Review on Countermeasure Selection and Networking Intrusion Detection using Virtual Network Systems

Bhagyashri S.Virkhare **Sonali P Pote**

Abstract **-Virtually every factory and some parts of the public sector are using on cloud computing in this ERA, either as a provider or as a consumer. Despite being young it has not been kept untouched by hackers, criminals and other malicious initiator to break into the web servers. Once weakened these web servers can serve as a launching point for conducting further attacks against users in the cloud. One such attack is the DoS or its version DDoS attack. Particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions like multi-step exploitation, low frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of attacks exploration attacks is extremely difficult. To prevent vulnerable virtual machines from being compromised in the cloud, some projects are their who propose a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph based analytical models and reconfigurable virtual network-based countermeasures. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution. NICE are used by some organizations to detect the weaknesses in their security policies, documenting existing attacks, threats and violating preventing and secured an individual from security policies.**

Keywords- **Network Security, Cloud Computing, Intrusion Detection, Attack Graph, Zombie Detection.**

I. INTRODUCTION

Recent studies have shown that users migrating to the cloud consider privacy as the most important factor. A recent Cloud Security Alliance (CSA) survey shows that among all security issues, abuse and treacherous use of cloud computing is considered as the top security threat, in which attackers can utilize vulnerabilities in clouds and utilize cloud system resources to deploy attacks [1]. In traditional data centers, where system administrators have full control over the host machines, vulnerabilities can be detected and patched by the system administrator in a centralized manner. However, patching known security holes in cloud data centers, where cloud users usually have the privilege to control software installed on their managed VMs, may not work effectively and can violate the Service Level Agreement (SLA). Furthermore, cloud users can loaded vulnerable software on their VMs, which essentially contributes to loopholes in cloud security. The challenge is to organize an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impression of security breach to cloud users. In, M. Arm burst et al. addressed that protecting "Business continuity and services availability" from service outages is one of the top concerns in cloud computing systems [2]. In a cloud system where the infrastructure is shared by potentially millions of users, abuse and treacherous use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resources to locate attacks in more efficient ways. Such attacks are more effective in the cloud environment since cloud users usually share computing resources, e.g., connected through the similar switch, sharing with the similar data storage and file , even with potential attackers. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, etc. Attracts attackers to compromise multiple VMs.

II. LITERATURE SURVEY

A lot of papers were studied and finally the following were shortlisted for careful analysis. The method adopted after the study is briefly sketched out at the end of the chapter.

The paper titled

"Securing cloud computing environment against DDoS attacks"

By

B.Joshi, A. Vijayan, and B. Joshi,

They proposed in their paper that Cloud Computing is the freshly emerged technology of Distributed Computing System. Cloud Computing user concentrate on API security & provide services to its consumers in multitenant environment into three layers namely, Software as a service, Platform as a service and Infrastructure as a service, with the help of web services [3]. It provides service facilities to its consumers on their demand. These service provided can easily invites attacker to attack by Saas,

Paas, and Iaas. Since the resources are gathered at one place in data centers in cloud computing, the DDOS attacks such as HTTP & XML in this environment is dangerous & provides harmful effects and also all consumers will be affected at the same time. These attacks can be resolved & detected by a proposed approach. By that approach, problem can be overcome by using proposed system. The various kinds of vulnerabilities are analyzed in proposed system. The SOAP request makes the connection between the client and the server provider. Through the Service Oriented Trace back Architecture the SOAP request is sended to the cloud. In this architecture service oriented trace back mark is present which contain proxy within it the proxy that marks the incoming packets with source message identification to identify the real client. Then SOAP message is travelled via XDetector. The XDetectors used to monitors and filters the DDoS attacks such as HTTP and XML DDoS attack. Finally the filtered real client message is transferred to the cloud service provider and the corresponding services are given to the client in secured manner.

The paper titled

"Security and privacy challenges in cloud computing environments"

H.Takabi, J. B. Joshi, and G. Ahn

This paper mentioned that Cloud computing has generated significant interest in both academia and industry, but it's still an evolving prototype. Essentially, it goal is to to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pools of computers, networks, and storage resources. Confusion exists in IT communities that how can a cloud differs from existing models and how these differences affect its adoption.

Some see a cloud as a novel technical revolution, while others consider it a natural evolution of technology and economy .

1) 1 Nevertheless, cloud computing is an important prototype, with the potential to significantly reduce costs through optimization and increased operating and economic efficiencies.

2) Furthermore, cloud computing could significantly enhance collaboration, agility, and scale, thus enabling a truly global computing model over the Internet infrastructure. However, without appropriate security and privacy solutions designed for clouds, this potentially revolutionizing computing paradigm could become a huge failure. Several review of potential cloud adopters indicate that security and privacy is the primary concern hindering its adoption.

3) This article illustrates the unique issues of cloud computing that exacerbate safety and privacy challenges in clouds.

4) We also discuss various approaches to address these challenges and explore the future work needed to provide a trustworthy cloud computing environment.

The paper titled

"Detecting Spam Zombies by Monitoring Outgoing Messages"

by

Z.Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker

In this paper they focus on to detect of compromised machines in a network that are used for sending spam messages, which are commonly referred to as spam zombies[6]. Given that spamming provides a critical economic incentive for the controllers of the compromised machines to recruit these machines, it has been nearly observed that many compromised machines are involved in spamming. A number of recent research efforts have studied the aggregate global characteristics of spamming botnets (networks of compromised machines

III. CONCLUSION

The architecture, Efficient Implementation and effectiveness of a testing of group and dual mode mechanism for cloud services are presented. The allotment of Clients to dual mode is based on the requests. The SA (Scenario Attack) algorithm achieves both control of requests and mugger identification.

REFERENCES

1. Coud Sercurity Alliance, "Top threats to cloud computing v1.0,"https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010.

2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D.Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," ACM Commun., vol. 53, no. 4, pp. 50–58, Apr. 2010.

3. 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.

4. 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.

5. G. Gu, J. Zhang, and W. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," Proc. of 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb. 2008.

6."Openflow."http://www.openflow.org/wp/learnmore/, 2012.

7."Citrix XenServer." [Online]. Available: http://www.citrix.com/xenserver.