Software as a Model for Security in Cloud over Virtual Environments

S.Vengadesan, B.Muthulakshmi

PG Student, Department of Computer Science and Engineering, A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu, India.
vengad60@gmail.com

Assistant Professor, Department of Computer Science and Engineering, A.V.C. College of Engineering, Mayiladuthurai, Tamil Nadu, India.
kavithakamalan@gmail.com

Abstract: Cloud computing is becoming increasingly important for provision of services and storage of data in the Internet. An effective firewall security has been implemented for blocking and filtering the unwanted requests coming from the clients before the request approach to the virtual machine. Security issues in cloud concerns and mainly associated with security issue faced by cloud service providers and the service issues faced by customers. Security issues in cloud concerns and mainly associated with security issues faced by cloud service providers and the service issues faced by the cloud customers. In the proposed system, an effective firewall security has been implemented for blocking and filtering the unwanted requests coming from the clients before the request approach the virtual machine. However there are several significant challenges in securing cloud infrastructures from different types of attacks. Our main contribution 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. 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.

Keywords- Cloud security, security architecture, security and privacy.

1 INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

The five essential characteristics are as follows:

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Location independence
- Rapid elasticity
- Measured service

The service models are as follows:

Cloud Software as a Service (SAAS) is a use of provider's applications over a network. Cloud Platform as a Service (PAAS) is the deploy customer-created applications to a cloud. Cloud Infrastructure as a Service (IAAS) is a rent processing, storage, network capacity, and other fundamental computing resources.
The deployment models, which can be either internally or externally implemented, are summarized in the NIST presentation as follows:

Private Cloud: Enterprise owned or leased.
Community Cloud: Shared infrastructure for specific community.
Public Cloud: Sold to the public, mega-scale infrastructure.

Hybrid Cloud: Composition of two or more clouds.

2 BACKGROUNDS

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 (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Virtualization 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 and Microsoft 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. 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. However there are several issues that arise when developing security as a service for cloud infrastructures. In the current environment, the cloud service providers do not generally offer security as a service to their tenants. For example, in 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. Hence tenants need to make their own arrangements for securing their virtual machines that are hosted in the cloud. Although tenants can use different security tools such as anti-virus and host based intrusion detection systems to secure their virtual machines, the limitations arise due to these tools residing in the same system as the one being monitored and hence are vulnerable to attacks. Also some tenants may not be capable of securing their tenant virtual machines. Hence there is a need for the cloud service provider 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 gather more information about the operating system and applications running in the tenant's virtual machines. This in turn may lead to greater privacy concerns for the tenant. Here privacy concerns refer to the ability of the provider to find details about the services and applications' data in a tenant's machine. 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. 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 determine how much control they wish to have over their own virtual machines. The baseline security is needed by the provider to ensure that malicious tenants are not attacking the cloud infrastructure or even hosting malicious software. Every tenant has to have the security functionalities that forms part of the security baseline, which offers basic security guarantees in its default mode of operation. Hence our security as a service model provides options to have additional security functionalities that suit tenants' security requirements. These additional security functionalities can require the tenant to reveal more information about its services and applications, which may create privacy concerns for the tenant. Our approach offers a choice to the tenant to managing this tension between the privacy concerns and the security controls offered by the cloud provider. An important feature of our model is that it makes this trade-off between security and privacy explicit. Furthermore, the choice by a tenant to opt in for additional security services can provide the cloud provider to develop a framework for charging the tenants for these additional security services. The threat model is considering the different types of attackers and attacks that can occur in the infrastructure as a service cloud environment. Then we summarize the capabilities of the security architecture that is proposed in this paper. It describes the design of the security architecture and discusses how different types of attacks are counteracted by the proposed architecture.

3 EXISTING SYSTEM WORK

- In the existing system, providing security in cloud option is a huge amount of pay, based on the service of usage by the customers in cloud environment.
- The extensive use of virtualization in implementing cloud environment brings unique security providence for the cloud customers and all other reseller's & subscribers of a public cloud service access.
- The request raised by client to the cloud server by stopping unwanted request by firewall.
- The unwanted request will be stored in virtual machine not raised to cloud server.

