ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

Cloud Computing and Security Models: A Survey

Ritesh G. Anantwar, Dr. P.N. Chatur, Swati G. Anantwar
M tech., HOD, GCOE Amravati (MH) (INDIA), ME SGBAU Amravati (MH)

Abstract-- ***Cloud computing is introducing many huge changes to people's lifestyle and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always the focus of numerous potential cloud customers, and a big barrier for its widespread applications. In this paper, to facilitate people to understand the concept of cloud computing and contribute some efforts to pursue one of the major issues that is security of cloud computing, we surveyed the existing popular security models of cloud computing, e.g. multiple-tenancy model, risk accumulation model, cube model of cloud computing, and summarized the main threats of cloud computing.***

Keywords: **Cloud Computing, Cloud Computing Security Models, Threats in Cloud**

I. INTRODUCTION

A. Difference between Grid and Cloud Computing

Grid Computing emerged in the early 1990s, as high performance computers were interconnected via fast data communication links, with the aim of supporting complex calculations and data-intensive scientific applications. Grid computing is defined as ‘‘a hardware and software infrastructure that provides dependable consistent, pervasive, and inexpensive access to high-end computational capabilities’’. Cloud Computing has resulted from the convergence of Grid Computing, Utility Computing and SaaS, and essentially represents the increasing trend towards the external deployment of IT resources, such as computational power, storage or business applications, and obtaining them as services [1]. 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 [2].

The name cloud computing was inspired by the cloud symbol that is often used to represent the Internet in flow charts and diagrams. A distinct migration to the clouds has been taking place over recent years with end users, ‘‘bit by bit’’ maintaining a growing number of personal data, including bookmarks, photographs, music files and much more, on remote servers accessible via a network. Cloud computing is empowered by virtualization technology; a technology that actually dates back to 1967, but for decades was available only on mainframe systems. In its quintessence, a host computer runs an application known as a hypervisor; this creates one or more virtual machines, which simulate physical computers so faithfully, that the simulations can run any software, from operating systems, to end-user applications [3]. At a hardware level, a number of physical devices, including processors, hard drives and network devices, are located in datacenters, independent from geographical location, which are responsible for storage and processing needs. Above this, the combination of software layers, the virtualization layer and the management layer, allow for the effective management of servers. Virtualization is a critical element of cloud implementations and is used to provide the essential cloud characteristics of location independence, resource pooling and rapid elasticity. Differing from traditional network topologies, such as client–server, cloud computing is able to offer robustness and alleviate traffic congestion issues. The management layer is able to monitor traffic and respond to peaks or drops with the creation of new servers or the destruction of nonnecessary ones. The management layer has the additional ability of being able to implement security monitoring and rules throughout the cloud. According to Merrill Lynch, what makes cloud computing new and differentiates it from Grid Computing is virtualization:

‘‘Cloud computing, unlike grid computing, leverages virtualization to maximize computing power. Virtualization, by separating the logical from the physical, resolves some of the challenges faced by grid computing’’ [4]. While Grid Computing achieves high utilization through the allocation of multiple servers onto a single task or job, the virtualization of servers in cloud computing achieves high utilization by allowing one server to compute several tasks concurrently [5]. While most authors acknowledge similarities among those two paradigms, the opinions seem to cluster around the statement that cloud computing has evolved from Grid Computing and that Grid Computing is the foundation for cloud computing.

