Providing Flexible Security as a Service Model for Cloud Infrastructure

Dr. M. Newlin Rajkumar, P. Banu Priya, Dr. V. Venkatesakumar

Abstract— **Security-as-a-Service model for cloud systems enable application service providers to deliver their applications via massive cloud computing infrastructures securely. However, due to their sharing nature, storage and service clouds are vulnerable to malicious attacks. In this study, this presents a security architecture that offers a flexible security as a service model that a cloud service provider can offer to its tenants and customers of its tenants. The proposed work provides a novel integrated security with a Virtual Machine analysis scheme that can provide stronger attacker prevention than previous schemes. The proposed security as a service model offers a baseline security to the provider to protect its own cloud infrastructure and also provides flexibility to tenants to have supplementary security utilities that suit their security requirements. This describes the design of the security architecture and deliberates how various types of attacks can be counteracted by the proposed architecture.**

Index Terms—**Security as a Service, Infrastructure, Cloud Environment, Service Models, Tenants, TSAD, SPAD, Cloud Computing, Security.**

I. INTRODUCTION

CLOUD computing [1]–[3] has become an important technology where cloud services providers provide computing resources to their customers (tenants) to host their data or perform their computing tasks. Cloud computing can be categorized into different service deliver models like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Virtualisation [4] is one of the key technologies used in the IaaS cloud infrastructures. For instance, virtualisation is used by some of the major cloud service providers such as Amazon [2] and Microsoft [3] in the provision of cloud services. We will use the term tenant to refer to cloud customers who wish to access services from cloud providers. Tenants can themselves be using their virtual machines to provide services to their own customers; we will refer to customers (or users) as those who use the services of the tenants. Hence customers in our architecture are the customers of the tenants.

In general, the tenants in the cloud can run different operating systems and its applications in their virtual machines. As these operating systems and the applications of the tenants can be potentially large and complex, they may consist of security susceptibilities. Furthermore, there can be several numbers of tenants on the same physical platform sharing resources in a cloud infrastructure. The susceptibilities in the operating systems and applications can be potentially exploited by an attacker to generate various attacks. These attacks can be targeted against the cloud infrastructure as well as against other virtual machines belonging to other tenants. Due to this reason, there is a need to design security architecture and develop techniques that can be used by the cloud service provider for securing its infrastructure and virtual machines of tenants.

However there are several disputes that arise when developing security as a service for cloud infrastructures. In the available present environment, the service providers of cloud do not generally offer security as a service to their tenants. For example, in [5] Amazon mentions that security of tenant virtual machines is the responsibility of the tenants since they are free to run any of the operating systems or applications (though it claims to secure the underlying infrastructure). Hence tenants must make their personal arrangements for securing their virtual machines that are hosted in the cloud. Even though tenants can use various security tools such as anti-virus and host based intrusion detection systems to secure their virtual machines, the limitations arise [6] due to these tools residing in the same system as the one being monitored and hence are susceptible to

ISSN: 2278 – 1323

attacks. Also some tenants may not be efficient enough for securing their tenant virtual machines. Hence there is a necessity for the service provider of cloud to offer security as a service to such tenants.

Furthermore, security requirements for tenants may vary and some tenants may opt for more security services from the cloud provider while others may opt for the baseline default security. For example, a tenant who is running financial services on its virtual machines is likely to need more security measures compared to a tenant who is providing basic web hosting. However, greater the level of security measures taken up by the tenant from the provider, greater is the possibility for the cloud provider to get to know more about the tenant's system. That is, the security mechanisms and tools offered by the cloud provider (as part of its security as a service) can collect more information about the operating system and applications running in the tenant's virtual machines. This may lead to greater privacy concerns for the tenant of cloud. Here privacy concerns refer to the ability of the provider to find details about the services and applications' data in a tenant's machine.

II. RELATED WORKS

The resource management is still performed by the conventional VMM, the compromise of VMM can contribute the operation of the virtual machines. Later some existing systems allocate a separate privileged domain for each tenant. The tenants can use this for the enforcement of VMM based security on their virtual machines. The above model can become more complex as different tenant virtual machines can be hosted on the same physical server. Attacks can lead to increase of load on the tenant virtual machines. Later packet marking techniques have been used. The packet marking techniques helps to trace the attacks in VM.

