International Journal of Advanced Information In Engineering and Technology ISSN: 2454 – 6933
Vol.5, no.7, July 2018

Security in Cloud over the Virtual Environment

Dr. B. Jayachandran
Professor
Department of Electronics and Communication Engineering
E.G.S. Pillay Engineering College
Nagapattinam

Abstract— 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 existing system, providing security in cloud opt 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 & subscriber's of a public cloud service access. 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.

Index Terms—Firewall, Virtualization, Cloud Provider, Authentication, Tenants, MAC address blocking, IP address blocking, security.

1. 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 such as 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 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.

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 [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 applications1 (though it claims to secure the underlying infrastructure). 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 [6] 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.

2. SYSTEM ARCHITECTURE

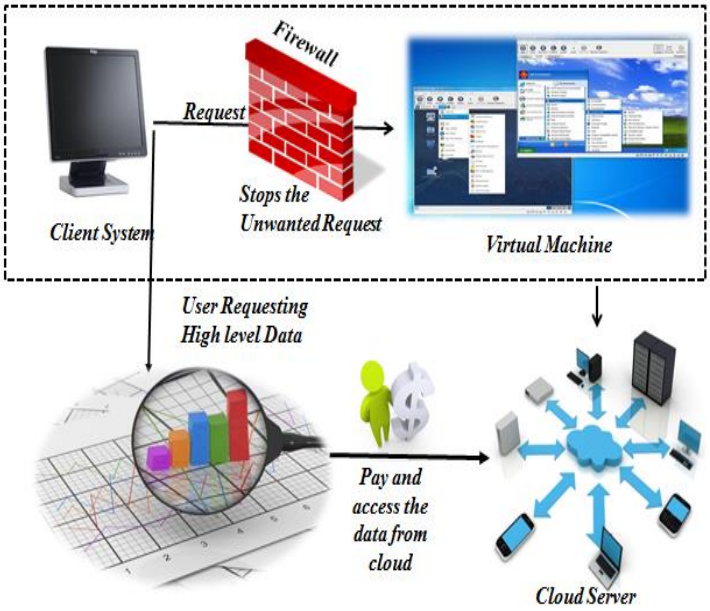

Fig 1.System Architecture

The architecture of the firewall helps to block unwanted request by analyzing and blocking it. The MAC(media access control) address , IP address and system information will be blocked If an unauthorized or unsolicited person trying to access.This provides high level security to the data in the cloud. In the existing system, providing security in cloud opt 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. 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 server.When the client some data to the server it first goes to the firewall, this analyses the type of data if it is an authorised request the firewall request the data to the server. Firewall is created specific to the user needs and this enables fast computing.

3. RELATED WORKS

3.1 Firewall Creation Module

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

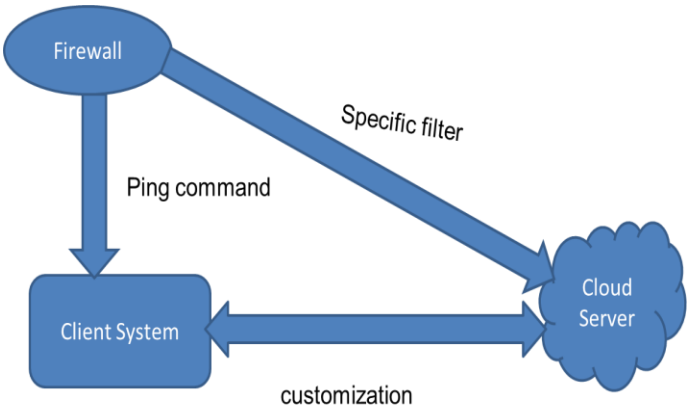

Fig 2. Firewall Creation Module

3.2 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. Resource based packet filtering is created within same virtual device to remove zones in a network. RBPF in different virtual devices are also accepted.

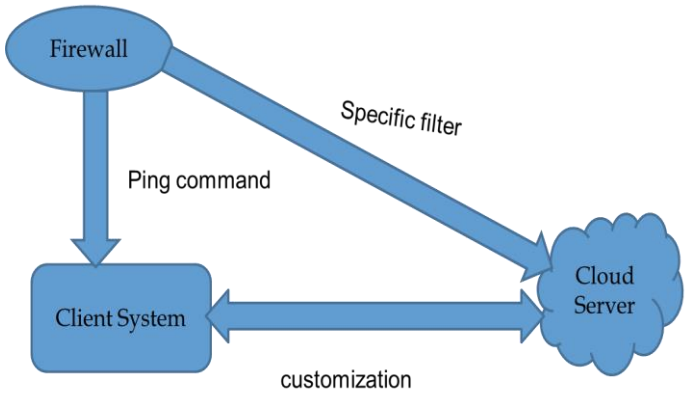

Fig 3. Virtualized Firewall Creation Module

3.3 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.

