Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Network Intrusion Detection, Countermeasure Selection and Prevention in Cloud

Mandar Mahadeokar*
Department of Computer Engineering,
Sinhgad Academy of Engineering,
University of Pune, Maharashtra, India

S. B. Rathod
Department of Computer Engineering,
Sinhgad Academy of Engineering,
University of Pune, Maharashtra, India

Abstract— Cloud computing offers great potential to improve productivity and reduce costs, but at the same time it possesses many new security risks. In this paper we identify the possible security attacks on clouds. Cloud computing technology is a new concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. Consumers can typically requests cloud services via a web browser or web service. Using cloud computing, consumers can safe cost of hardware deployment, software licenses and system maintenance. On the other hand, it also has a few security issues. To prevent such a vulnerable virtual machines from being compromised or hacked in the cloud by the attacker, we proposed a system which has multi-phase vulnerability detection mechanism, after detection it will take appropriate counter measure mechanism. Finally it will prevent the cloud environment from being compromised by attacker by providing security mechanism

Keywords— Cloud computing, Infrastructure as a service (IaaS), Zombie, Information secrecy, Information integrity, Vulnerable

I. INTRODUCTION

Cloud Computing enables multiple users or clients to access the resources independently and concurrently. Cloud computing is internet based computing which allow large groups of remote servers to allow sharing of data-processing tasks, centralized data storage, and provides online access to computer services or resources. Cloud computing also allows access to any resources to any client at anytime from anywhere in world. So there are several fields in cloud computing that required more attention to be given such as data privacy, data secrecy, data integrity, data security. When we are talking about cloud security, it is very important to keep in mind that to maintain security of cloud environment it is very difficult and most challenging task. One of the most important threats to cloud is nothing but Intruders. In computer security Intruders is nothing bur outsiders or attackers who try to disturb functionality of system by performing various illegal actions such as DOS, DDOS attacks. There are normally two types of Intruders. First Network Intruders and second is Host Intruders. So depending on this there are two types of Intrusion Detecting Systems (IDSs). A Network Intrusion Detection System (NIDS) is intrusion detection systems that try to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. A recent Cloud Survey Alliance (CSA) survey reports state that among all Security issues exploitation and despicable use of cloud computing is considered as the main security threat. The purposed system normally focuses on Network Intrusion Detection and tries to prevent the system from attacker.

II. RELATED WORK

All Chun-Jen Chung,Pankaj Khatkar,TianyiXing,Jeongkeun Lee purposed a NICE framework which having advantage of attack detection and detection accuracy. But the disadvantage is that they do not provide any prevention mechanism. That means system only find out an attack and take appropriate counter measure[1]. H. Takabi, J. B. Joshi, and G. Ahn gives brief description of Cloud computing include on-demand self-service, broader network access, location independent resource pooling, rapid elasticity and measured service. This paper also focuses on disadvantages of cloud computing such as Authentication and Identity Management, Access control and Accounting, Privacy and Data protection, Secure Service Management [4]. Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker paper focuses on effective spam zombie detection system named SPOT which is useful for monitoring outgoing messages of network. SPOT is designed which is based on Statistical tool called as Sequential Probability Ratio Test, which has bounded false positive and false negative error rates[5]. G. Gu, P. Porras, V.Yegneswaran, M. Fong, and W. Lee gives detail information about BotHunter. It is an application designed to track the two-way communication flows between internal assets and external entities, it is also helpful to monitor system for real-time detection of Internet malware infections [6].

III. EXISTING SYSTEM

In existing system there are several drawbacks were identified. User or Client install the vulnerable software on their own virtual machine because of this attacker can easily find an entry point in cloud through such software. So the main

challenge is to establish an effective vulnerability/attack detection and response system which will accurately identifying attacks and minimizing the impact of security breach to cloud users. In cloud system as infrastructure is shared among multiple users this is helpful for attacker to use its resources for carrying out an attack in more efficient ways. The existing system is nothing but approaches which are used by different cloud service provider within their own cloud environment. So it depends on cloud service provider that which approach is to be suitable for them. Cloud Security is such vast and big issue now days we are facing. To provide security is not an easy task because different provider may use different architecture, different protocols and so on. So it is very important to provide a centralized architecture so cloud will be enough secure. The disadvantage of the existing system is that it does not provide attack prevention mechanism as well as there is low accuracy in the attack detection.

