ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 3 (July - Sept. 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Integrated Security Architecture for Multitenant Environment of Public Cloud

Suresh Mohan
Research Scholar, School of CSE, Vellore Institute of Technology University, Vellore, India

Abstract
This paper is the product of investigation on the security issues that are faced in this multi-tenant model of cloud. The paper is analyzed from the perspectives of the provider of the cloud and the consumer of the cloud. We initially discuss various common models of cloud computing used present day. Later we discuss the various security issues in multi-tenant model of cloud. We propose an Integrated Security Architecture across the OSI layers which establishes a high security over the Cloud Multi-tenant Environment.

Keywords
Multitenant, public cloud, security

I. Introduction

The computer industry is rapidly growing over the past 2 decades. In recent past, the industry is totally eclipsed by cloud. Cloud is growing to be everywhere in the industry. The technology has grown rapidly and the cost of almost all of the computer components has reduced drastically. From simple to mouse to complex processors, cost of everything is coming down. But at the same time, the power of all such components has increased manifolds. This has led into a new era of cloud computing.
Internet is the backbone of cloud. We can use the resources for a specific time and release it for others to use it for a small cost. This is the tip of the cloud iceberg. NIST defines cloud computing as [1] "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

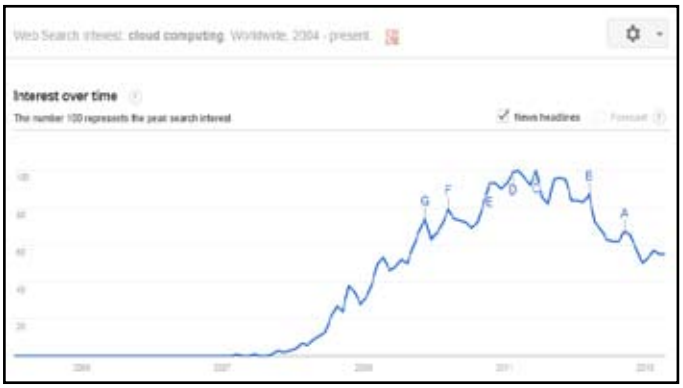

Fig. 1: Web Search Interest of Cloud Computing

Google trends are used as one of the measurement tool for the technology trends among the computing analysts. The figure below can be used to analyze the popularity of the term "cloud computing" in Google website during the period of 2004 till 2013.
As the Google trend depicts, we can see that until 2007 the term was used very low. Around 2008 it started to gain popularity and it was at its peak during 2011 and early 2012. And it can also be seen that the trend has not come down but still maintains at a high level. This makes it to say that the industry and the technologists have been driven towards cloud computing and the trend is still on.
Cloud has many characteristics out of which elasticity and multi-tenancy are the most important characters as we see. Multi tenancy in cloud computing is an architecture in which server space can be shared by many customers. Here the customers are referred as tenants. This is very cost effective way of providing service. In single tenancy, each customer is provided with separate instance. Tenants may also have some customizable features in the application. In recent times, the multi tenancy is also referred with remote access and virtualization architectures.
This paper analyzes the security problems that are in cloud computing and in specific multi tenancy architecture. The issues are categorized according to the impact it makes in the Multi tenancy architecture. The objective is to identify the issues in the model and suggest a possible fix to these issues.

II. Literature Review

Cloud computing issues are been discussed by many researchers. These researchers consider that this is a pressing problem and still clarity is not identified in the cloud technologies. Mohamed Al Morsy et al analyze the cloud computing security problems. Mohamed specifies that many of the issues are inherited from the SOA architecture. Kresimir et al discusses high level security concerns in the cloud computing model such as payment, data integrity and privacy of Information. Kresimir discussed different security model standards such as ITIL, ISO/IEC 27001 and Open Virtualization Format (OVF). Ilango Sriram and Ali Khajeh discusses about various aspects of cloud computing, cloud types and different issues related to it. They have also specified Research agenda in Cloud. Qi Zhang et al have documented a section in the Journal published by The Brazilian Computer Society in 2010. In this they have discusses about cloud computing and the research challenges associated with it.