A. Prior Work

In the previous work there was security architecture which is based on centralized scheme. One of the existing works is CloudVisor, which uses nested virtualization to transact with the compromise of the hypervisor. In the existing technique a secure hypervisor is introduced below the traditional hypervisor and their relationship between the traditional VMM and virtual machines which are monitored by the secure hypervisor.

The major drawback of this existing system is VM can be easily compromised and it is difficult to maintain individual monitoring system. This will increase the communication overhead. A hypervisor or virtual machine monitor (VMM) is a piece of computer software, hardware or firmware that initiates and operate virtual machines. Host Machine is a computer on which a hypervisor is operating one or more virtual machines. Each virtual machine is known as a guest machine.

B. Unified Ontology of Cloud Computing

Progress of research efforts is provisional on having a rigorous organization of its knowledge domain and a complete understanding of all the relevant components of this technology and their association. Cloud Computing is one existing technology in which the research community has recently embarked. The recent evolution of cloud computing has copied its basics from various other computing areas and systems engineering concepts.

C. Virtual Machine Introspection Based Architecture

This article propose a new architecture for building intrusion detection systems that provides good visibility into the state of the proctored host, while still providing strong seclusion for the IDS, thus lending considerable resistance to both evasion and attack. Our approach leverages virtual machine monitor (VMM) technology. This procedure allows us to extract our IDS "outside" of the host it is supervising, into a completely different hardware secured province, affording a high-confidence barrier linking the IDS and an attacker's malicious code. A key part of our conversation is the presentation of Livewire, a prototype VMI-based intrusion detection system that we have fostered and evaluated against a collection of real world attacks. Using Livewire, we instructs that this architecture is a useful and effective means of implementing intrusion detection policies.

ISSN: 2278 – 1323

D. Resource Freeing Attacks

Cloud computing is promises great efficiencies by multiplexing resources among different customers. For eg., Amazon's Elastic Compute Cloud (EC2), Microsoft Azure, Google's Compute Engine, and Rackspace Hosting all provides Infrastructure as a Service (IaaS) solutions that place multiple customer virtual machines (VMs) onto the same physical server. The profited efficiencies have some cost, the past work has shown that the performance of a customer's Virtual Machine can suffer due to interference from another.

E. Security Analysis of Cloud Management Interfaces

Cloud Computing resources are handled through control interfaces. It is by these interfaces that the new machine images can be added, the existing ones can be changed, and instances can be started. Effectively, a successful attack on a Cloud control interface provides the attacker a complete power over the victim's account, with all the stored data included. To view the Cloud control interface security as significant and challenging research topic, additionally marked by its high impact factor for many stakeholders.

III PROPOSED WORK

In Software as a Service (SaaS) model, the client has to rely on the service provider for proper security measures. The service provider must make sure that the multiple users don't get to see each other's information. So, it becomes more important to the user to make sure that right security measures are in place and also very difficult to get an assurance that the application will be available when needed. While using SaaS model, the cloud customer will, by definition, be replacing new software applications for old ones. Therefore, the emphasis is not upon portability of applications, but on conserving or enhancing the security functionality may be provided by the legacy application and achieving a successful data migration.

The SaaS software vendor may host the application on their own private server or may deploy it on a cloud computing infrastructure service provided by a third-party service provider (e.g. Amazon, Google, etc.). The use of cloud computing merged with the 'pay-as-you-go' approach helps the application service provider reduce the investment in infrastructure services and enables it to concentrate on serving better services to the customers. Today enterprises see data and business transactions as strategic and guard them with access control and agreement policies. But, in the SaaS model, enterprise data is stored at the SaaS provider's information center, together with the information of more enterprises. In addition to, if the Software as a Service provider is influencing a public cloud computing service, the enterprise information might be stored along with the data of other irrelevant SaaS applications. The study proposed a security architecture that provides a security as a service model that a cloud provider can offer to its multiple tenants and customers of its tenants. The proposed security as a service model while offering a baseline security to the provider to protect its own cloud infrastructure also provides flexibility to tenants to have additional security functionalities that suit their security requirements. The customized architecture helps the tenant user to select appropriate security service in the cloud environment. The paper described the design of the security architecture and discussed how different types of attacks are counteracted by the proposed architecture. So the system specifies the counter measure techniques to neutralize the impact of attacks.