B. Cloud Computing

Cloud computing, to put it simply, means “Internet Computing.” The Internet is commonly visualized as clouds; hence the term “cloud computing” for computation done through the Internet. With Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides, databases in cloud are very dynamic and scalable.“ 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, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

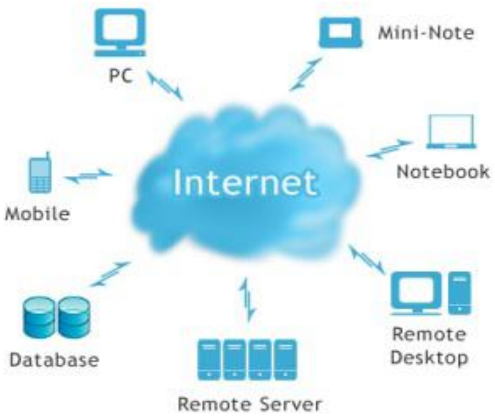


Fig 1: CLOUD COMPUTING [1]

C. Cloud Service Models

a) Software-as-a-Service (SaaS). The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer. The cloud provider is responsible for the management the application, operating systems and underlying infrastructure. The consumer can only control some of the user-specific application configuration settings. Example: Yahoo!, Gmail, Google Diocs, etc.

b) Platform-as-a-Service (PaaS). The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud-based infrastructure. “The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations”. Example: Google Aps, SQL Azure, etc.

c) Infrastructure-as-a-Service (IaaS). The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, processing power and network capacity. The consumer can the use IaaS based service offerings to deploy his own operating systems and applications, offering a wider variety of deployment possibilities for a consumer than the PaaS and SaaS models. “The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)”. Example: Amazon (S3, EC2), Windows Azure, etc.

D. Cloud Deployment Models

Regardless of which delivery model is utilized, cloud offerings can be deployed in four primary ways, each with their own characteristics. The characteristics to describe the deployment models are; (i) who owns the infrastructure; (ii) who manages the infrastructure; (iii) where is the infrastructure located; (iv) and who accesses the cloud services.

a. Public Clouds

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

Public cloud computing is based on massive scale offerings to the general public. The infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure. Public cloud users are considered to be untrusted, which means they are not tied to the organization as employees and that the user has no contractual agreements with the provider.

b. Private clouds

Private clouds run in service of a single organization, where resources are not shared by other entities. "The physical infrastructure may be owned by and/or physically located in the organization's datacenters (on-premise) or that of a designated service provider (off-premise) with an extension of management and security control planes controlled by the organization or designated service provider respectively". Private cloud users are considered as trusted by the organization, in which they are either employees, or have contractual agreements with the organization.

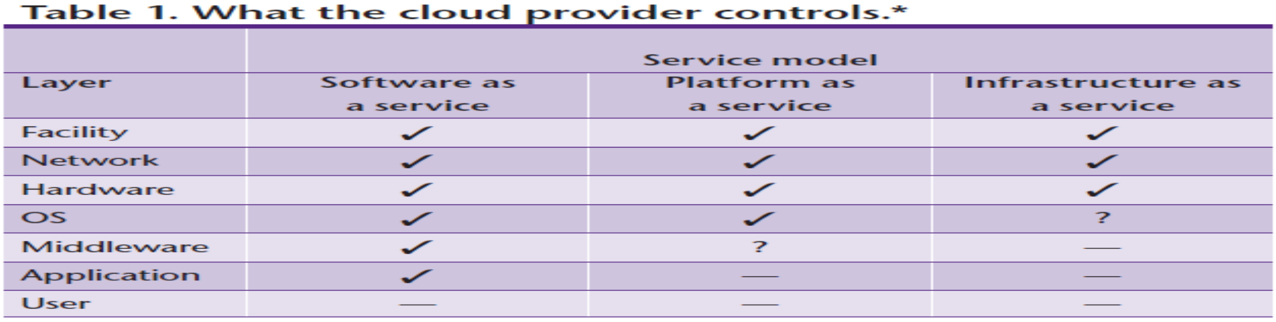
c. Community clouds

Community clouds run in service of a community of organizations, having the same deployment characteristics as private clouds. Community users are also considered as trusted by the organizations that are part of the community.

d. Hybrid clouds

Hybrid clouds are a combination of public, private, and community clouds. Hybrid clouds leverage the capabilities of each cloud deployment model. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other. Where private and community clouds are managed, owned, and located on either organization or third party provider side per characteristic, hybrid clouds have these characteristics on both organization and third party provider side. The users of hybrid clouds can be considered as trusted and untrusted. Untrusted users are prevented to access the resources of the private and community parts of the hybrid cloud.