III. Cloud computing introduction

Cloud computing ('cloud') is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates the information and application resources from the underlying infrastructure and its mechanisms used to deliver it.
Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption [2].

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

There are many definitions today which attempt to address cloud from the perspective of academicians, architects, engineers and consumers. This document focuses on a definition that is specifically tailored to the unique perspectives of IT network and security professionals.

The keys to understanding how cloud architecture impacts security architecture are a common and concise lexicon, coupled with a consistent taxonomy of offerings by which cloud services and architecture can be deconstructed, mapped to a model of compensating security and operational controls, risk assessment and management frameworks, and in turn to compliance standards.

IV. Service models in cloud

Cloud can be categorized according to the service model it offers. The cloud is strongly focused towards Service orientation. Instead of offering a packaged solution, cloud computing offers solutions as a service. So here the end users are saved from investing in large scale systems, servers etc. More over this model is best suitable for those users who want the resources as a one-time requirement. Cloud Services can be classified in to three types. Software as a Service, Platform as a Service and Infrastructure as a Service. Salesforce.com is an example of Software as a service. Google App Engine is an example of Platform as a Service. Amazon Elastic Compute Cloud (EC2) is an example for Infrastructure as a service. Even though we are trying to classify the cloud in to the three types. Most of the Cloud facilities do not fit exactly into these categories. The exact line of difference between these types is blurred. We can consider that the Software as a Service is highly optimized but less flexible. In case of Infrastructure as a Service, it will have high flexibility but less optimization. Platform as a service falls in the mid-way between these two models.

In the Cloud Computing the different models can be ordered as shown in the below figure.

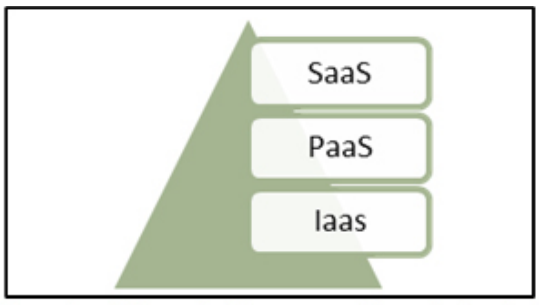

Fig. 2: Cloud Computing Models

In this the Software as a Service shall form the top of the hierarchy. In SaaS an application or software is hosted as a service to the users. At the highest level of the hierarchy, the application layer consists of the actual cloud applications. Compared to the traditional server hosting, the architecture of the cloud is more modular. Each layer has loose coupling with the other layers. This helps the other layers to evolve without changing the other layer.

In Platform as a service layer, the development environments are offered. This layer is capable of hosting cloud ready applications. This layer has dynamic scaling capabilities so that it can grow whenever required. This layer typically consists of operating systems and application frameworks. This layer reduces the burden of deploying the application.

The Infrastructure as a service layer is responsible for managing the physical resources of the cloud, including the physical servers, routers, etc. Rather than buying and owning the infrastructure, clients can buy these resources fully outsourced services. Clients pay only for the resources they consume.

V. Cloud computing characteristics

Cloud computing provides many salient features that are different from traditional service computing, which we summarize below.

A. Multi-tenancy

In a cloud environment, services owned by multiple providers are co-located in a single data center. The performance and management issues of these services are shared among service providers and the infrastructure provider. The layered architecture of cloud computing provides a natural division of responsibilities: the owner of each layer only needs to focus on the specific objectives associated with this layer. However, multi-tenancy also brings difficulties in understanding and managing various stakeholders.

B. Shared Resource Pooling

The infrastructure provider offers a pool of computing resources that can be dynamically assigned to multiple resource consumers. Such dynamic resource assignment capability provides much flexibility to infrastructure providers for managing their own resource usage and operating costs. For example, an IaaS provider shall leverage Virtual Machine migration technology to attain a high degree of server consolidation, thereby maximizing the resource utilization while minimizing cost such as power consumption and cooling.

