International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1499-1506

http://www. irphouse.com

Parametric Analysis of Various Cloud Computing Security Models

Barinder Kaur[1] and Sandeep Sharma[2]

[1,2]G.N.D.U./CSE, Amritsar, India

Abstract

Cloud Computing has established itself as one of the most popular technologies available currently. It has gained much adoration, but with rapid utilization of cloud computing, the security factor has come to forefront. The various popular security models of cloud computing like “The Cloud Multiple-Tenancy Model of NIST”, “The Cloud Risk Accumulation Model of CSA”, “Jerico Formu’s Cloud Cube Model” and “Multi-Clouds Database Model” have been surveyed in this paper and parametric analysis has been made.

Index Terms— Cloud computing, Security models, malicious insiders, virtualization, multi-clouds.

I. Introduction

The cloud computing becomes the significant issue in industry and academia with the active advancement in computer hardware and software. Cloud computing provides the future generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely referred definition of the cloud computing model is introduced by NIST as “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”.

The technology of cloud computing adheres to the demands of the users and renders high scalability and reliability. In the cloud computing system, the resources are transparent for the applications and the location of resources is not to the user using it. The applications can be accessed by the user from any place and at anytime. Multi-tenancy is followed in which various users can share resources. When the workload is increasing, the efficiency of the cloud system can be dealt by adding more hardware to it. Cloud resources are delivered on as a service and as per requirement. When the demand is high the required resources are increased and vice versa.

The cloud computing is bringing significant change in information technology and have accelerated the growth of information technology for the society. The majority of cloud computing infrastructure comprises of reliable services delivered through data centre that are built on servers with different levels of virtualization technologies. The services are accessible throughout the world, with the cloud acting as a single point of access for all the computing needs of consumers. The cloud computing changed the style of software. The user can store data in the cloud system that can be accessed anywhere and at anytime which is often otherwise stored in private and personal systems such as laptops or personal computers. Data security is provided by the cloud computing system and user need not to personally take care of it. So it becomes the responsibility of cloud computing system to ensure proper data safety. Microsoft, Google, Amazon, is few of such companies which offer cloud computing services.

Security is the crucial factor which must be given utmost importance in the cloud computing. As the personal and private data of the user is stored in the cloud which the user may not want to share with anyone or seen by any outside person, so it becomes important that it must be kept safe from hackers. Even business companies who deploy cloud computing in their organizations repose their trust in the security system provided that no malicious outsider can poke into their private data. So security and authorization are important to cloud computing. There is a need to move outside the traditional security mechanisms which are not sufficient. As the cloud computing technology is advancing, so are the risks involved in it. The factors as data security, authorization, user data privacy are integral to the cloud computing and must be safeguarded. [1][2]

II. THE CLOUD COMPUTING SECURITY MODELS

Data security and privacy protection are the primary safety objective of the cloud users. The cloud service provider must neither disclose nor leak the user's private data nor it should itself analyze user's data and poke into the privacy. For example there may be a secret treaty signed by two organizations about their customers and their profit strategies which should not become public. The privacy and data security comprises of life cycle of creation, storage, usage, sharing, updating and destroying of data. The utmost important problem of present scenario is security of cloud computing and to solve it there is a need to build cloud computing security models and analyze the key technologies used in these models. [3]

A. The Cloud Multiple-Tenancy Model of NIST

The significant functional characteristic of cloud computing is Multiple-tenancy.[4] It allows cloud service providers' currently running multiple applications in physical server to offer cloud services to customers. The physical server divides different customer's demands in into equal partitions and processes them with virtualization technique. Sharing and isolation are the key factors of virtualization and is the important technology of cloud computing. By allowing running of multiple virtual machines (VMs) in a physical machine, virtualization enables different customers' applications to share computing resource such as memory, storage, processor, and I/O among, and improves the utilization of cloud resources. By hosting different customers' applications into different virtual machines, virtualization is able to isolate fault, virus, and intrusion from other virtual machines and hardware, and reduce the damage caused by malicious applications. The technology difficulties suffered by multiple-tenancy model are architecture extension, data isolation, configuration self-definition, and performance customization. Data isolation means that the business data of different customers do not intervene mutually. Architecture extension means that multiple-tenancy should provide a basic framework to implement high flexibility and scalability. Configuration self definition means that different customers' respective demands cloud computing should be supported on its service platform configuration. By Performance customization it is meant that different demands of multiple customers should be efficiently met under different levels of workload. Multiple-tenancy model impacts in different ways in different cloud deployment models.