Table 1. What the cloud provider controls.*



Layer	Service model Software as a service	Platform as a service	Infrastructure as a service
Facility	✓	✓	✓
Network	✓	✓	✓
Hardware	✓	✓	✓
OS	✓	✓	?
Middleware	✓	?	—
Application	✓	—	—
User	—	—	—

* Question marks indicate layers in which either the provider or user could be in control.

II. ISSUES WITH CLOUD COMPUTING

1. ***Host security issues***

   The host running the job, the job may well be a virus or a worm which can destroy the system from malicious users

2. ***Network security issues***

   Denial of Service**:** where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service. Like DNS Hacking, Routing Table "Poisoning", XDoS attacks

   QoS Violation: through congestion, delaying or dropping packets, or through resource hacking.

   Man in the Middle Attack**:** To overcome it always use SSL

   IP Spoofing**:** Spoofing is the creation of TCP/IP packets using somebody else's IP address.

3. ***Security issues from virtualization***

   Type of virtualization provider is using Para Virtualization or full system virtualization.

   Instance Isolation: ensuring that Different instances running on the same physical machine are isolated from each other.

   Control of Administrator on Host O/s and Guest o/s.

   Current VMMs do not offer perfect isolation: Many bugs have been found in all popular VMMs that allow to escape from VM!

Virtual machine monitor should be ‘root secure’, meaning that no level of privilege within the virtualized guest environment permits interference with the host system.

4. ***Ensuring both data and code safety?***

Very hard for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing service provider because the customer generally has no access to the provider’s facility which can be comprised of multiple facilities spread around the globe.

III. THE SECURITY MODELS 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 cloud computing. 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 formu’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:

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.

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]

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.

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.

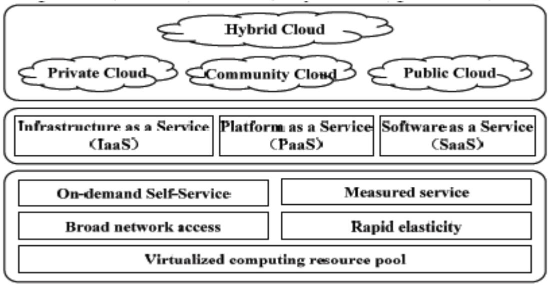


Fig.1. the NIST's definition model of cloud computing[1]

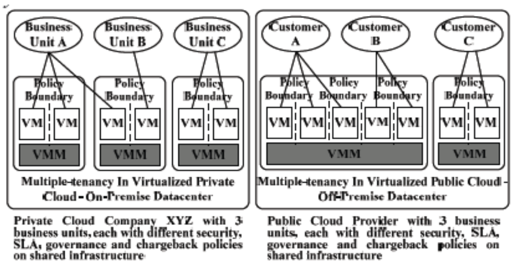

Business Unit A
Business Unit B
Business Unit C
Customer A
Customer B
Customer C
Policy Boundary
VM
VMM
Multiple-tenancy In Virtualized Private Cloud - On-Premise Datacenter
Multiple-tenancy In Virtualized Public Cloud - Off-Premise Datacenter
Private Cloud Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure
Public Cloud Provider with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

Fig.2. the multiple-tenancy model of cloud computing[4]

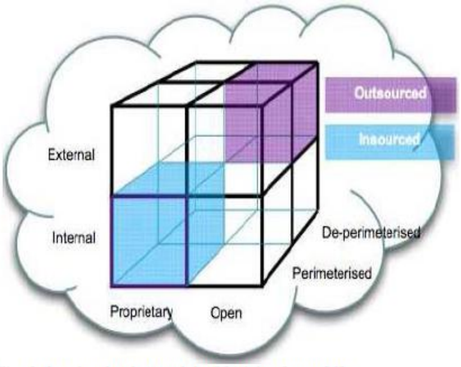


Fig. 3 the cloud cube model of Jericho forum[6]