C. Geo-distribution and ubiquitous network access

Clouds are generally accessible through the Internet and use the Internet as a service delivery network. Hence any device with Internet connectivity like mobile phone, PDA or laptop, will be able to access the cloud services. Additionally, to achieve high network performance and localization, many of today's clouds consist of data centers located at many locations around the globe. Using this, a service provider can easily leverage geodiversity to get maximum service utility.

D. Service Oriented

As mentioned previously, cloud computing adopts a service-driven operating model. Hence it has a strong emphasis on service management. In a cloud, each IaaS, PaaS and SaaS provider offers its service according to the Service Level Agreement (SLA) negotiated with its customers. SLA assurance is hence a critical objective of every provider.

E. Dynamic resource provisioning

One of the key features of cloud computing is that computing resources can be obtained and released on the fly. Compared to the traditional model that provisions resources according to peak demand, dynamic resource provisioning will allow service providers to acquire resources based on the current demand, which can reduce the operating cost. Self-organizing: Since resources can be allocated or DE allocated on-demand, service providers are empowered to manage their resource consumption according to their own needs. Moreover, the automated resource management feature yields high agility that enables service providers to respond quickly to rapid changes in service demand such as the flash crowd effect.

F. Utility-based pricing

Cloud computing employs a paper-use pricing model. The exact pricing scheme may vary from service to service. For instance, a SaaS provider can rent a VM from an IaaS provider on a per-hour basis. On the other hand, a SaaS provider which provides on-demand customer relationship management (CRM) may charge its customers based on the number of clients it serves (e.g., Sales force). Utility-based pricing lowers service operating cost as it charges customers on a per-use basis. However, it also introduces complexities in controlling the operating cost. In this perspective, companies like VKernel provide software to help cloud customers understand, analyze and cut down the unnecessary cost on resource consumption

VI. Multitenancy approach

Although not an essential characteristic of Cloud Computing in NIST's model, CSA has identified multi-tenancy as an important element of cloud. Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure. [4]

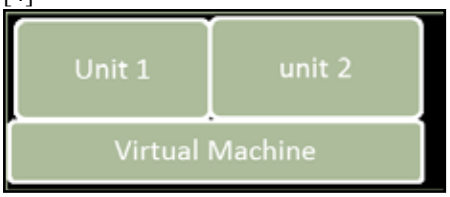

Fig. 3: Multi-tenancy model

From a provider's perspective, multi-tenancy suggests an architectural and design approach to enable economies of scale, availability, management, segmentation, isolation, and operational efficiency; leveraging shared infrastructure, data, metadata, services, and applications across many different consumers. In as much as it may entail enabling the capabilities described above at the infrastructure, database, or application levels. An example would be the difference between an IaaS and SaaS multi-tenant implementation.

A Secure multi-tenant infrastructure (MTI) can combine two types of components.

MTI capable: components that provide explicit multi-tenancy support and are trusted to process and segregate information belonging to multiple tenants.

Non_MTI: components unable to enforce such segregation, which must not receive multiple tenants' information in a form that could enable leakage across tenant boundaries.

It must be able to segregate non-MTI components and across tenant boundaries via physical, network based or crypto methods. Generally we expect MTI – based components to evolve upwards from platforms, hypervisors and selectively into application stack. Trustworthy components require trustworthy supporting layers. Trusted MTI-capable hyper visors are fundamental components for cloud architecture. Multi tenancy can be classified in to two types.

Multi-Tenant with Identical Schemas - While this approach offers substantial scalability, it limits the configuration options for each individual customer forcing them to cope with limited business process support from the application.

Multi-Tenant with Custom Schemas - While this approach offers a wide range of configuration options for the customer, it limits the vendor's ability to maintain one core code base and/or forces the vendor to introduce customer specific complexity into the master code line potentially impacting performance.

VII. OSI layer architecture

The OSI (Open System Interconnection), model defines a networking framework to implement protocols across seven layers.[5] Control is passed from one layer to the next layer. It starts with the application layer in one site, and proceeds to the bottom layer, over the channel to the next site and back up the same hierarchy.