For example, SaaS with multiple-tenancy has two significant function characteristics:

- It is easy to scale-out and scale-up to serve multiple customers based on Web service.
- It helps cutomers to enlarge its service platform and satisfy needs of larger enterprises through additional business logic.

Multiple-tenancy model of cloud computing implemented by virtualization technology offers a method to satisfy different customer demands on governance, segmentation, security, SLA , isolation and billing/chargeback etc. [4]

In simple words, usage of same applications or resources at the same time by multiple customers that may or may not belong to same organization can be termed as Multi-tenancy. From a provider perspective, multi-tenancy can be described as an architectural and design approach to cater to the needs of different customers and to enable economies of scale. [5] [13]

B. The Cloud Risk Accumulation Model of CSA

To examine the security risks posed by cloud computing it is vital to understand the layer dependency of cloud service models.[4] IaaS is the basic foundation layer of all cloud services, PaaS is built upon IaaS and SaaS is built upon PaaS, so there is hereditary among the service capability of different layers in cloud computing. The security risks of cloud computing is also inherited among different service layers similar to cloud service capability inheritance.

- Maximum extensibility is offered by IaaS. It provides negligible security functions and capabilities with exception to its own infrastructure. IaaS in charge customers with the security of software applications and contents, operating systems, etc.

- The capability of developing customized applications for customers based on the PaaS platform is offered by PaaS. It provides more extensibility than SaaS, at the cost of reducing those available distinctive functions of SaaS. Similarly, PaaS offers more flexibility to customers for implementing additional security.
- The least customer extensibility is offered by SaaS but it presents the most integrated service and the highest integrated security among three service layers. Cloud service providers take charge of more security responsibilities in SaaS, and customers has to pay for little security efforts on the SaaS platform.

Lower the service layer that a cloud service provider lies in, the more management duties and security capabilities that a customer is in charge of is one of the important characteristic of cloud security architecture. Cloud service providers need to satisfy the demands on SLA, security, monitor, compliance and duty expectation etc in SaaS. In PaaS and IaaS, the above demands are taken care of by customers, and cloud service provider is only responsible for the availability and security of elementary services such as infrastructure component and underlying platform. [4]

C. Jerico formu's cloud cube model

Jerico formu's cloud cube model [4] is a visualization of combination of deployment models, cloud service models of cloud computing , the attributive detail of management and ownership and physical location of resources, owner and manager of resources Different model parameters used in cloud cube model is as follows:

- Internal/External: It describes the physical location where actual data is stored If data is stored inside the boundaries of owner of the data, then the value of model parameter is internal and vice versa. For example, the data center of a private business organization cloud is internal, and the data center of Amazon's SC3 is external. The cloud with internal data storage is not necessarily more secure than the one with external data storage. The combination of internal and external data storage may be best appropriate solution to more secure usage model.
- Proprietary/Open: The ownership of cloud's technology, interface and service etc is best described by this parameter. The degree of interoperability, i.e. the ability of transforming data from a cloud modality to other cloud modality without any constraint, the portability of data and application between proprietary system and other cloud modalities is indicated by this parameter. When a cloud service provider holds the ownership of facilities providing cloud services, it is termed as proprietary, hence the operation of cloud is proprietary and customers can not transfer their applications among different cloud service provider with ease. The technologies used in public cloud are generally open and uniform, meaning more available service providers and less constraint on data share and incorporation with business partners. Unproven but most, open clouds can promote easily and effectively the incorporation between multiple organizations.
- Parameterized/De-parameterized: To present the "architectural mindset" of security protection, i.e. whether a customer's application is inside the