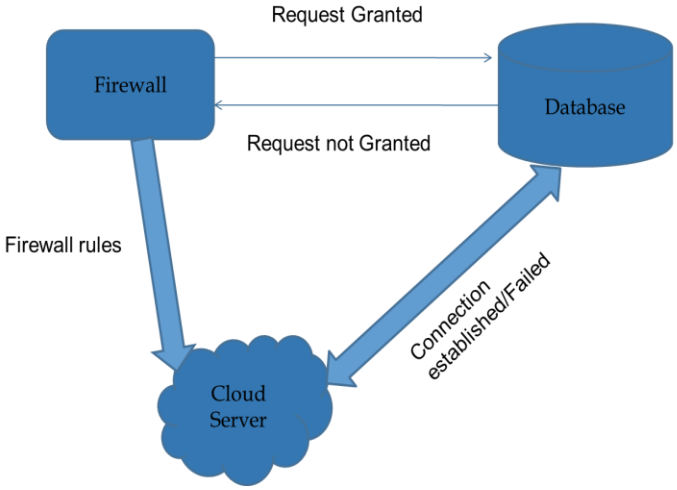

Fig 4.Data Access Module

3.4 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 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.

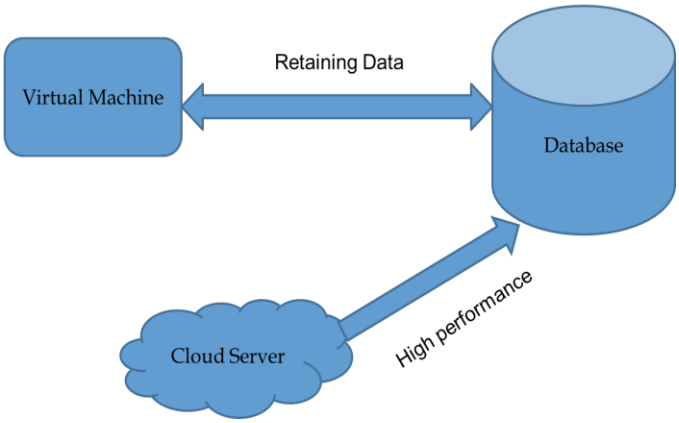

Fig 5. Cost Computation Module

3.5 Blocked User Access Module

Firewal allows to block 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. A content filter is created to block user access in group of websites in a network.

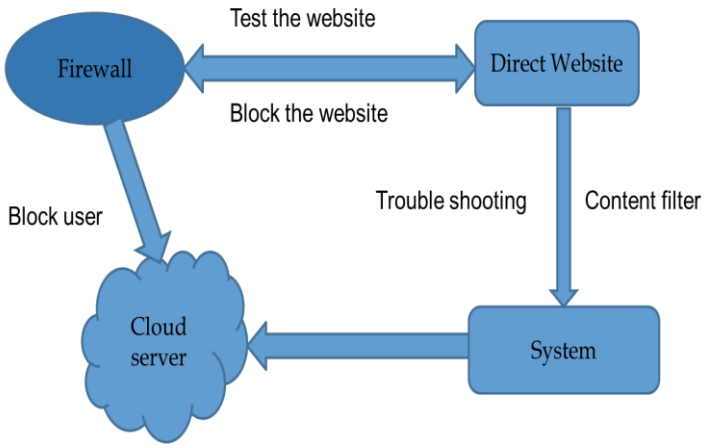

Fig 6. Blocked User Access Module

3.6 MAC Priveledge 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 addresses filters to pre-

vent devices from sending outgoing TCP/UDP traffic to the WAN.