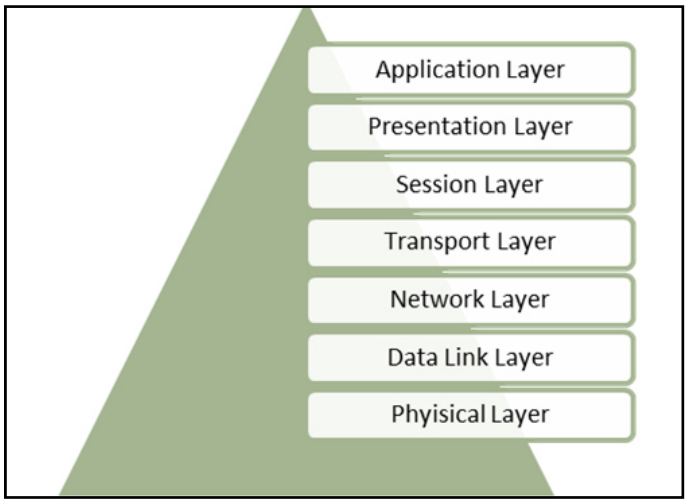

Fig. 4: OSI Layer Architecture

The Physical Layer conveys the bit stream through the network at both the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects.[5] The Data Link Layer furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The Network Layer provides switching and routing technologies, creating logical paths, also called as virtual circuits, to transmit data from one node to the other node. Routing and forwarding are done in this layer. The Transport Layer provides transparent transfer of data between systems or hosts, and is responsible for end-to-end flow control and error recovery[6]. It ensures complete data transfer. The Session Layer does all the tasks like establishing connection, managing connection and terminating connection between applications. The presentation layer works to transform data into the form that the application layer can accept.[7] This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. The Application Layer supports application and end-user processes.

VIII. Factors affecting the security architecture

Security Architecture of any application needs to be chosen very carefully as it is directly tied to the end user complexity to use an application and performance. Same holds good for cloud computing as well. Below are some general issues/key deciding factors which when discussed in detail will help in deciding the right security architecture for a cloud application.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

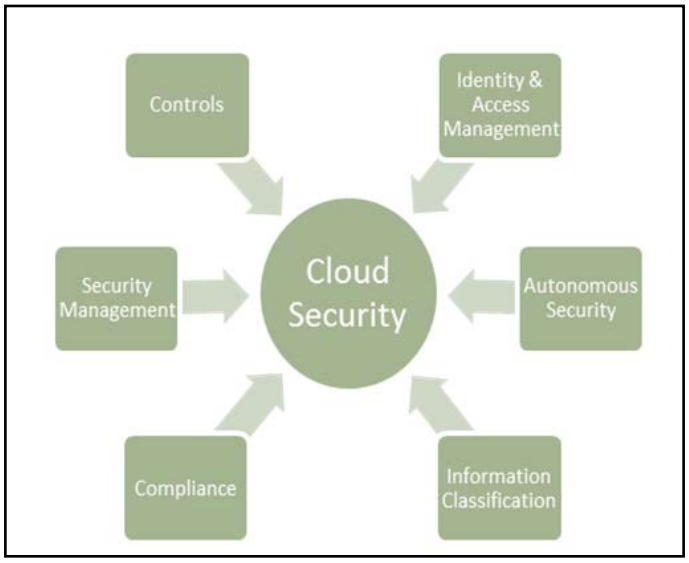

Fig. 5: Factors related to Cloud Security

IX. Security solution providers

Many organizations have come up with their model for addressing these security issues. But the current trend signifies that the organization usually concentrate on addressing only some of the issues regarding to the security. On analysis it has been found that companies concentrate on most common issues and they are less stringent at finding solutions to smaller issues. Moreover some of the organizations have shown interest and brought out solution to some of the other problems. Data has been collected from some of the important security solution providers and the issues they address.

A. AEP Networks

AEP Networks provides CloudProtect as its Security solution product. This product addresses the Application Security, Network Security and Client Security part of Security Solution. This will protect from Insecure Interfaces and APIs and Data Loss or Leakage.

B. Forum Systems

Forum Systems provides specialized solutions like XML Gateway, WAF Gateway and STS Identity Broker. They address the Identity Management and secure firewall at web application level. This will address the concerns like Insecure Interfaces and APIs and also Identity & Access Management.