traditional security boundary or outside this modal parameter is used. Parameterized is when a customer's application operates within traditional IT security boundary signaled by firewall that blocks the incorporation of different security zones. In fact, customers running some applications inside of security zone can expand/shrink their application perimeter to/back from external cloud environment by virtual Private Network. De-parameterized is the fade way of traditional IT security boundary and the exposure of a customer's application operation. For the security protection of deperimeterised environment, Jerico Forum uses the meta-data and mechanisms in their commandments and Collaboration Oriented Architectures Framework (COA) to encapsulate data of customer.

- Insourced/Outsourced :This model parameter is used to define the 4th dimension that has two states in each of the eight cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO). Insourced can be defined as cloud service presented by an organization's own employees, and Outsourced can be termed as that cloud service which is presented by a third party. This is a policy issue a business one but not a technical or architectural decision. [4] [6] [5]

D. Multi-Clouds Database Model

Multi-Clouds Database Model [7] presents cloud with database storage in multi-clouds service provider. It is different from Amazon cloud service which provides a single cloud storage data. MCDB model does not safeguard security by single cloud; rather security and privacy of data will be provided by implementing multi shares technique on multi-cloud providers. By doing so, it lessens the negative effects of single cloud, reduces the security risks from malicious insider in cloud computing environment, and narrows the negative impact of encryption techniques.

MCDB provides security and privacy of user's data by replicating data among several clouds and by using the secret sharing approach. It deals with the database management system (data source) to manage and control the operations between the clients and the cloud service providers (CSP). At the client side, this sends data inquiries to server or instance such as in Amazon in CSP. The data source stores the data in the cloud side which is supposed to be a trusted cloud, additional to ensuring the privacy of any query that the client has made and for the security of the client stored data. A problem occurs when we cannot guarantee cloud is a trusted service. [7]

III. COMPARATIVE ANALYSIS OF CLOUD COMPUTING SECURITY MODELS

In this section analysis and evaluation of the cloud computing security models has been done on the basis of following parameters:

- Technology Used: It depicts which technology forms the basis of the working of the foresaid model.
- Authorizations: It represents that whether the user or the provider has more

say in the security management of the cloud computing.

- Security: It tells how secure the particular cloud computing security models is.
- Malicious insiders: It describes the chances that up to which extend the unauthorized used or hacker can have access to the stored data in the cloud computing system.

The comparison and analysis of these parameters are shown in Table1 and Table2.

TABLE1. Comparative Analysis

Models **Parameters**	**The Cloud Multiple-Tenancy Model of NIST**	**The Cloud Risk Accumulation Model of CSA.**	**Jerico Formu's Cloud Cube Model**	**Multi-Clouds Database Model**
Technology Used	Virtualization	Layer Dependency of Cloud Service Models	Attribute information implied in service and deployment of cloud computing and location, owner and manager of computing resources	Multi-cloud service providers and secret sharing algorithm
Authority	User not in charge	User not in charge (Depends on which layer the cloud service provider lies in)	User in charge partially (Depends on model parameters as Internal/External, Proprietary/Open, Perimeterised/De-perimetrised Insourced/Outsourced)	User not in charge (provides cloud database which permit customers with different database queries to store different data
Security	Medium	Medium	High	High
Malicious Insiders	Less	More	More	Less

Table 2. Pros And Cons Of Various Cloud computing security models

Cloud Computing Security Models	**Pros**	**Cons**
The Cloud Multiple-Tenancy Model of NIST	Isolate fault, virus, and intrusion of one from other virtual machines and hardware, and reduce the damage of malicious applications.	The technology difficulties like data isolation, architecture extension, configuration self-definition, and performance customization
The Cloud Risk Accumulation Model of CSA	The layer dependency of cloud service models help to analyze the security risks of cloud computing.	Lower service layer that a cloud service provider lies in, the more management duties and security capabilities that a customer is in charge of, more risk of security breach.
Jerico Formu's Cloud Cube Model	Selecting cloud formations for secure collaboration.	When closing down an agreement with a provider, care should be taken to ensure that the data is appropriately deleted from the cloud service provider's infrastructure (including backups), otherwise a data leak risk will remain.
Multi-Clouds Database Model	Lowers the risk of malicious insider in the cloud and avoid failing of cloud services	More time and cost consumption

