An Overview of Security Models and Threats in Cloud Computing

Jitendra Singh Rajawat[*], Sanjay Gaur[**]
*Research Scholar, Pacific University
**Associate Professor and Coordinator, Faculty of Computer Application, Pacific University
[*]jits.rajawat@gmail.com, sanjay.since@gmail.com

***Abstract*-Cloud computing is an upcoming computing paradigm in which resources of the computing infrastructure are provided as services over the internet. As promising it is, this paradigm also brings forth many new challenges. However, the security of cloud computing is always center of attention of various potential cloud customers, and big obstacle for its widespread applications. In this Paper, to assist people to understand the basics concept of cloud computing and put in some efforts to deal with one of the major security issues that is security of cloud computing, we surveyed the existing popular security models of cloud computing and summarized the mains threats of cloud computing.**

Keywords: Cloud Computing, Security Models, Threats in Cloud

I. INTRODUCTION

The advent of cloud computing in recent years has sparkled interest from different stakeholders of Information Technology (IT) and Computer Science, such as academicians, business organization, institutions. Cloud computing is new computing model which has been adapted from the former grid computing paradigm, and other computing paradigm like utility computing, autonomic computing and cluster computing. The definition and specifications of cloud computing were standardized by the U.S. National Institute of Standards and Technology (NIST) in September 2011. According to NIST the definition of Cloud computing is 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. This cloud model consists of essential characteristics, three service models and four deployment models.

A. Cloud Service Models

Cloud service models are divided among three models. The three fundamental classifications are often referred to as the "SPI Model, "where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively.

a) Software as Service (SaaS): In Software as Service (SaaS) model user are provided with capability to use services as application running on the top of a cloud infrastructure. The user cannot manage or control the operating system, network, server or even application. The user can only control limited user specific application configuration settings.
Example: SalesForce CRM, Google Diocs

b) Platform as Service (PaaS): In Platform as Service (PaaS) user are provided a computing platform, typically including operating system, programming language execution environment, database and web server. The user can control over the deployed applications and possibly application hosting environment configuration.
Example: Google Apps and Microsoft Window Azure.

c) Infrastructure as Service: In Infrastructure as Service (IaaS) model user are provided infrastructure like virtual machines, server, load balancers and network. The user can use the IaaS based service offering to deploy his own operating system and application, providing a variety of deployment possibilities for a user in comparison to PaaS & SaaS. The user has control over operating systems, storage, deployed application, and possibility limited control of selecting network component (e.g host firewall).
Example: Amazon (S3, EC2) etc.

B. Cloud Deployment Models

Irrespective of the service model use (SaaS, PaaS, IaaS) there are four deployment models based on user requirement.

a) Public Cloud: In the public cloud (or external cloud) computing resources are dynamically provisioned over the Internet via Web applications or Web services from an off-site third-party provider. Public clouds are run by third parties, and applications from different customers are likely

to be mixed together on the cloud's servers, storage systems, and networks.

b) Private Cloud: Private cloud (or internal cloud) refers to cloud computing on private networks. Private clouds are built for the exclusive use of one client, providing full control over data, security, and quality of service. Private clouds can be built and managed by a company's own IT organization or by a cloud provider.

c) Community Cloud*:* In community cloud infrastructure is shared between several organizations having common goals (Security, Compliance, and Judriction etc.). It is managed by the organizations or a third party and may exist on campus or off-campus.

d) Hybrid Cloud: A hybrid cloud environment combines multiple public and private cloud models. Hybrid clouds introduce the complexity of determining how to distribute applications across both a public and private cloud.

II. SECURITY ISSUE WITH CLOUD COMPUTING AND THEIR MITIGATION

There are various security concern that prevent customer from taking benefit of the cloud. The security threat present in the cloud and their mitigation are following:

A. VM-Level Attacks

The cloud computing is based on VM technology. For implementation of cloud, a hypervisor such as VMWarevSphere, Microsoft Virtual PC, Xen etc. are used. This threat arises because of the vulnerabilities appearing in these hypervisors due to some facts being overlooked by developers during the coding of these hypervisors.

Mitigation: - The threat arising due to VM-Level vulnerabilities can be mitigated by monitoring through IDS (Instruction Detection System)/IPS (Intrusion Prevention System) and by implementing firewall.

B. Abuse and Nefarious Use of Cloud Computing

This threat arises due to relatively weak registration systems present in the cloud computing environment. In cloud computing registration process, anyone having a valid credit card can register and use the service. This facilitates anonymity, due to which spammer, malicious code authors and criminals can attack the system.