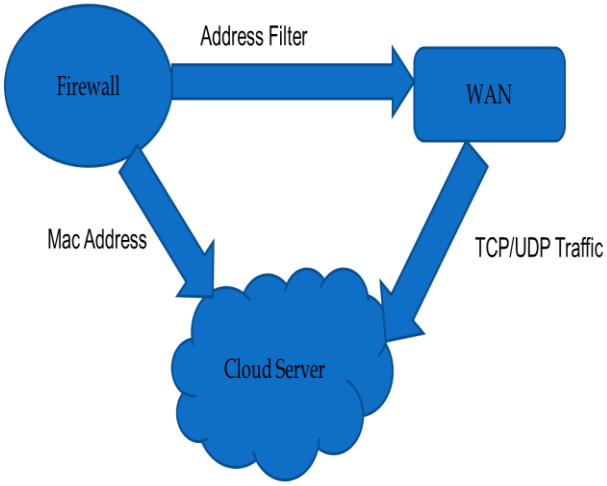

Fig 7. MAC Information

3.7 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.

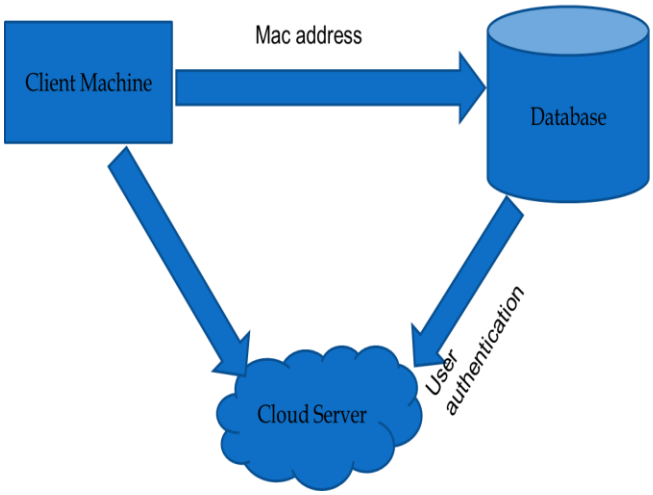

Fig 8.System Information Module

3.8 Performance Evaluation Module

Adoption of cloud, virtualization and mobility provide more vulnerabilities than ever for hackers to exploit. Now a days, Firewall performance is 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.

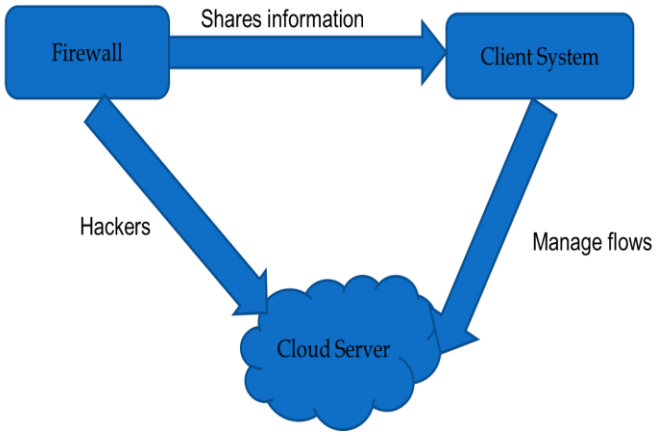

Fig 9. Performance Evaluation Module

4. Conclusion

The firewall is created which gives greater security by blocking the unwanted request from the client side. The extensive use of virtualization in implementing cloud environment brings unique security providence for the cloud customers. 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.

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] S. Bahram, *et al.*, "DKSM: subverting virtual machine introspection for fun and profit," in *Proc. 2010 IEEE Symp. Reliable Distrib. Syst.*

[8] J. Pfoh, C. Schneider, and C. Eckert, "Exploiting the x86 architecture to derive virtual machine state information," in *Proc. 2010 Int. Conf. Emerging Security Inf., Syst. Technol.*

[9] F. Zhang, *et al.*, "CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization," in *Proc. 2011 Symp. Operating Syst. Principles.*

[10] C. Yu, *et al.*, "Protecting the security and privacy of the virtual machine through privilege separation," in *Proc. 2013 Int. Conf. Comput. Sci. Electron. Eng.*

[11] L. Zhou, V. Varadharajan, and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud," *Comput. J.*, vol. 54 , no. 10, pp. 1675–1687, 2011.

[12] *eXtensible Access Control Markup Language (XACML), Version 3.0*, OASIS Standard, Jan. 22, 2013.

[13] Y. Zhang, *et al.*, "Cross-VM side channels and their use to extract private keys," in *2012 ACM Comput. Commun. Security Conf.*

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

[15] 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/initial-longitudinal-analysis-ipsource spoof-ing-capability-internet