iv. CONCLUSIONS AND FUTURE WORK

Cloud computing is the up surging technology which is widely gripping whole of the information industry. The four models have been surveyed and compared. It has been concluded that Jerico Formu's Cloud Cube Model and Multi-Clouds Database Model are more secure in comparison to The Cloud Multiple-Tenancy Model of NIST and The Cloud Risk Accumulation Model of CSA. It has been analyzed that Multi-Clouds Database Model has less malicious insiders among the other compared models. As the future point of view work can be carried on to provide more secure cloud computing security model to improve the technology used, authorization, security and malicious insiders.

References

[1] Wentao, Liu. (2012). Research on cloud computing security problem and strategy. Consumer Electronics Communications and Networks (CECNet), 2012 2nd International Conference on, vol., no., pp.1216, 1219, 21-23.

[2] AlZain, M.A.; Pardede, E.; Soh, B.; Thom, J.A. (2012). Cloud Computing Security: From Single to Multi-clouds. System Science (HICSS), 2012 45th Hawaii International Conference on, vol., no., pp.5490, 5499, 4-7.

[3] Su Qinggang; Wang Fu; Hang Qiangwei. (2012). Study of Cloud Computing Security Service Model," Engineering and Technology (S-CET), 2012 Spring Congress on, vol., no., pp.1,4, 27-30.

[4] Che Jianhua, Duan Yamin, Zhang Tao, Fan Jie. (2012). Study on the security models and strategies of cloud computing. 2011 International Conference on Power Electronics and Engineering Application. Procedia Engineering 23 (2011) 586 – 593.

[5] Hopkins Hupert. (2012). Securing the Cloud. diebold.

[6] Chang, V.; Bacigalupo, D.; Wills, G.; De Roure, D. (2010). A Categorisation of Cloud Computing Business Models. Cluster, Cloud and Grid Computing (CCGrid). 2010 10th IEEE/ACM International Conference on , vol., no., pp.509,512, 17-20.

[7] AlZain, M.A.; Soh, B.; Pardede, E. (2011). MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. Dependable, Autonomic and Secure Computing (DASC). 2011 IEEE Ninth International Conference on , vol., no., pp.784,791, 12-14.

[8] Chang, V.; Bacigalupo, D.; Wills, G.; De Roure, D. (2010). A Categorisation of Cloud Computing Business Models. Cluster, Cloud and Grid Computing (CCGrid). 2010 10th IEEE/ACM International Conference on , vol., no., pp.509,512, 17-20.

[9] AlZain, M.A.; Pardede, E.; Soh, B.; Thom, J.A. (2012). Cloud Computing Security: From Single to Multi-clouds. System Science (HICSS). 2012 45th Hawaii International Conference on, vol., no., pp.5490, 5499, 4-7.

[10] Anantwar G. Ritesh, Chatur Dr. P.N, Anantwar G. Swati. (2012). Cloud Computing and Security Models: A Survey. International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2.

[11] Chang, V.; Bacigalupo, D.; Wills, G.; De Roure, D. (2010). A Categorisation of Cloud Computing Business Models. Cluster, Cloud and Grid Computing (CCGrid), 2010 10th IEEE/ACM International Conference on , vol., no., pp.509,512, 17-20.

[12] Aljahdali, H.; Townend, P.; Jie Xu. (2013). Enhancing Multi-tenancy Security in the Cloud IaaS Model over Public Deployment. Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on , vol., no., pp.385,390, 25-28.

[13] Cloud Security Alliance. (2009). Security guidance for critical areas of focus in cloud computing (v2.1).

[14] Jericho Formu. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration. (2009). http://www. opengroup.org/jericho/ cloud_cube_model_v1.0.pdf.