International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Security Service Model for Cloud Environment

Shafali Gupta[1], Neha R Gedam[2]

[1]Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

[2]Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

Abstract: ***Cloud computing is becoming increasingly important for provision of services and storage of data in the Internet. However there are several significant challenges in securing cloud infrastructures from different types of attacks. The focus of this paper is on the security services that a cloud provider can offer as part of its infrastructure to its customers (tenants) to counteract these attacks. We have to describes the design of the security architecture and discusses how different types of attacks are counteracted by the proposed architecture.***

Keywords: Cloud security, security architecture, security issues and privacy

1. Introduction

Cloud computing 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 such as Software as a Service (Saabs), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Virtualization [4] is one of the key technologies used in the IaaS cloud infrastructures. For instance, virtualization 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 applications in their virtual machines .As the operating systems and applications of the tenants can be potentially large and complex, they may contain security vulnerabilities .Furthermore, there can be several tenants on the same physical platform sharing resources in a cloud infrastructure. The vulnerabilities in operating systems and applications can be potentially exploited by an attacker to generate different types of attacks. These attacks can be targeted against the cloud infrastructure as well as against other virtual machines belonging to other tenants. So 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 tenant virtual machines. Our main contribution in this paper is a security architecture that provides a flexible security as a service model that a cloud provider can offer to its tenants and customers of its tenants.

2. Security Architecture

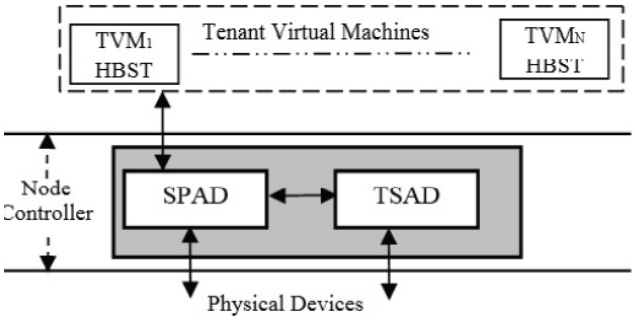


Figure 1: Basic Security Architecture

Our security architecture assumes that the cloud service provider provides a trusted VMM platform (for example, equipped with Trusted Platform Module (TPM)[5]). We also assume that the security components of our architecture embedded within the VMM are trusted. The cloud provider also provides controls and auditing procedures which ensure the physical security of the cloud infrastructure to overcome hardware based attacks such as cold-boot attacks on its privacy concerns. Our security architecture protects the cloud infrastructure from attacks generated within a tenant virtual machine by the tenant administrator and tenant users. It also protects co-located tenants from the attacks generated by such tenant entities. In our architecture, the baseline security mechanisms. Our security architecture also protects tenants from threat posed by cloud system administrators who misuse their privileges and exploits against privileged domain Our security architecture also provides mechanisms to deal with some attacks on the VMM. This is done using a Security Gateway component which specifies cluster wide policies and mechanisms to detect attacks on the VMM platforms. Finally our security architecture provides the ability to charge a tenant depending on the security services that are The security architecture proposed in this paper focus mainly on the infrastructure-as-a-service (IaaS) platform. Consider the basic security architecture diagram shown in Fig..As mentioned above, 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. the Service Provider Attack Detection (SPAD) and the Tenant 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. The security policies enforced by the SPAD component are concerned with the detection of spoofed source address and 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 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.

3. Proposed Work

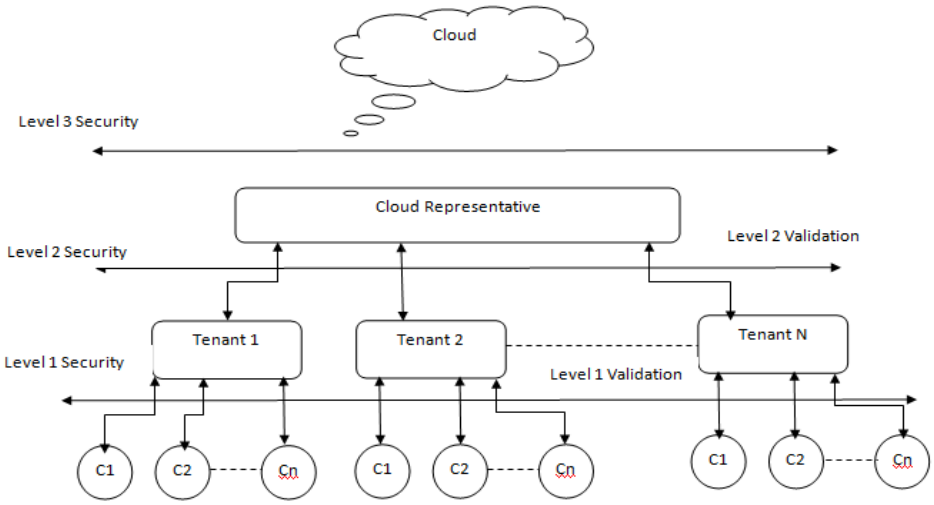
The proposed statement of the system is to propose a security architecture that provides a security as a service model that a cloud provider can offer to its multiple tenants and customers of its tenants. Our security as a service model while offering a baseline security to the provider to protect its own cloud infrastructure also provides flexibility to tenants to have additional security functionalities that suit their security requirements. The 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

4. Proposed Architecture

In order to provide customers with secure storage, three level security approach is proposed. A cloud representative, Tenant and its client are three levels of security. Client of tenant was not able to access any data or file directly such that without permission of tenant. At each level. Authentication was performed. Only authorized client and tenant can get access to data or file stored at cloud. As per concept of encapsulation, cloud infrastructure was hidden from tenant and client. A cloud representative will communicate with tenant and client and also authentication was performed at each stage. This not only rules out the possibility of a CSP misusing the customers' data, breaching the privacy of data, but also avoids vendor lock-in.

Following figure shows system architecture;

Architecture Diagram



5. 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. Our 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 paper described the design of the security architecture and discussed how different types of attacks are counteracted by the proposed architecture.

6. Acknowledgement

We would like to thank the principal and staff members of RMD Sinhgad School of Engineering, University of Pune, friends and family members for their support their valuable reviews and support to bring this article.

References

[1] L. Youseff, M. Butrico, and D. Da Silva,"Towards a unified ontology of cloud computing," in Proc2008 Grid Computing EnvironmentsWorkshop

[2] Amazon Inc., "Amazon elasticomputecloud (Amazon EC2)," 2011.Availablehttp://aws.amazon.com/ec2
[3] "Windows Azure." Available:
[4] J. E. Smith and R. Nair, "The architecture of virtual machines,"IEEE InternetComput., May 2005.
[5] B. Balacheff, et al., Trusted Computing Platforms — TCPA Techonology in Context. Hewlett-Packard Books.
[6] "VMescape."Available:http://www.zdnet.com/blog/security
[7] "Xen security advisory 19 (CVE-2012-4411)–guest administrator access QEMU monitor console."
[8] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security Privacy,

Author Profile

Shafali Gupta, Professor, Department of Computer Engineering RMD Sinhgad School of Engineering, University of Pune, India

Neha Gedam, Research Scholar RMD Sinhgad School of Engineering Warje, Pune, University of Pune