This proposed work provides fast security thread detection and the appropriate countermeasure helps to recover and prevent the data. The advantage of this proposed system is it reduces the communication overhead and it is easy to deploy.

A. System Architecture

Consider the basic security architecture diagram shown in Fig. 1. The tenants may wish to have their own host based security tools (HBST) to run on the virtual machines that they are obtaining from the cloud provider. Since host based security tools have good visibility into the system being monitored, this acts as a primary layer of defense in our security architecture. The other important components in our security architecture shown in Fig. 1 are the Service Provider Attack Detection (SPAD) and the Tenant

ISSN: 2278 – 1323

Specific Attack Detection (TSAD) components. First let us look the operation of our architecture at a high level. The tenant virtual machine traffic is received by the SPAD component. SPAD enforces the security baseline policies required by the cloud service provider. If a tenant virtual machine's traffic violates any of the security policies in the SPAD, then the tenant virtual machine is isolated and an alert is generated to the tenant administrator and the cloud system administrator. In such cases, the tenant virtual machine can be activated only after the issues are resolved by the tenant administrator and the cloud system administrator.

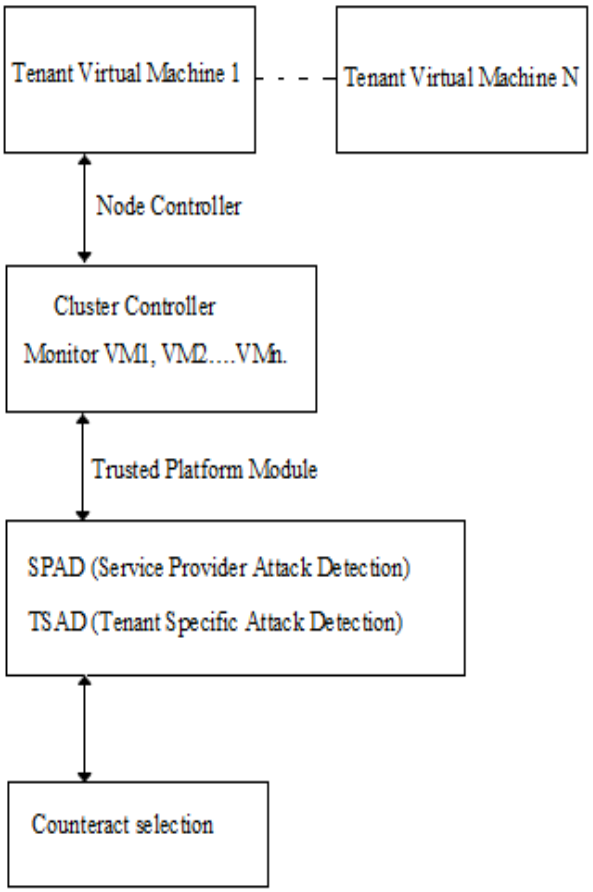

Fig 1: System Architecture

The security policies enforced by the SPAD component are concerned with the detection of spoofed source address and associated attacks. The SPAD component also has policies for logging traffic from tenants. Since the SPAD security policies are enforced on all the tenant virtual machines, they are designed to be lightweight and provide basic security baseline with minimal privacy violations. As the SPAD security mechanisms are needed for secure operation of the cloud provider, we envisage that these services will be offered to the tenant by the provider without any additional charges.

The traffic which is validated by the SPAD component is then forwarded to the actual destination or to the TSAD depending on the tenant's service registration requirements. The traffic is forwarded to the actual destination if the tenant has not requested for any additional security services (apart from the default security baseline) from the cloud provider. If the tenant requires additional security from the cloud provider, then the traffic is forwarded to the TSAD component. The TSAD enforces tenant specific security policies on the tenant traffic. The security policies in the TSAD are decided by the tenants at the time of registration. As tenants' requirements can change, tenants are able to update the security policies in TSAD. However to minimize misuse, policies can be updated with the consent of the cloud provider.