Disadvantages

1. Unauthorized users can able to access cloud data, which is the major drawback.

2. High payable cloud charges.

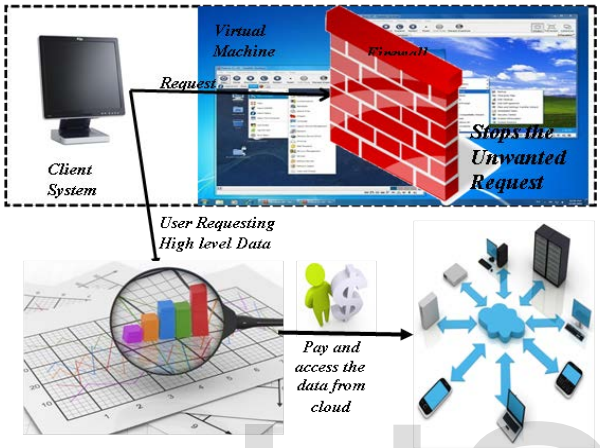
4 PROPOSED SYSTEM WORK

- In the proposed system, an effective firewall security has been implemented for blocking and filtering the unwanted requests coming from the clients before the request approach the virtual machine.
- During the request processing, if the user requests the high level of data from the cloud, then based on the payment made by the cloud user, they can use and access the data's from the cloud server.
- The MAC (Media Access Control) address, IP address and system information will be blogged If an unauthorized or unsolicited person trying to access.
- Fast computing
- Highly authenticated user only can access the information.
- The users have to pay if the user wants high level data.

Advantages

1. Virtual firewall provides enhanced level of security in user level access.
2. Highly authorized user alone able to access.

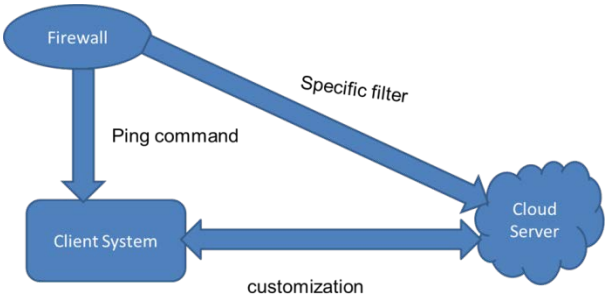
5 ARCHITECHTURE DIAGRAM



6 IMPLEMENTATION MODULES

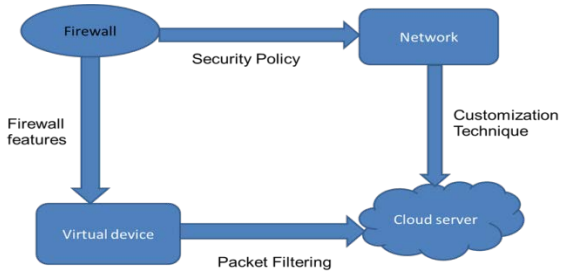
6.1 FIREWALL CREATION MODULE

A Firewall is a system designed to prevent unauthorized access to or from a private network (especially Intranets). Create a firewall rule that permits the ping command first and customize the implementing type. Using this rule to deploy all windows server and create a specific filter. Using this rule to verify the remote servers and work stations along with ping configurations.



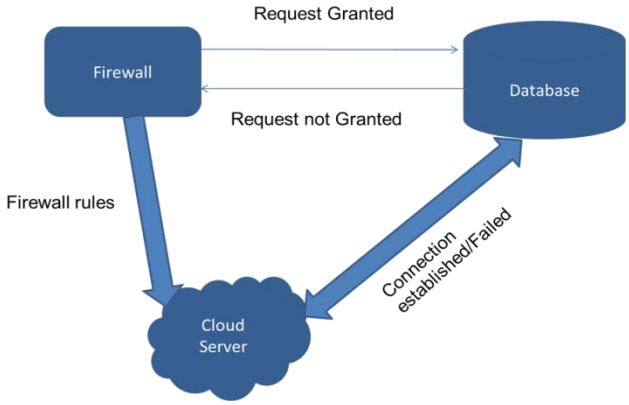
6.2 VIRTUALIZED FIREWALL CREATION MODULE

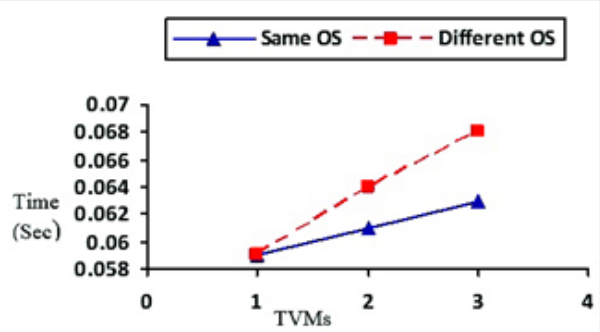
A firewall product is required to support virtual devices in most of its firewall features. In network configured zones, not necessary to configure security policy for each interface in a firewall network. Create resource based packet filtering within same virtual device to remove zones in a network. RBPF in different virtual devices are also access.

