.T.) in 2011 and received his Master’s from Uttarakhand Technical University, Dehradun, India (M.Tech-C.S.E.) in 2014. Currently he is working in Roorkee College of Engineering as Assistant Professor in the department of Computer Science and Engineering. His area of interest are wireless networks and cloud computing.

Garima Pundir graduated from Uttarakhand Technical University, Dehradun, India (B.Tech) in 2015 and received her Master’s from Uttarakhand Technical University, Dehradun, India (M.Tech) in 2017. Currently she is working in Roorkee College of Engineering as Assistant Professor in the department of Computer Science and Engineering. Her area of interest are image processing and cloud computing.

Dr. Yashveer Singh completed his Master of Technology (M.Tech) in 2011 and Doctorate of philosophy (Ph.D) in 2016. He published more than 15 International journals and attends many conferences in reputed institute and university.