Mitigation: - This type of threat can be mitigated in following ways:

- By implementing stricter registration process and validation process.
- By credit card fraud monitoring and coordination.
- Detailed introspection of user's network traffic.
- Network blocks through monitoring public black lists.

C. Loss of Governance

The client gives up control to the cloud provider on a number of issues while using the cloud infrastructure. The Service Level Agreements (SLA) may not have commitment on the part of cloud provider, to provide such services, thus having a gap in security defences affecting security. This loss of control may lead to a lack of confidentiality, integrity and availability of data.

Mitigation: - There are no publicly available standards specific to cloud computing security. Thus organizations considering cloud services need to exercise persistent and careful efforts for the execution of Service Level Agreements (SLA).

D. Lock-IN

Lock-IN means inability of the customer to migrate from one cloud service provider to another. This is due to loss of portability of the customer data and programs. Presently, there are few tools, procedures or standard data formats which provide data, application or service portability. This prevents customers or organizations from adopting cloud computing.

Mitigation: - Standardized cloud Application Programming Interface (API) should be used. This standardization will ensure cloud computing to be more fully accepted.

E. Insecure Interfaces and APIs

Customers use a set of software Interfaces or APIs to interact with cloud services. The provisioning, management, orchestration and monitoring of the cloud service are generally done using these interfaces. If the weak set of interfaces and APIs are used, this may expose organizations to various security threats, such as anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities.

Mitigation:- To mitigate the above threats, the security model of cloud provider interfaces should be analyzed. Strong authentication and access controls should be implemented. Encryption should be used for transmission of content and dependency chain associated with the API should be clearly understood.

F. Data Loss or Leakage

Data loss or leakages have an adverse effect on the business. The brand or reputation is completely lost and the customers' morale and trust are eroded. This data loss or leakage may be due to insufficient authentication, authorization and audit controls, inconsistent use of encryption and software keys, disposal challenges, a data centre reliability, and disaster recovery.

Mitigation: - The threats arising due to data loss or leakage can be mitigated by encrypting and protecting integrity of data in transit, analyzing data protection at both design and runtime, implementing strong key generation, storage and management. Contractually demanding provider to wipe persistent media before it is released in to pool and contractually specifying provider backup and retention strategies.

III. SECURITY MODEL OF CLOUD COMPUTING

A. The Cloud Multiple-Tenancy Model of NIST

Multiple-tenancy [4] is an important function characteristic of cloud computing that allows multiple applications of cloud service providers currently running in a physical server to offer cloud service for customers. This physical server partitions and processes different customer demands with virtualization. Virtualization possesses good capability of sharing and isolation, and is a right core technology of cloudcomputing. By running multiple virtual machines (VMs) [5] in a physical machine, virtualization enables to share computing resource such as processor, memory, storage, and I/O among different customers' applications, and improves the utilization of cloud resources. By hosting different customers' applications into different virtual machines, virtualization enables to isolate fault, virus, and intrusion of one from other virtual machines and hardware, and reduce the damage of malicious applications. The technology difficulties of multiple-tenancy model include data isolation, architecture extension, configuration self-definition, and performance customization. Data isolation means that the business data of multiple 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 cloud computing should support different customers' respective demands on its service platform configuration. Performance customization means that cloud computing should assure different customers' demands on the performance of multiple-tenancy platform under different workload. The impact of multiple-tenancy model is different corresponding to different cloud deployment models. Taking SaaS as an example, SaaS with multiple-tenancy function characteristic has two basic features. First, it is easy to scale-out and scale-up to serve for a mass of customers based on Web service. Second, it can present additional business logic that enables customers to extend its service platform and satisfy larger enterprises" demands. Multiple-tenancy model of cloud computing implemented by virtualization offers a method to satisfy different customer demands on security, segmentation, isolation, governance, SLA and billing/chargeback etc.

B. The Cloud Risk Accumulation Model of CSA

Understanding the layer dependency of cloud service models is very critical to analyze the security risks of cloud computing. IaaS is the foundation layer of all cloud services, PaaS is built upon IaaS and SaaS is built upon PaaS, so there is an inherited relation between the service capability of different layers in cloud computing. Similar to the inheritance of cloud service capability, the security risks of cloud computing is also inherited between different service layers [4].