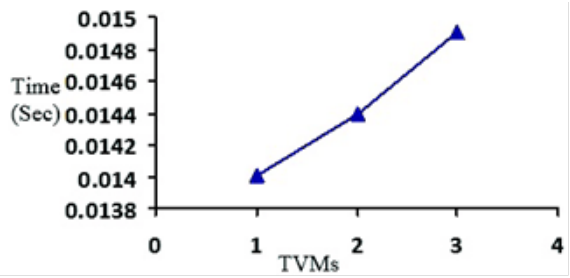


6.3 DATA ACCESS MODULE

If the IP address of request is within one of the ranges specified in server level firewall rules, the connection is granted to SQL Database server has a matching database-level rule. If the IP address request is not within the ranges specified in server level firewall rules mean, connection failed otherwise database firewall rules are checked. The connection established only when the client passes through firewall in SQL database.

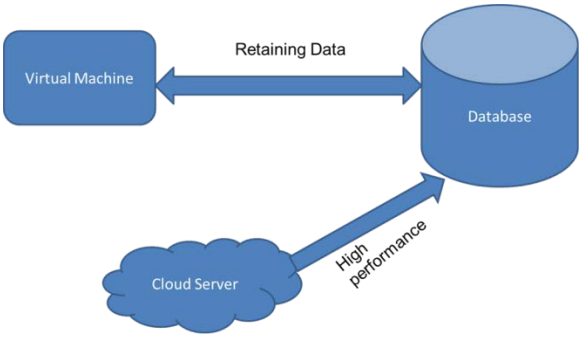






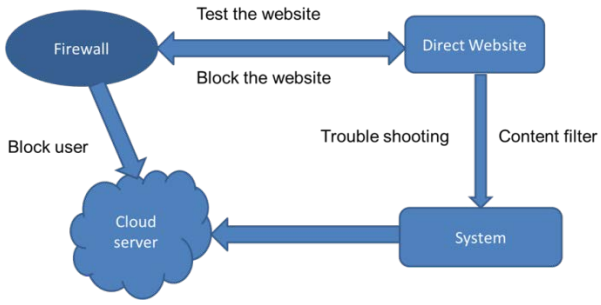
6.4 COST COMPUTATION MODULE

Flexible cloud hosting services, reliable and secure information all those involved in cost computation. It produces very low rate for the compute capacity is actually consuming and produce high performance over data. Having route access to each one and interact with machine, retaining data based on boot partition also added an advantage.



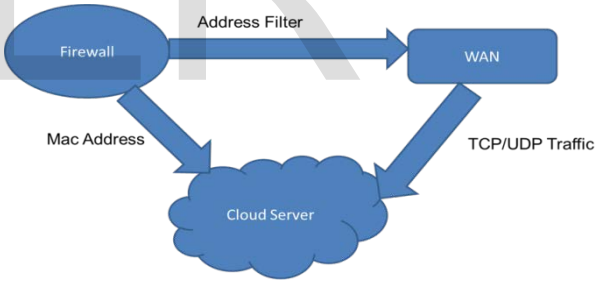
6.5 BLOCKED USER MODULE

Firewall that allows to blocking programs from being accessed by other people on the internet or network. It helps to keep computer secure. Testing a blocking rule, this rule used to test the website and block the website by network administrator. To create a content filter to block user access in group of websites in a network. Troubleshooting the block page to avoid unauthorized person using a network.



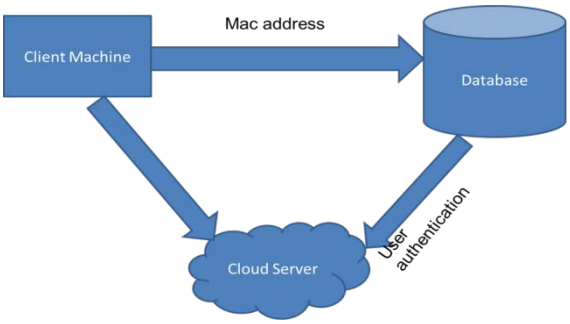
6.6 MAC PRIVILEGE MODULE

Mac address is a unique address assigned to almost all networking hardware's (ex: Mobile phones). Creating firewall rules based on Mac address this also very effective while accessing system from cloud server. It Address filters to prevent devices from sending outgoing TCP/UDP traffic to the WAN.