IV. PROPOSED SYSTEM

In this article, we propose a system which will overcome the drawback of existing system. From the figure 1, we see that overall project lies within the boundary of cloud. To implement and test result it is very important to build own private cloud. So cloud is build by using OpenStack software framework. We are going to use architecture of OpenStack having Ice House version. Following figure shows that final environment consists of attacker, legitimate

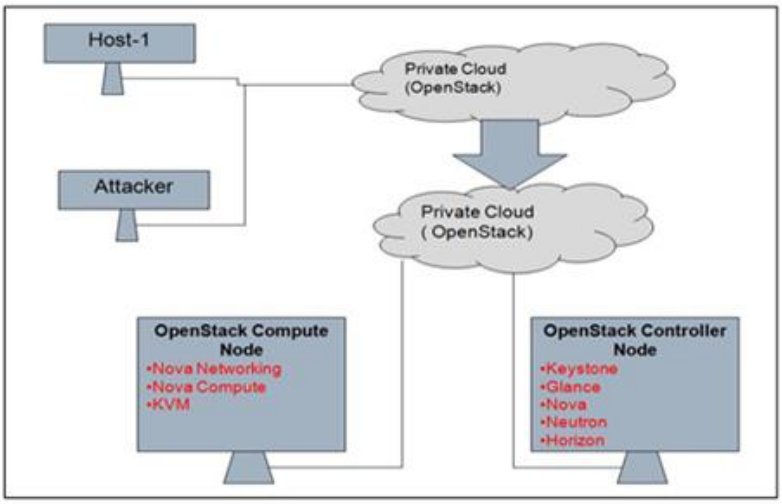

Fig.1Proposed Architecture

user and finally cloud service provider. This cloud was being built by using open source framework called as Openstack. Proposed systems overcome the drawback of existing system. In this system we are mainly focuses on attack detection and prevention. Existing system allowed user to install vulnerable software because of this attacker can easily find the susceptible point to enter into cloud and compromise them. But in proposed system we provide strong authentication management and provide only limited access to cloud.

V. PROJECT FLOW

The final scenario is that attacker attacks on cloud which contains multiple cloud services. Attacker tries to access the cloud illegally. So it is responsibility of CSP that is Cloud Service Provider to provide security to the cloud. As we are

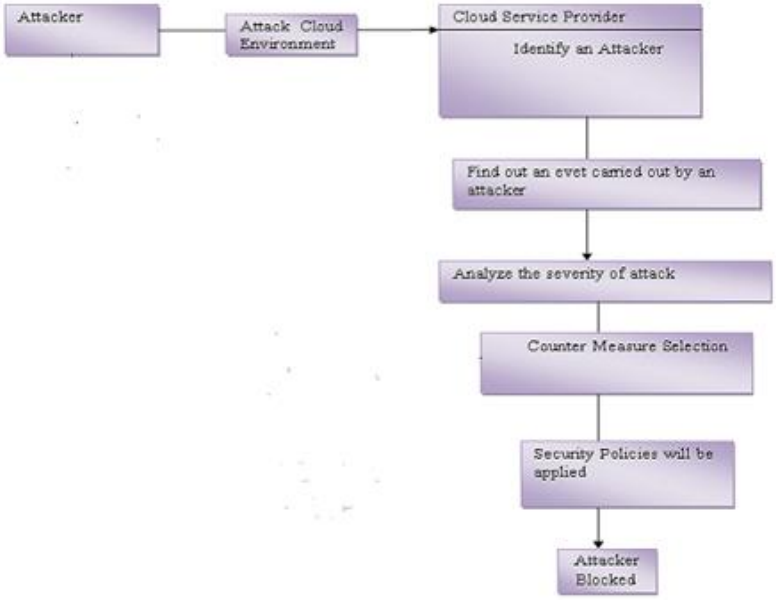

Fig 3. Project Flow

going to develop our own private cloud so it is very important to consider venerable parts of the cloud. So when attacker attack on cloud, the Cloud Service Provider detect attacker. There after system check or find out events those are carried out by an attacker. System also analyzes and determines the severity of attacks. And depending on that Counter measure selection process is carried out. And finally by using the built in policies or security mechanism proposed System block the attacker forever so that the attacker will never or cannot access the cloud services illegally. Countermeasure is nothing but simply blocking the ip address of attacker. And deal with this ip, so that attacker can't perform any malicious activity in future.

VI. IMPLEMENTATION DETAILS

1. OpenStack Software

OpenStack is opensource cloud computing platform. It is normally use to deploy Infrastructure as a Service (IaaS) solutions. It can controls a large pools of compute storage and networking resources through datacenter which is managed through dashboard or via OpenStack API.

2. Ubuntu Operating System

Ubuntu is a Debian-based Linux operating system, with Unity as its default desktop environment. It is based on free software and named after the Southern African philosophy of ubuntu. Development of Ubuntu is led by UK-based Company owned by South African entrepreneur Mark Shuttleworth.The Ubuntu project is publicly committed to the principles of open source development; people are encouraged to use free software, study how it works, improve upon it, and distribute it. Ubuntu's goal is to be secure "out-of-the box". By default user's programs run with low privileges and cannot corrupt the operating system or other user's files.