If the traffic does not violate any of the security policies in TSAD then it is forwarded to the actual destination. If the traffic is violating any of the security policies in TSAD, then the traffic is dropped or rate limited according to the tenant requirements. For example, the tenants can specify the policies to drop the traffic if it matches with any of the attack signatures. Alternatively, the policies can be configured to rate limit the traffic in the case of sudden burst traffic. TSAD can also be used for pre-monitoring the traffic destined to the tenant virtual machines. In this case, the incoming traffic is first received by the TSAD. This case is similar to the case in traditional networks where a security gateway such as a firewall monitors all the incoming traffic that is destined to the servers. The tenants are charged additional amounts depending on the overhead of the TSAD security policies.

B. Node Controller

The module contains both the administrator and tenant user authentications. The tenant admin manages the tenant virtual machines that are hosted in the cloud. The tenant users are the customers of the

ISSN: 2278 – 1323

tenant. The admin would have the privilege to view the whole process processed by the tenant user. Once the tenant user registers, tenant user would be able to view only the authenticated page. The personal information and the data which are transferred by the tenant user can be viewed by the tenant user. The login in the secure module is non-dynamic and secure. Once logged in the server would be able to receive the data packets.

C. Connected Network

The network is classified by workgroups. The active and the connected systems over the network are obtained with the use of this module. Once logged in to the process, the module obtains the active systems and displays to the tenant user. The tenant user would be able to choose the system to which the data needs to be transmitted by file transfer.

D. VM Profile and Rule Generation

The VM profile module phase defines the initialization and description of virtual machines in the cloud environment. This VM profile module also defines the influence to access the resources in the cloud. Only the authenticated persons can upload and download the files in virtual machines. For this process VM should enter with all basic information. The Virtual machines in the cloud can be profiled to get precise information about their state, services running and open ports. One major factor that counts toward a VM profile is its connectivity with other VMs. Admin should define with the IP and proper details to initiate the VM. VM profiles are maintained in a database and comprises a comprehensive data about vulnerabilities, alert, and traffic and the data comes from.

E. Security Architecture

The security architecture module brings the complete security as a service model for tenants. This helps to prevent the attack, identify the attack and recover data from attack. This consist of the following process.

- Request processing and packet inspecting
- Alert correlation and Process monitoring
- Counteract process

This module will get the detail about the normal data transfer between the source and destination. Based on the data traffic level it analyses the node link ability and scalability. This process of considering traffic level will improves the data non repudiation as well as data integrity. The module implemented the solution against the problem. Since SPAD validates all the tenant traffic for correct source address, it helps to eliminate Smurf attack and ICMP, UDP, TCP SYN attacks that are produced with spoofed source address.

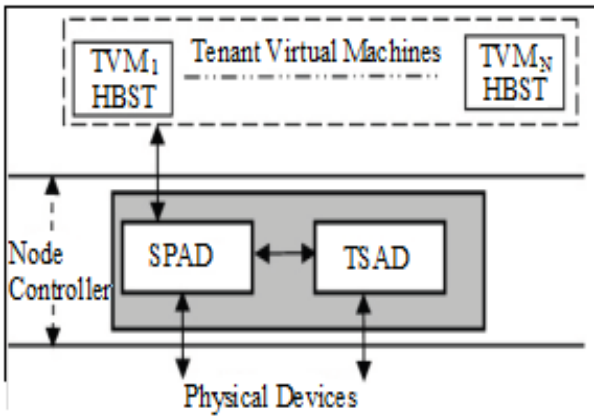

Fig 2: Security Architecture

F. SPAD (Service Provider Attack Detection)

Let us first consider the implementation of the mechanism in SPAD that detects spoofed traffic from the tenant virtual machine. The SPAD module captures network packets from the kernel using iptables in connection with libipq module which is "ip queue kernel module" and validates the source address of the traffic.