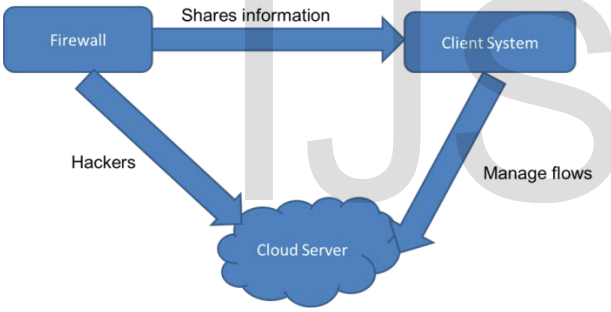
6.7 SYSTEM INFORMATION MODULE

Mostly to check whether the person is authenticated user or unauthenticated user in a database while access the information in cloud server. Authenticated user information is stored in database this helps to make a user to access the cloud server. And, system information (IP address, Mac address) are also checked in a database to allow the user to utilize the system.



6.8 PERFORMANCE EVALUATION

Adoption of cloud, virtualization and mobility providing more vulnerabilities than ever for hackers to exploit. Now a day, Firewall performance based on shares and information about applications, attack signatures and address is increased. Firewall needs to manage flows between tiers of virtualized servers to increase the performance in a line-server.



7 CONCLUSION

A Cloud service discovery system specially designed for users for finding Cloud service over the internet is provided. Cloud ontology is also introduced for enhancing performance of the CSDS. The contributions of this work include: 1) building of the Cloud service discovery system and 2) constructing the Cloud ontology. It is the first attempt in building an agent-based discovery system that consults ontology when retrieving information about Cloud services. In future when the Cloud computing is more commonly and widely used, it can be helpful for Cloud users to find a Cloud service under their specific preference. By consulting a Cloud ontology to reason about the relations among Cloud services, the CSDS is more successful in locating Cloud services and more likely to discover Cloud services that meets consumer requirements. The Cloud service discovery system is enhanced by, making more depth of the Cloud ontology so that it can make more difference between two services in terms of service utility, completing functionalities of query processing, filtering and rating.

REFERENCES

[1] T. C. Chieu, *et al.*, "Dynamic scaling of web applications in a virtualized cloud computing environment," in *Proc. 2009 IEEE Int. Conf. e-Business Eng.*

[2] K. Beaty, *et al.*, "Network-level access control management for the cloud," in *Proc. 2013 IEEE Int. Conf. Cloud Eng.*

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

[4] J. Idziorek, M. F. Tannian, and D. Jacobson, "The insecurity of cloud utility models," *IEEE Cloud Comput.*, pp. 14–18, May–June 2013.

[5] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," *ACM/IEEE Trans. Network.*, vol. 9, no. 3, pp. 226–237, June 2001.

[6] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy, *8*(6), 24-31.

[7] Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidis, J., Paxson, V., & Shenker, S. (2002). Controlling high bandwidth aggregates in the network. ACM SIGCOMM Computer Communication Review, 32(3), 62-73.

[8] S. Butt, et al., —Self-service cloud computing,‖ in Proc. 2012 ACM Computer Communication Security Conf.
[9] T. C. Chieu, et al., —Dynamic scaling of web applications in a virtualized cloud computing environment,‖ in Proc. 2009 IEEE Int. Conf. e-Business Eng.
[10] S. T. Jones, et al., —VMM-based hidden process detection and identification are usingclosed,‖ in Proc. 2008 ACM Virtual Execution Environments.
[11] K. Beaty, et al., —Network-level access control management for the cloud,‖ in Proc. 2013 IEEE Int. Conf. Cloud Eng.
[12] J. Somorovsky, et al., —All your clouds belong to us security analysis ofcloud management interfaces,‖ in 2011 ACM Compute. Communication Security Conf.
[13]P. Barham, et al., —Xen and the art of virtualization,‖ in Proc. 2003 ACM Symp. Operating Syst. Principles.