VII. RESULT

This section contains the practical implementation. Figure 3 is nothing but snapshot of OpenStack Horizon. To configure a private cloud is a main challenge in front of us. The above snapshot gives overall idea of OpenStack and show that it is user friendly because of graphical user interface. The figure 4 shows the actual result.

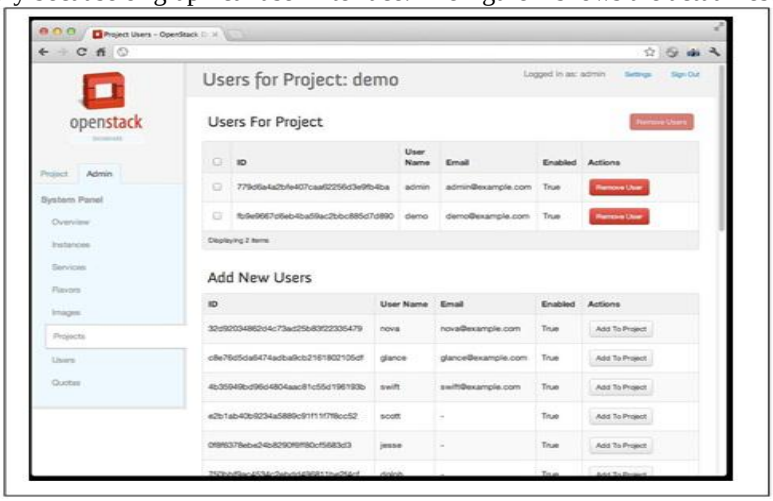

Fig 3. OpenStack Dashboard/Projects

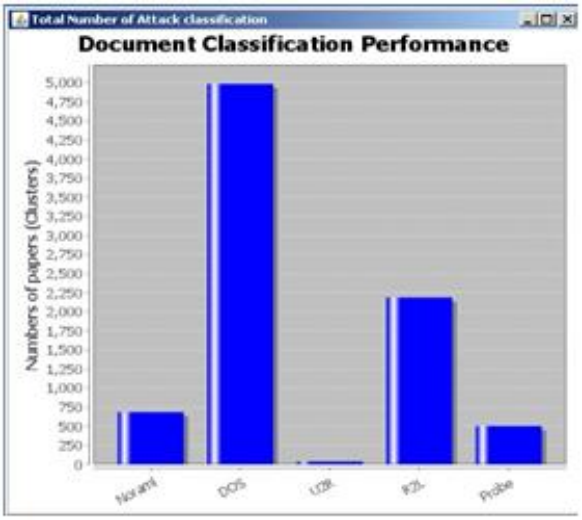

Fig 4. Result Classification

VIII. CONCLUSION

Use The proposed architecture is used to detect and mitigate collaborative attacks in the cloud virtual networking environment. The purpose is not to improve existing algorithms. It only investigates network IDS approach to counter zombie explorative attacks. The proposed system is able to identified by or distinguish between client and attacker by using efficient algorithms. And also the proposed system is providing security mechanism to cloud thus making secure cloud environment. In order to improve results that are the detection accuracy, we need to consider host-based IDS solutions are needed to be incorporated which will cover the whole spectrum of IDS in the cloud system.

ACKNOWLEDGMENT

The For First and foremost, we would like to thank to our P.G. Co-ordinator**, Prof. S. N.Shelke,** for his guidance and support. We will forever remain grateful for the constant support and guidance extended by guide. Through our many discussions, he helped us to form and solidify ideas. The invaluable discussions we had with him, the penetrating questions he has put to us and the constant motivation, has all led to the development of this project. We wish to express my sincere thanks to Head of the department **Prof. B. B. Gite**. Grateful thanks to the departmental staff members for their support. We would also like to thank to our friends for listening to our ideas, asking questions and providing feedback and suggestions for improving ideas.

REFERENCES

[1] R Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee. *"NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems."* IEEE Transaction on Dependable and Secure Computing VOL: 10 NO: 4 Year 2013.

[2] Anil Kumar Fatehpuria, Sandeep Raghuwanshi. *"An Efficient Wormhole Prevention in MANET through Digital Signature."* ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3.

[3] B.Joshi, A.Vijayan. *"Securing cloud computing environment against DDoS attacks."* IEEE Intl Conf. Computer Communication and Informatics (ICCCI 12), Jan. 2012.

[4] H.Takabi, J.B.Joshi, and G.Ahn. *"Security and privacy challenges in cloud computing environments."* IEEE Security and Privacy, vol. 8, no. 6, pp. 2431, Dec. 2010.

[5] 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. 198210, Apr. 2012.

[6] G.Gu, P.Porras, V.Yegneswaran, M.Fong, W.Lee. *"BotHunter: detecting malware infection through IDS-driven dialog correlation."* Proc. of 16th USENIX Security Symp. (SS 07), pp. 12:112:16, Aug. 2007.