SPAD is designed to enforce security policies in the baseline that is offered by the cloud provider. They are intended to minimize the attacks on the cloud provider infrastructure as well as preventing attacks between the tenant virtual machines. Note SPAD policies are enforced on all the tenant virtual machines. In our architecture, the basic SPAD

ISSN: 2278 – 1323

security policies prevent attacks with spoofed source address from the compromised tenant virtual machine and maintain traffic logs originating from the tenant virtual machines for detecting anomalies.

This mechanism in SPAD helps to prevent attacks from the tenant virtual machines with spoofed source addresses. Evenif the attacker was successful in exploiting the vulnerability in the operating system or applications in the tenant machine, the attacker is not successful in generating the attacks with spoofed source address on other cloud tenant virtual machines or on the cloud infrastructure or external hosts on the Internet.

Spoofing is the fundamental challenges which make it more difficult to deal with the attacks in the current environment [14]. Hence one security objective of the SPAD is to ensure that the tenant virtual machine will not send malicious traffic with spoofed traffic to external hosts. This is achieved by the SPAD monitoring all the traffic that is originating from the tenant virtual machines and dropping the traffic with spoofed source addresses. The traffic with correct source address is logged and forwarded to TSAD or actual destination depending on tenant's security requirements.

G. TSAD (Tenant Specific Attack Detection)

TSAD component enforces tenant specific attack detection policies. In the security architecture, the tenant can request the cloud service provider to enforce signature based detection and/or anomaly based detection policies in the TSAD. In our architecture, the tenant can request the cloud service provider to enforce signature based detection and/or anomaly based detection policies in the TSAD. First, the tenant is able to specify application specific attack signatures depending on the applications that are running in its virtual machines. This will vary with the tenant as different tenants can have different applications and services at different times.

Furthermore, greater the information that a tenant is willing to reveal about the applications and services that are running in its virtual machines, more specific security mechanisms can be implemented by the cloud service provider to detect service or application specific attacks. Though this provides a higher level of security, the tenant is revealing more information to the provider and hence potentially its privacy can be reduced.

IV RESULT AND ANALYSIS

By evaluating our proposed system, we have been carrying out many sets of experiments with different types of malware attacks. In this paper, we present performance results with some of these experiments as well as those involving in malware attacks.

Comparison Metrics	Existing	Proposed
Attack	4.3	2.4
Security	4.0	7.0
Time	8.6	5.5

As per theoretical analysis the above table shows the difference between the existing and the proposed techniques. The comparison has been considered with 3 metrics, which are Attacks, Security and Time and achieving a better performances from this approach based on the security thread in the Cloud computing.

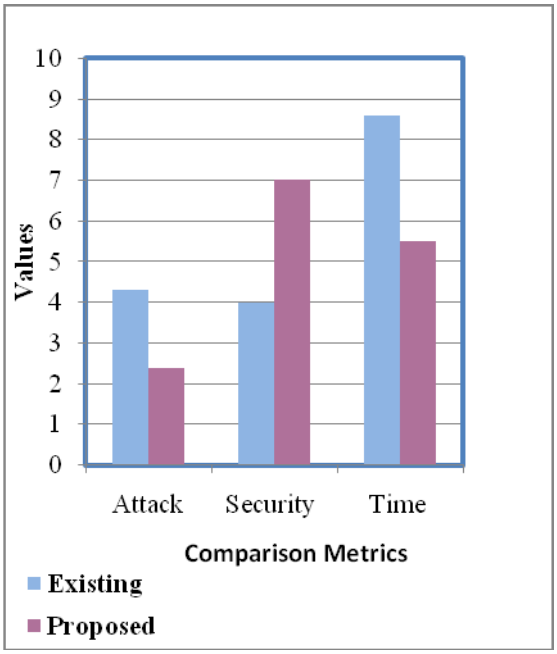

Fig 3: Comparison Chart

ISSN: 2278 – 1323

V CONCLUSION

In this paper we have proposed a security architecture that provides a security as a service model that a cloud provider can offer to its multiple tenants and customers of its tenants. This security as a service model offers a baseline security to the provider to protect its own cloud infrastructure also provides flexibility to tenants to have additional security functionalities that suit their security requirements. The paper described the design of the security architecture and discussed how different types of attacks are counteracted by the proposed architecture. We have described the implementation of the security architecture and gave a detailed analysis of the security mechanisms and performance evaluation results.