• IaaS provides no distinctive function similar to application service but maximum extensibility for customers, meaning that IaaS holds little security functions and capabilities except for the infrastructure's own security functions and capabilities. IaaS demands that customers take charge of the security of operating systems, software applications and contents etc.

• PaaS offers the capability of developing customized applications based on the PaaS platform for customers and more extensibility than SaaS, at the cost of reducing those available distinctive functions of SaaS. Similarly, the intrinsic security function and capability of PaaS are not complete, but customers possess more flexibility to implement additional security.

• SaaS presents the least customer extensibility, but the most integrated service and the highest integrated security among three service layers. In SaaS, cloud service providers take charge of more security responsibilities, and customers pay for little security effort on the SaaS platform. One critical feature of cloud security architecture is that the lower service layer that a cloud service provider lies in, the more management duties and security capabilities that a customer is in charge of. In SaaS, cloud service providers need to satisfy the demands on SLA, security, monitor, compliance and duty expectation etc. In PaaS and IaaS, the above demands are charged by customers, and cloud service provider is only responsible for the availability and security of elementary services such as infrastructure component and underlying platform.

C. Jerico Forum's Cloud Cube Model

Jerico forum's cloud cube model is a figuration description of security attribute information implied in the service and deployment models of cloud computing and the location,

manager and owner of computing resources and so on as figure 3 shown. In cloud cube model, the definitions of model parameters are as follows:

a) Internal/External: a model parameter to define the physical location of data storage. If the physical location of data storage is inside of the data owner's boundary, then the model parameter value is internal. Contrariwise, the model parameter value is external. For example, the data center of a private enterprise cloud is internal, and the data center of Amazon's SC3 is external. Note: the cloud with internal data storage is not more secure than the one with external data storage. The combination of internal and external data storage maybe present more secure usage model.

b) Proprietary/Open*:* a model parameter to define the ownership of cloud's technology, service and interface etc. This model parameter indicates the degree of interoperability, i.e. the portability of data and application between proprietary system and other cloud modalities, the ability of transforming data from a cloud modality to other cloud modality without any constraint. Proprietary means that a cloud service provider holds the ownership of facilities providing cloud services, hence the operation of cloud is proprietary and customers can not transfer their applications from one to another cloud service provider without great effort or investment. 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 effectively the incorporation between multiple organizations. Fig. 3 the cloud cube model of Jericho forum[6] Fig. 4 the mapping model of cloud, security and compliance[4]

c) Perimeterised/De-perimeterised: a model parameter to describe the "architectural mindset" of security protection, i.e. a customer's application is inside or outside of traditional security boundary? Perimeterised means that 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 extend/shrink their application perimeter to/back from external cloud environment by VPN. De-perimeterised means that the fadeway 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 a customer's data.

d) Insourced/Outsourced*:* a model parameter 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 means that cloud service is presented by an organization's own employees, and Outsourced means that cloud service is presented by a third party. These two states answer the question "who do you want to build or manage your cloud service?" This is a policy issue (i.e. a business but not a technical or architectural decision).In cloud cube model, other attributes such as Offshore and Onshore are also relevant to cloud computing, but in this paper we have focused on the four dimensions identified in cloud cube model.

D. The Mapping Model of Cloud, Security and Compliance

The mapping model of cloud ontology, security control and compliance check presents a good method to analyze the gaps between cloud architecture and compliance framework and the corresponding security control strategies that should be provided by cloud service providers, customers or third parties [4] as figure 4 shown. To protect effectively the security of cloud environment, we should firstly analyze the security risks confronted by cloud environment, and then find out the gap matrix according to cloud architecture and its compliance framework, and finally adopt some relevant security controls. Here, the compliance framework of cloud computing is not naturally existed with the cloud model. Correspondingly, the mapping model of cloud, security and compliance contributes to determining whether accept or refuse the security risks of cloud computing. Note that as a computing paradigm, cloud computing does not influence the satisfaction of compliance. Several surveys such as the security architecture documents of Open Security Architecture Group and NIST 800-53 revision 3- Recommended Security Controls for Federal Information Systems and Organizations brilliantly expatiate the above general control framework.