C. Cipher Cloud

Cipher Cloud provides CipherCloud as its security solution product. This product address the Data level Security aspect of Security Solution. This will protect from Address Information and Lifecycle Management.

D. Symantec

Symantec provides VeriSign Authentication Services, which provides solution for Data Protection, reliability and access Control. This address the Data Loss or Leakage, issues due to shared technology and protect against account or service hijacking.

X. Integrated security architecture

We have analyzed about the various products by different providers which addresses multiple issues related to Cloud security. We propose an architecture which will use the above software at various levels of cloud implementation, thus enabling a robust cloud system.

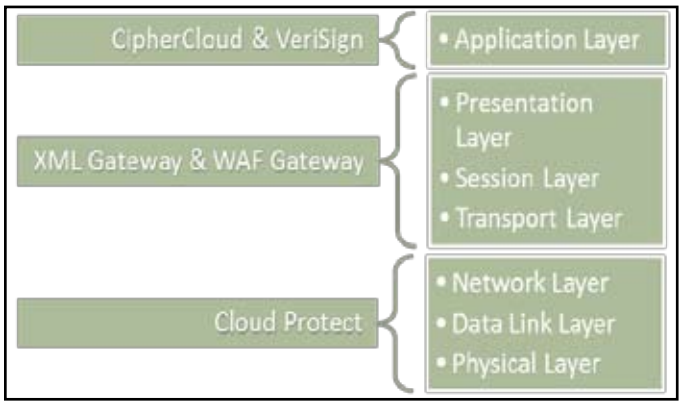

Fig. 6: Proposed Integrated Security Architecture

The CloudProtect works at the network, data link and physical layer thus protecting the system from the attacks that arises out of the network. So this will make sure that the penetration into the cloud architecture from the bottom layer of the topology is handled. The XML Gateway and WAF gateway protects the Presentation, Session and Transport Layer of OSI. This ensures the reliable sending of the data packets between nodes located on Cloud and also it establishes and manages secure connections between the various nodes. The CipherCloud and VeriSign both shall operate at the Application Layer that facilitates interaction with the software. They also addresses the issues with the SaaS type of cloud, ensuring security. Even though both operates at the same level the CipherCloud shall secure the data whereas the VeriSign takes care of access control operations.

So a tight Security mechanism is implemented at all the 7 OSI layers of Networks, so that the cloud does not become vulnerable at any of the layer. This avoids attacks that can happen at a specific level and propagate through the system to other levels eventually breaking the whole application.

XI. Conclusion

In this paper we discuss about the multitenant architecture of public cloud and the security issues that are present in it. We provide an integrated solution to the security issues in the Multi-tenant environment of public cloud. This Integrated Security Solution integrates four different products, which specializes in providing security at various levels of the OSI architecture, hence protecting the Cloud Multi-tenant environment from various threats. Providing a concrete demonstration for the discussed concepts in this paper shall be taken as the future work. In this paper we also discuss about the various Cloud Security products and which layer it protects from threats.

XII. Acknowledgment

I am very thankful to Dr. M. Anand, for his continuous motivation and support during this paper.

References

[1]. Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009.

[2]. Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues" in Proceedings of the 2009 IEEE International Conference on Services

Computing,2009.

[3]. K.Govinda, V.Gurunathaprasad and H.Sathishkumar, "Third party authentication for secure data storage in cloud through digital signature using RSA". IJASTR, Vol.4, Issue 2, August 2012.

[4]. The Growing Importance Of Cloud Brokers, Rakesh Dogra, March 2013 http://www.datacenterjournal.com/the-daily-buzz/growing-importance-cloud-brokers

[5]. Amazon Web Services: Overview of Security Processes, September 2008

[6]. Cloud Computing and Compliance : Be Careful Up There, Wood, Lamont, ITWorld, January 30, 2009

[7]. Mysore R et al (2009) PortLand: a scalable fault-tolerant layer 2 data center network fabric. In: Proc SIGCOMM

[8]. Santos N Gummadi, Rodrigues R (2009) "Towards trusted cloud computing." In. Proc of HotCloud.