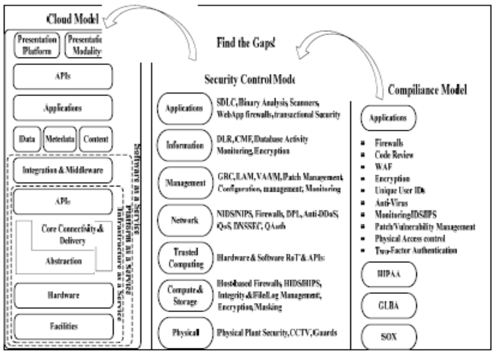

Cloud Model
Presentation Platform
Presentation Modality
APIs
Applications
Data
Metedata
Content
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Software as a Service
Platform as a Service
Infrastructure as a Service
Find the Gaps!
Security Control Mode
Applications
SDLC, Binary Analysis, Scanners, WebApp firewalls, transactional Security
Information
DLR, CMF, Database Activity Monitoring, Encryption
Management
GRC, IAM, VA/VM, Patch Management, Configuration, management; Monitoring
Network
NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing
Hardware & Software RoT & APIs
Compute & Storage
Host-based Firewalls, HIDS/HIPS, Integrity & File/Log Management, Encryption, Masking
Physical
Physical Plant Security, CCTV, Guards
Compiliance Model
Applications
Firewalls
Code Review
WAF
Encryption
Unique User IDs
Anti-Virus
Monitoring/IDS/IPS
Patch/Vulnerability Management
Physical Access control
Two-Factor Authentication
HIPAA
GLBA
SOX

Fig. 4 the mapping model of cloud, security and compliance[4]

IV. CONCLUSION AND FUTURE WORK

Cloud computing is a kind of computing paradigm that can access conveniently a dynamic and configurable public set of computing resources (e.g. server, storage, network, application and related service), provided and published rapidly and on-demand with least management and intervention. However, the prevalence of cloud computing is blocked by its security to a great extent. To contribute some effort to improving the security of cloud computing, finally, we surveyed the main existing security models of cloud computing, and summarized the main security risks of cloud computing from different Organizations. In the future, we will give and implement some security strategies with technology and management ways.

REFERENCES

[1] Wikipedia, http:// en.wikipedia.org/ wiki/ Cloud Computing.

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

[3] Cloud Security Alliance. Top Threats to Cloud Computing, 2010.http://www.cloudsecurityalliance.org [accessed on: March, 2010].

[4] “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.

[5] Virtual PC vulnerability. http://www.microsoft.com/technet/security/bulletin/ms07-049.mspx.

AUTHOR BIOGRAPHY

Ritesh G. Anantwar pursuing Masters of Technology in Computer Science and Engineering at Government College of Engineering Amravati, (MH) (INDIA),awarded with scholarship from HR department of Government of India for the research fellowship. Published paper based on latest trends like pattern recognition using ANN. **Email ID:riteshanantwar36@gmail.com**

Dr P. N. Chatur is the doctorate in Neural Networks and Expert Systems, now working as the Head of Computer Science and Engineering Department , Government College of Engineering , Amravati ,(MH)(INDIA).Published 20 National and 30 international papers in journals and conferences o expert systems and Neural networks. **Email ID: chatur.prashant@gcoea.ac.in**

Swati G. Anantwar pursuing Masters of Engineering in Computer Science and Engineering affiliated to Sant Gadge Baba Amravati University Amravati MH (INDIA),working as an Assistant Professor at HVPM’s College of Engineering Amravati(MH)(INDIA).published and presented various research papers at national and international journals and conferences. **Email ID: swatianantwar@gmail.com**