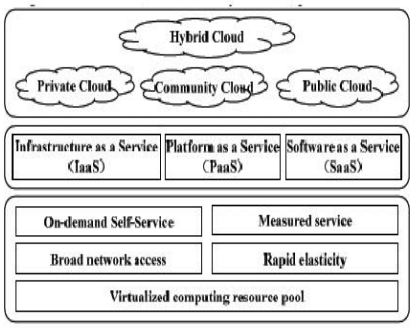
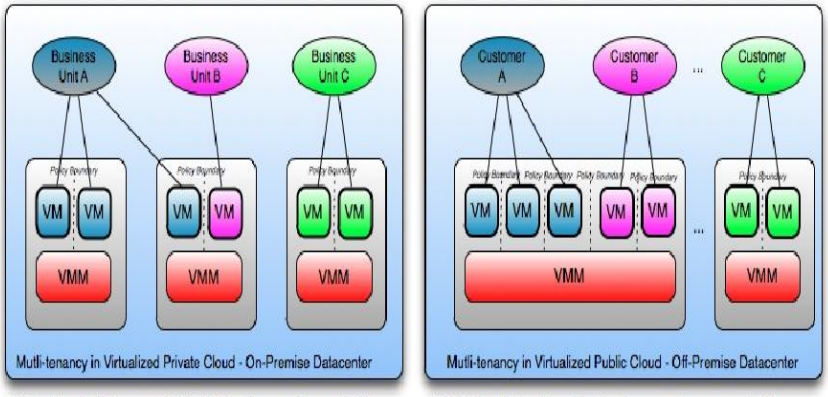


Fig.1. the NIST's definition model of cloud computing[1]



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Fig. 2 Multiple-Tenancy model of cloud computing[4]

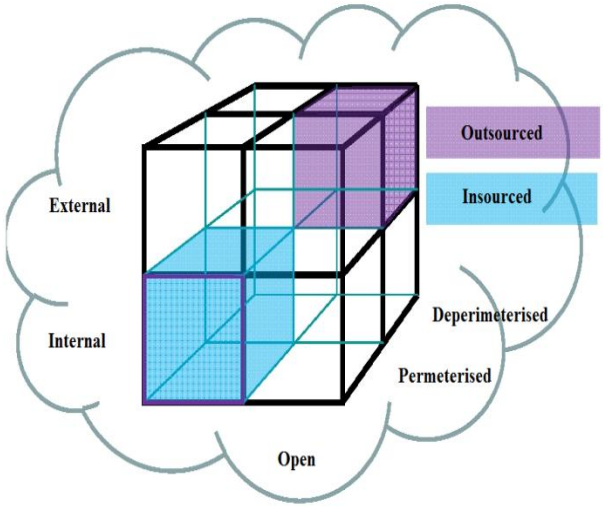


Fig. 3 Cloud cube model of Jericho Forum[6]

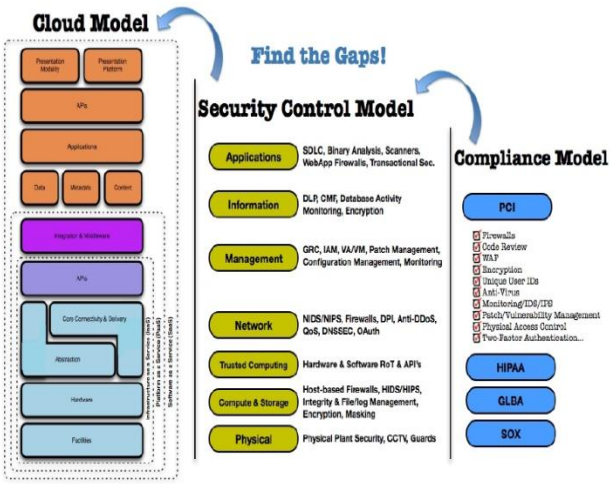


Fig. 4 Mapping model of cloud security and compilance[4]

CONCLUSION

Cloud Computing embodies the as-a-Service paradigm and allows for services to be provided en masse to consumers. In this paper we presented the concepts related to cloud computing like definition of cloud computing, various service models, cloud deployment model. In addition to this we also provided security threats present in cloud computing along with their mitigation and at last we surveyed the existing security models of cloud computing. In future we will try to implement security strategies by use of technology.

REFERENCES

[1] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In:

ACMSIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009. p. 50–5.

[2] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing, 2009. http://www.ibm.com/developerswork/websphere/zones/hipods/library.html.

[3] "Study on the security models and strategies of cloud computing" Jianhua Chea*, Yamin Duanb, Tao Zhanga, Jie Fanaa 2011 International Conference on Power Electronics and Engineering Application.

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

[5] VMware. Inc. Understanding full virtualization, paravirtualization and hardware assist. Technical report, VMware, 2007.

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