REFERENCES

[1] L. Youseff, M. Butrico, and D. Da Silva, "Towards a unified ontology of cloud computing," in Proc. 2008 Grid Computing Environments Workshop.
[2] Amazon Inc., "Amazon elastic compute cloud (Amazon EC2)," 2011. Available: http://aws.amazon.com/ec2/
[3] "Windows Azure." Available: http://www.windowsazure.com/en-us/
[4] J. E. Smith and R. Nair, "The architecture of virtual machines," IEEE Internet Comput., May 2005.
[5] "AWS security center." Available: http://aws.amazon.com/security/
[6] T. Garfinkel and M. Rosenblum, "A virtual machine introspection based architecture for intrusion detection," in Proc. 2003 Netw.Distrib.Syst. Security Symp.
[7] T. Garfinkel and M. Rosenblum, "A virtual machine introspection based architecture for intrusion detection," in Proc. 2003 Netw.Distrib.Syst. Security Symp.
[8] V. Varadarajan, et al., "Resource-freeing attacks: improve your cloud performance (at your neighbor's expense)," in Proc. 2012 ACM Comput. Commun.Security Conf.
[9] J. Somorovsky, et al., "All your clouds belong to us—security analysis of cloud management interfaces," in 2011 ACM Comput.Commun.Security Conf.
[10] P. Barham, et al., "Xen and the art of virtualization," in Proc. 2003 ACM Symp.Operating Syst. Principles.
[11] Y. Zhang, et al., "Cross-VM side channels and their use to extract private keys," in 2012 ACM Comput.Commun.Security Conf.
[12] J. Idziorek, M. F. Tannian, and D. Jacobson, "The insecurity of cloud utility models," IEEE Cloud Comput., pp. 14–18, May–June 2013.
[13] R. Beverly, R. Koga, and K. C Claffy, "Initial longitudinal analysis of IP source spoofing capability on the Internet," July 2013. Available: http://www.internetsociety.org/doc/initiallongitudinal-analysis-ipsource-spoofing-capability-internet
[14] B. Balacheff, et al., Trusted Computing Platforms — TCPA Technology in Context. Hewlett-Packard Books, 2003.

Authors

Dr. M. Newlin Rajkumar is presently working as Assistant Professor in The Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Engineering Degree from Bharathiyar University, Master of Science (M.S by Research) from National ChiaoTuns University, Taiwan and Master of Business Administration (IBM) from Anna University, Coimbatore. He has completed his Ph.D in Anna University Chennai. He has more than ten years of Teaching Experience. He has published several papers in reputed International Journals. He is a Professional Member of ACM, Member of IEEE India Council, Life Member of International Association of Computer Science and Information Technology, International Association of Engineers and in many International Associations. His research interest includes cloud Computing, Internet of Things, Big Data Analytics, Network Security, Security Protocols and Network Management.
Contact Number – 9952153334

P. Banu Priya is pursing M.E Computer Science and Engineering (Specialization with Networks) in the Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. She received her Bachelor of Engineering Degree from Anna University Chennai. Her research interests are Cloud Computing, Network Security and Cloud Security.
Contact Number – 8678988054

Dr. V. Venkatesakumar is presently working as Assistant Professor in The Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Engineering Degree from Bharathiyar University, Master of Engineering Degree and Ph.D from Anna University Chennai. He has more than ten years of Teaching Experience. He has published many papers in reputed International Journals and has Chaired many Conferences. He is a Life Member of International Association of Computer Science and Information Technology, International Association of Engineers and in many International Associations. His research interest includes Cloud Computing, Internet of Things, Big Data Analytics, Operating System, Software Engineering and Web Technologies.
Contact Number – 9600930799

ISSN: 2278 – 1323